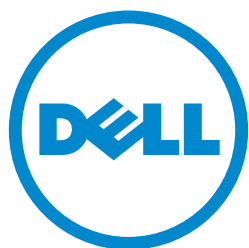


# Analyzer 7.2 Software Getting Started Guide



SonicWALL

## Notes, Cautions, and Warnings



**NOTE:** A NOTE indicates important information that helps you make better use of your system.



**CAUTION:** A CAUTION indicates potential damage to hardware or loss of data if instructions are not followed.



**WARNING:** A WARNING indicates a potential for property damage, personal injury, or death.

© 2014 Dell Inc.

Trademarks: Dell™, the DELL logo, SonicWALL™, SonicWALL Analyzer™, and all other SonicWALL product and service names and slogans are trademarks of Dell Inc.

2014 – 10    P/N 232-002286-00    Rev. C

# Overview

This Getting Started Guide contains installation procedures and configuration guidelines for deploying the Dell SonicWALL Analyzer Software on a server on your network. The Analyzer Software is a Web-based application that can generate dynamic real-time and historical reports for a complete view of all activity through Dell SonicWALL security appliances.

This getting started guide contains the following sections:

- 1 [Before You Begin](#) on page 4
  - [System Requirements](#) on page 4
  - [Record Configuration Information](#) on page 7
- 2 [Introduction to the Management Interfaces](#) on page 8
  - [Overview of the Two Interfaces](#) on page 8
  - [Switching Between Management Interfaces](#) on page 9
  - [UMH System Interface Introduction](#) on page 9
  - [Management Interface Introduction](#) on page 9
- 3 [Installing and Upgrading](#) on page 13
  - [Fresh Install Using Universal Management Suite](#) on page 13
  - [Upgrading From an Earlier Version of Dell SonicWALL Analyzer](#) on page 17
- 4 [Registering and Licensing](#) on page 18
  - [Registering/Licensing After a Fresh Install](#) on page 18
- 5 [Configuring UMH Deployment Options](#) on page 20
  - [Configuring the Deployment Role](#) on page 20
  - [Configuring Deployment Settings](#) on page 21
  - [Controlling Deployment Services](#) on page 25
- 6 [Provisioning and Adding Units](#) on page 26
  - [Provisioning a Dell SonicWALL Firewall Appliance](#) on page 26
  - [Provisioning a Dell SonicWALL SRA SMB Appliance](#) on page 27
  - [Provisioning a Dell SonicWALL E-Class SRA Series Appliance](#) on page 28
  - [Provisioning a Dell SonicWALL CDP Appliance](#) on page 28
  - [Adding Dell SonicWALL Appliances](#) on page 29
- 7 [Support](#) on page 31
  - [Related Technical Documentation](#) on page 31
  - [Live Product Demos](#) on page 32

# Chapter 1

## Before You Begin

---

See the following sections for information about system requirements for the Dell SonicWALL Analyzer Software:

- [System Requirements](#) on page 4
- [Record Configuration Information](#) on page 7

## System Requirements

The Dell SonicWALL Analyzer Software comes with a base license to manage either 5, 10, or 25 nodes. You can purchase additional licenses on MySonicWALL. For more information on licensing additional nodes, visit:

<http://www.sonicwall.com/us/en/products.html>



Note

---

Dell SonicWALL Analyzer Software is not supported on laptops or tablets.

---

Before installing, review the requirements in the following sections:

## Operating System Requirements

The Dell SonicWALL Analyzer Software supports the following operating systems:

- Windows Server 2012 Standard 64-bit
- Windows Server 2012 R2 Standard 64-bit (Japanese Language Version)
- Windows Server 2012 R2 Datacenter
- Windows Server 2008 R2 Datacenter
- Windows Server 2008 SBS R2 64-bit
- Windows Server 2008 R2 Standard 64-bit
- Windows Server 2008 SP2 64-bit
- Windows Server 2003 32-bit and 64-bit (SP2)
- Windows 8 32-bit and 64-bit
- Windows 7 64-bit

These Windows systems can either run in physical standalone hardware platforms, or as a virtual machine under Hyper-V or ESXi.



Tip

---

For best performance and scalability, it is recommended to use a 64-bit Windows operating system. Bundled databases run in 64-bit mode on 64-bit Windows operating systems. All listed operating systems are supported in both virtualized and non-virtualized environments.

---

## Hardware for Windows Server

Use the [Capacity Calculator 2](#) to determine the hardware requirements for your deployment.



Note

A Windows 64-bit operating system with a minimum RAM of 8GB is highly recommended for better performance of reporting modules. Read the Capacity Planning and Performance Tuning appendix in the *GMS 7.2 Administrator's Guide*.

## MySQL Requirements

Dell SonicWALL Analyzer Software automatically installs MySQL as part of the base installation package. Separately installed instances of MySQL are not supported with Analyzer.

## Java Requirements

Download and install the latest version of the Java 7 plug-in on any system that accesses the Analyzer 7.2 management interface. This can be downloaded from:

[www.java.com](http://www.java.com)

or

<http://www.oracle.com/technetwork/java/javase/downloads/index.html>

## Browser Requirements

Dell SonicWALL Analyzer uses advanced browser technologies such as HTML5 that are supported in most recent browsers. Dell SonicWALL recommends using the latest Chrome, Firefox, Internet Explorer, or Safari browsers for administration of the Dell SonicWALL Analyzer.

This release supports the following Web browsers:

- Chrome 18.0 and higher (recommended browser for dashboard real-time graphics display)
- Firefox 16.0 and higher
- Internet Explorer 8.0 and higher (do not use compatibility mode)



Note

Internet Explorer version 10.0 in Metro interfaces of Windows 8 is currently not supported.

Mobile device browsers are not recommended for Dell SonicWALL Analyzer system administration.

## Network Requirements

To complete the Dell SonicWALL Analyzer Software deployment process documented in this *Getting Started Guide*, the following network requirements must be met:

- The Analyzer Software server must have access to the Internet
- The Analyzer Software server must have a static IP address

- The Analyzer Software server's network connection must be able to accommodate at least 1KB/s for each device under management. For example, if Dell SonicWALL Analyzer Software is monitoring 100 Dell SonicWALL appliances, the connection must support at least 100KB/s.

Depending on the configuration of Dell SonicWALL log settings and the amount of traffic handled by each device, the network traffic can vary dramatically. The 1KB/s for each device is a general recommendation. Your installation requirements might vary, refer to the [Capacity Calculator 2](#).

## Dell SonicWALL Appliance and Firmware Support

Dell SonicWALL Platforms	Dell SonicWALL Firmware Version
<b>Firewall / VPN</b>	
SuperMassive 10000 Series	SonicOS 6.0 or newer <b>Note:</b> Only partial reporting support is currently available. Contact your Dell SonicWALL Sales representative for more information.
SuperMassive 9000 Series	SonicOS 6.1 or newer
NSA Series	SonicOS Enhanced 5.0 or newer
TZ Series	SonicOS Enhanced 3.2 or newer SonicOS Standard 3.1 or newer
PRO Series	SonicOS Enhanced 3.2 or newer
CSM Series	SonicOS CF 2.0 or newer
<b>Secure Remote Access</b>	
SMB SRA Series	SonicOS SSL-VPN 2.0 or newer (management) SonicOS SSL-VPN 2.1 or newer (reporting)
E-Class SRA Series	SRA 9.0 or newer
<b>Backup and Recovery</b>	
CDP Series	CDP 2.3 or newer (management) CDP 5.1 or newer (reporting)



Note

Dell SonicWALL Analyzer 7.2 supports firewall App Control reporting. Refer to the SonicOS documentation for information on the supported SonicOS firmware versions.

Appliances running firmware newer than this Analyzer release can still be managed and reports can still be generated. However, the new features in the firmware release will be supported in an upcoming release of Analyzer.

Legacy SonicWALL XPRS/XPRS2, SonicWALL SOHO2, SonicWALL Tele2, and SonicWALL Pro/Pro-VX models are not supported for Dell SonicWALL Analyzer reporting. Appliances running SonicWALL legacy firmware including SonicOS Standard 1.x and SonicWALL legacy firmware 6.x.x.x are not supported for SonicWALL Analyzer reporting.

Dell SonicWALL Analyzer can be connected to SSL-VPN 2000 and 4000 appliances. Use the **Log > ViewPoint** page to set up the Analyzer connection (in addition to the configuration changes made on the Analyzer). In Dell SonicWALL SRA SSL-VPN 5.5 or later firmware versions, a **Log > Analyzer** page is provided for configuration of Analyzer settings.

---

## Record Configuration Information

Before continuing, record the following configuration information for your reference.

<b>SMTP Server Address:</b>	The IP address or host name of your Simple Mail Transfer Protocol (SMTP) server. For example, mail.emailprovider.com.
<b>HTTP Web Server Port:</b>	The number of your Web server port if customized. The default port is 80.
<b>HTTPS Web Server Port:</b>	The number of your secure (SSL) Web server port if customized. The default port is 443.
<b>Administrator Email 1:</b>	The email address of an Analyzer administrator who receives email notifications.
<b>Administrator Email 2:</b>	The email address of an additional Analyzer administrator who receives email notifications. This field is optional.
<b>Sender Email Address:</b>	The email address from which the email notifications are sent.
<b>Database User:</b>	The MySQL user name for the database administrator. This is not required when using the bundled database on this server.*
<b>Database Password:</b>	The MySQL password for the database administrator. This is not required when using the bundled database on this server.*

\*This information is needed if Microsoft SQL Server is used, or in the case of a distributed deployment.

# Chapter 2

## Introduction to the Management Interfaces

---

This section describes the two Dell SonicWALL Analyzer Software management interfaces. An almost identical URL is used when accessing either the Analyzer Software management interface or the Universal Management Host system interface, but the URL is modified to specify either “sgms” or “appliance.”

See the following sections:

- [Overview of the Two Interfaces](#) on page 8
- [Switching Between Management Interfaces](#) on page 9
- [UMH System Interface Introduction](#) on page 9
- [Management Interface Introduction](#) on page 9

## Overview of the Two Interfaces

The Analyzer Software Universal Management Suite (UMS) installs two separate management interfaces:

- **Dell SonicWALL Universal Management Host (UMH) System Management Interface** – Used for system management of the host server, including registration and licensing, setting the admin password, selecting the deployment role, and configuring other system settings.

To access the UMH system management interface on the default HTTP port using a browser on the host server, use the URL:

*<http://localhost/appliance/>*

From another system, access the UMH system management interface with the URL:

*<http://<IP address>:<port>/appliance/>*

If you are using the standard HTTP port, 80, it is not necessary to append the port number to the IP address.

- **Dell SonicWALL Analyzer Management Interface** – Used to access the Analyzer application that runs on the Windows server. This interface is used to configure Analyzer management of Dell SonicWALL appliances, including creating policies, viewing reports, and monitoring networks, and for configuring Analyzer administrative settings.

Access the Analyzer Software management interface with one of the following URLs:

*<http://localhost/sgms/>*

or

*<http://<IP address>:<port>/sgms/>*



# Switching Between Management Interfaces

On systems deployed in the All In One role, the “SuperAdmin” user can easily switch between the UMH system management interface and the Analyzer Software management interface. The SuperAdmin is the master administrator for the entire Analyzer Software installation.



When logged in to either interface, the SuperAdmin can switch to the login page of the other interface by clicking **Switch** in the top right corner of the page. **Switch** is only visible for users with SuperAdmin privileges.

## UMH System Interface Introduction

The Dell SonicWALL UMH system interface is used for system management of the Dell SonicWALL Analyzer Software instance, including registration and licensing, setting the admin password, configuring database settings, selecting the deployment role, and configuring other system settings.

When installing the Dell SonicWALL Universal Management Suite on a host, a Web server is installed to provide the system management interface. The system interface is available by default at <http://localhost/appliance/> after restarting the system.

The login screen allows you to securely log in to the Dell SonicWALL UMH system interface using your system user ID and password.



Note

---

The admin account on the system interface can have a different password than the admin account for Analyzer Software.

---

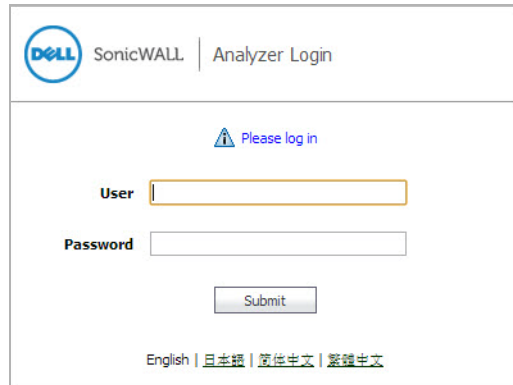
## Management Interface Introduction

Analyzer Software is a Web-based application for configuring and gathering reports from thousands of Dell SonicWALL Internet security appliances and non-Dell SonicWALL appliances, all from a central location. This section provides an introduction to the main elements of the Web-based management interface. This section contains the following subsections:

- [Login Screen](#) on page 10
- [Dashboard](#) on page 10
- [Management Interface](#) on page 11
- [Description of Managed Appliance States](#) on page 12

# Login Screen

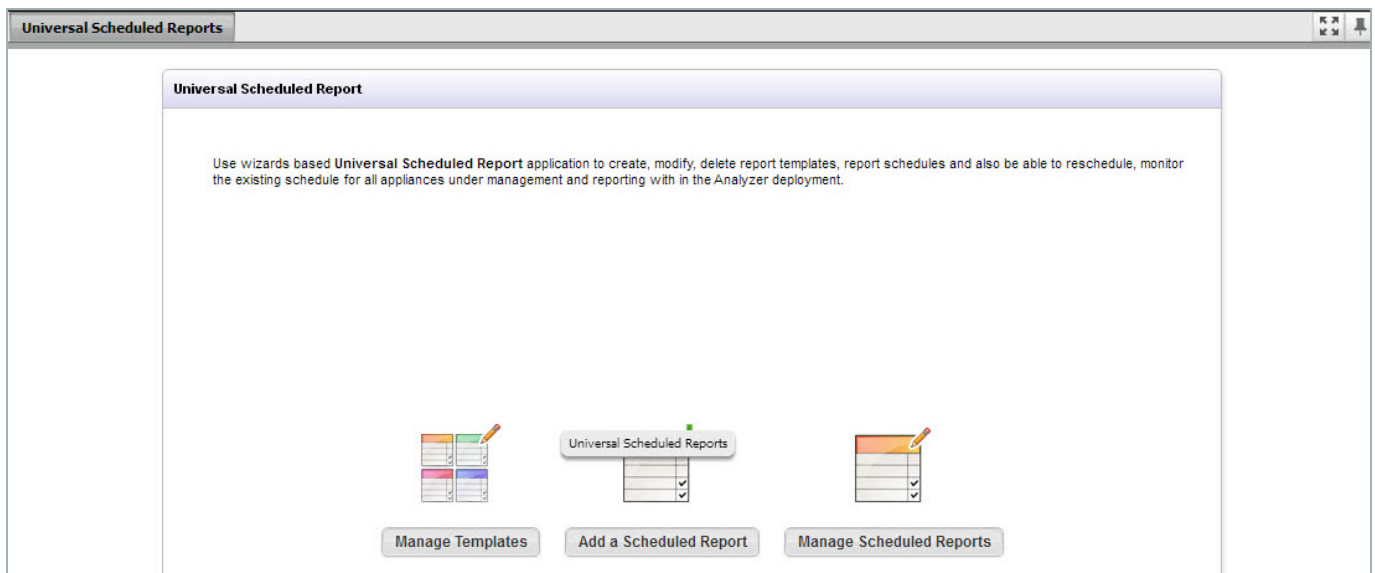
The login screen allows you to securely log in to Analyzer Software using your Analyzer application user ID and password. The Analyzer Software management interface is available by default at <http://localhost/sgms/> after completing registration.



The login screen features the SonicWALL logo and the text "Analyzer Login". Below this, there is a message "Please log in" with a warning icon. The form includes two input fields: "User" and "Password". A "Submit" button is located below the password field. At the bottom, there are language options: "English", "日本語", "简体中文", and "繁體中文".

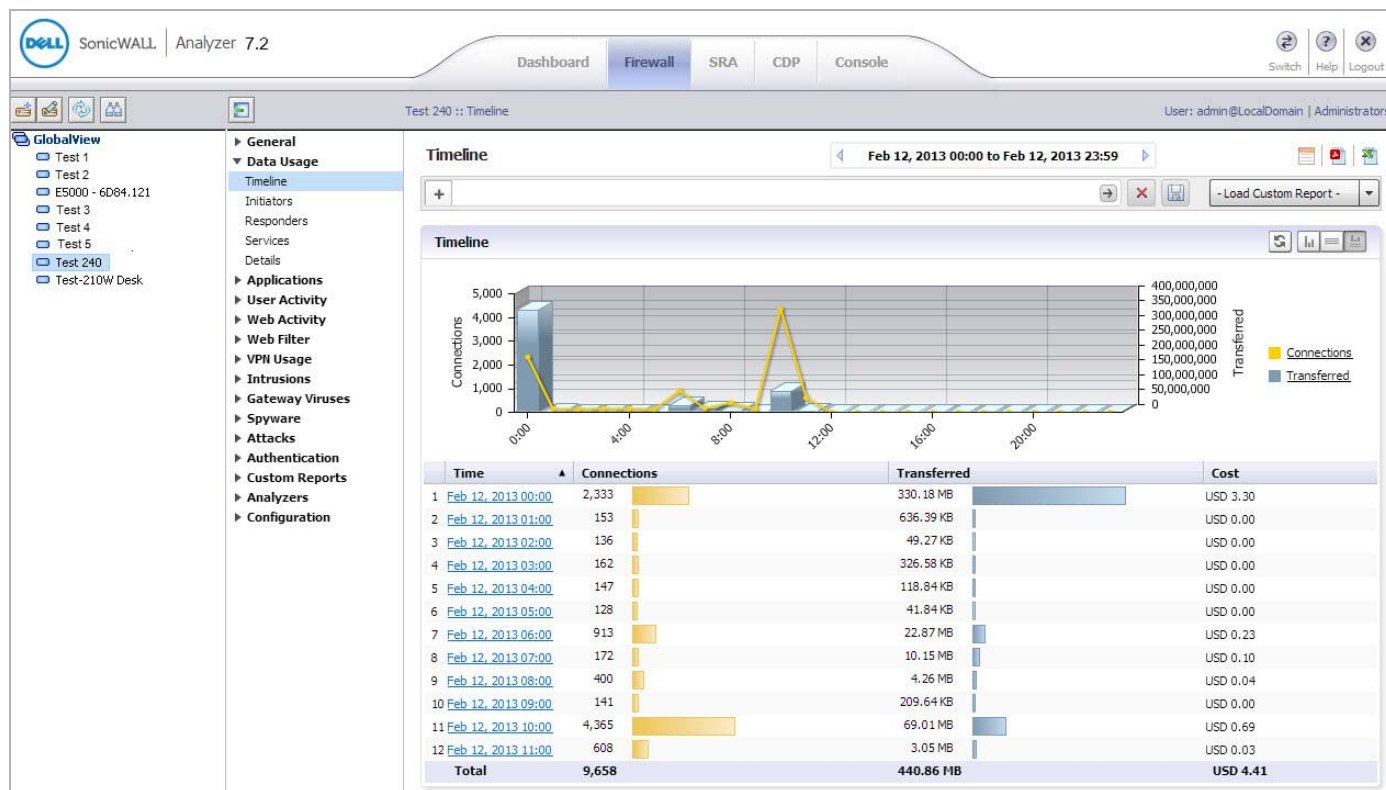
# Dashboard

The Dashboard control bar provides top-of-the page menu items for customizing the settings of this page. When the Dashboard loads after the Analyzer Software login, the control bar is displayed and then becomes hidden until you place your mouse cursor at the top of the page as shown in the following figure. You can lock the control bar by clicking on the “pin the control bar” icon.



# Management Interface

The Analyzer Software management interface is the main control panel. The management interface allows you to add and modify appliances, perform monitoring and reporting tasks, and configure Analyzer Software settings.



The management interface offers the following navigation features:

- [Navigation Tabs](#) on page 11
- [Left Pane](#) on page 11
- [Center Pane](#) on page 12
- [Right Pane](#) on page 12

## Navigation Tabs

The management interface navigation tabs are located at the top of the management interface.

The navigation tabs are: Dashboard, Firewall, SRA, CDP, and Console. The Console tab provides tools to customize options found in the other Analyzer tabs and to manage Analyzer Software settings that affect the environment globally.

## Left Pane

The left pane of the management interface provides a tree control that displays the current Analyzer Software view and a list of managed appliances within the current tab. The left pane is only displayed for the Firewall, SRA, and CDP appliance tabs. The current category and view are indicated by a blue highlighting. The left pane tree control provides the ability to switch between views and displays the current state of each appliance under management. A single box in the tree control indicates a node at appliance or unit level. Two boxes in the tree control

indicates a node at a group level. A global node at the top of the tree control is indicated by a three-box icon. The color and additional images superimposed on these icons provide useful status information. For detailed information about appliance states, refer to [Description of Managed Appliance States](#) on page 12.



Note

If there is only one appliance visible in the Left Pane, then the Left Pane automatically collapses to present a larger screen for the rest of the UI.

## Center Pane

The center pane displays in the appliance tabs: Firewall, SRA, and CDP. A navigational tree control that provides access to the configuration options available based on navigational tab and left pane selections. The Reports sub-tab provides reporting on the global or appliance level, and is only available for Firewall, SRA, and CDP.



The current selection in the center pane is indicated by the highlighted item. The center pane options change based on the navigational tab and left pane selections, and selections in the center pane modify the display in the right pane.

## Right Pane

The right pane displays the available status or tasks based on the current selection of navigational tab, left pane and center pane options. Configurations performed in the right pane modify global or appliance settings.

## Description of Managed Appliance States

This section describes the meaning of icons that appear next to managed appliances listed in the left pane of the Dell SonicWALL Analyzer Software management interface.

Appliance Status	Description
	One blue box indicates that the appliance is operating normally. The appliance is accessible from the Analyzer Software, and no tasks are pending or scheduled.
	Three blue boxes indicate that all appliances in the global group of this type (Firewall/SRA/CDP) are operating normally.

# Chapter 3

## Installing and Upgrading

---

This section provides procedures for installing the Dell SonicWALL Analyzer Software and upgrading the Dell SonicWALL Analyzer Software from a previous version. The Analyzer Software can only be configured for a single server.



**Note** You must disable the User Account Control (UAC) feature on Windows before running the Dell SonicWALL Analyzer Software installer. In addition, disable Windows Firewall or your personal firewall before running this installer.

---

This section contains the following subsections:

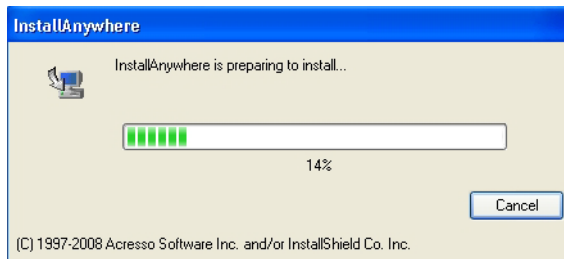
- [Fresh Install Using Universal Management Suite](#) on page 13
- [Upgrading From an Earlier Version of Dell SonicWALL Analyzer](#) on page 17

## Fresh Install Using Universal Management Suite

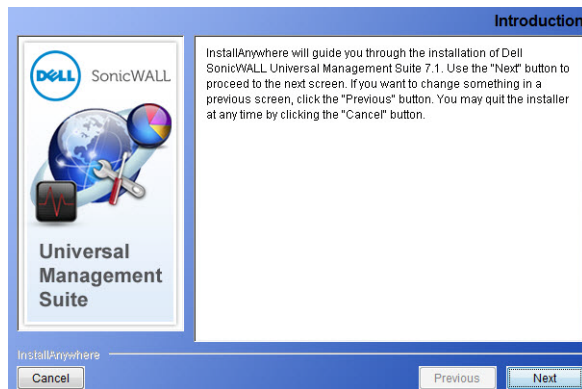
In Dell SonicWALL Analyzer, all software components related to GMS and Analyzer, including the MySQL database, executable binary files for all Analyzer services, and other necessary files, are installed using the Universal Management Suite single-binary installer. All GMS and Analyzer files are installed as the Universal Management Suite, but no distinction is made between GMS and Analyzer during the installation. The initial installation phase takes just a few minutes for any type of installation, such as GMS server, Analyzer server, database server, or any other role.

To do a fresh install of the Universal Management Suite from the single binary installer, complete the following steps:

- 
- Step 1** Log on to your Dell SonicWALL Analyzer management computer as **administrator** (Windows). Launch the Dell SonicWALL Universal Management Suite installer, by right-clicking the file **sw\_gmsvp\_win\_eng\_7.2.xxxx.xxxx.exe** (where “xxxx” represent the exact version numbers) and select **Run as administrator**. It can take several seconds for the InstallAnywhere self-extractor to initialize.



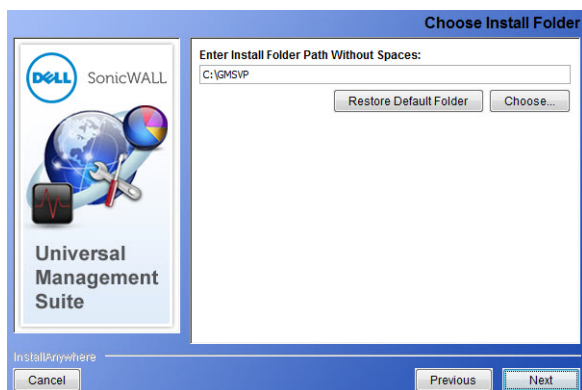
Step 2 In the Introduction screen, click **Next**.



Step 3 In the License Agreement screen, select the radio button next to **I accept the terms of the License Agreement**. Click **Next**.



Step 4 Select the path to the folder where you would like to install the files. You can accept the default path, **C:\GMSVP**, type in a new path, or click **Choose** to navigate to the selected folder. When you are finished, click **Next**.



**Note** Do not include spaces in the installation path.

Step 5 In the Universal Management Suite Settings screen, select or type in the IP address to which the Dell SonicWALL Analyzer services should bind to listen for inbound TCP, UDP, SNMP, syslog, or other packets. The installer detects and offers radio buttons for any IP addresses associated with the system. The default is your management computer IP address. To use a different IP address, select **Other** and type the IP address into the field. Click **Next**.

Step 6 To use a custom port for HTTP or HTTPS traffic to the system's Web Server, type the port number into the **HTTP Port** or **HTTPS Port** field.

If you receive the message "Cannot bind to the port number specified. Specify a different one," the port you specified is in use by another program, for example, Internet Information Services (IIS). Specify a different, unused port, such as 8080.



**Tip** If you specify a custom port, you need to modify the URLs you use to access GMS by using the following format:

*http://localhost:<port>/* (to login from the local host)

or

*http://<ipaddress>:<port>/* (to login from a remote location)

For example, if you specified HTTP port 8080, the URLs would look like this:

*http://localhost:8080/* (for a local host login)

or

*http://10.0.93.20:8080/* (for a remote login)

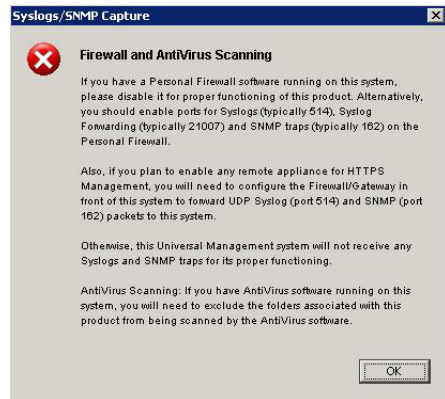
Step 7 Click **Install**.

Step 8 If you see a Windows Security Alert for Java, click **Unblock**.



Step 9 The installer displays a progress bar as the files are installed. Wait a few minutes for the installer to finish installing.

Step 10 After the files are installed, whether or not the system has a Personal Firewall such as Windows Firewall enabled, a dialog is displayed notifying you to either disable the firewall or manually open the syslog and SNMP ports, and to ensure that these ports are open on your network gateway or firewall if you plan to use HTTPS Management mode for managing remote appliances (instead of Management Tunnel or Existing Tunnel modes). It also mentions that if you have AntiVirus software running on your system, you need to exclude the folders associated with this product from being scanned by the AntiVirus Software. Click **OK**. Be sure to adjust the settings as recommended.



Step 11 The Important Registration Information screen provides the URL and credentials to use to log in to the Analyzer Universal Management Host system interface after restarting your system:

- The default URL for accessing the interface from the local system is:  
*http://localhost:80/*
- The default credentials are:  
**User name**—*admin*  
**Password**—*password*

To register a Analyzer Software installation, use the 12-character serial number that you received when you purchased this product.

Step 12 Click **Next**.

Step 13 In the Installation Complete screen, select **Yes, restart my system** to restart your system immediately, or select **No, I will restart my system myself** to restart your system later. Click **Done**.

Step 14 After restarting your system, you can access the Dell SonicWALL UMH system interface to register the product and configure the Analyzer server settings on this system.

Access the Analyzer Software UMH system interface by either clicking on the new desktop shortcut for **Dell SonicWALL Universal Management Suite** (your default Web browser launches <http://localhost/appliance/login>), or by pointing your browser to <http://localhost/>.

Step 15 Log in using the these credentials:

**username**—*admin*  
**password**—*password*

You are prompted to change your password.



**Note** You are forced to change your password the first time you login.

To register and license Dell SonicWALL Analyzer Software, see [Registering/Licensing After a Fresh Install](#) on page 18.



# Upgrading From an Earlier Version of Dell SonicWALL Analyzer

You can use the Dell SonicWALL UMS installer to upgrade the Dell SonicWALL Analyzer Software.

It is highly recommended that you backup your database, Analyzer installation folders, and the “<Analyzer installation folder>\conf\sgmsConfig.xml” file on the Analyzer server prior to performing the Analyzer Software upgrade.

To upgrade the Dell SonicWALL Analyzer Software, complete the following steps:

- 
- Step 1 Log on to your Dell SonicWALL Analyzer management computer as **administrator** (Windows). Launch the Dell SonicWALL Universal Management Suite installer, by double-clicking the file **sw\_gmsvp\_win\_eng\_7.2.xxxx.xxxx.exe** (where “xxxx” are the exact version numbers). It might take several seconds for the InstallAnywhere self-extractor to initialize.
  - Step 2 In the Introduction screen, click **Next**.
  - Step 3 In the License Agreement screen, select the radio button next to **I accept the terms of the License Agreement**. Click **Next**.
  - Step 4 Wait while the installer prepares to install Dell SonicWALL UMS on your system.
  - Step 5 Click **Install** to upgrade your installation.
  - Step 6 The Installer detects the previous installation of Analyzer Software. Click **Install** to proceed with the upgrade.
  - Step 7 If you see a Windows Security Alert for Java, click **Unblock**.
  - Step 8 The installer displays a progress bar as the files are installed. Wait a few minutes for the installer to finish installing.
  - Step 9 After the files are installed, whether or not the system has a Personal Firewall such as Windows Firewall enabled, a dialog is displayed notifying you to either disable the firewall or manually open the syslog and SNMP ports, and to ensure that these ports are open on your network gateway or firewall if you plan to use HTTPS Management mode for managing remote appliances (instead of Management Tunnel or Existing Tunnel modes). Click **OK**. Be sure to adjust the settings as recommended.
  - Step 10 The final installer screen contains the path of the installation folder, and warns you that the Universal Management Suite Web page will be launched next. Click **Done**.

# Chapter 4

## Registering and Licensing

---

All instances of the Dell SonicWALL Analyzer Software must be registered and licensed before use. This requirement applies to single server deployments, to fresh or upgraded installations, and to Software installations on Windows servers or to Dell SonicWALL UMA appliances.

### Registering/Licensing After a Fresh Install

The Analyzer Software registration is performed using the Dell SonicWALL Universal Management Host (UMH) system interface. When installing the Universal Management Suite on a server or host, a Web server is installed to provide the UMH system interface. The system interface is available by default after restarting the system at: <http://localhost/>.

On Dell SonicWALL appliances that send reporting data to the Analyzer, Analyzer is licensed and activated separately from the Dell SonicWALL appliances. MySonicWALL provides a way to associate Dell SonicWALL appliances with the Analyzer instance installed on the Windows system. Licensing your Analyzer application requires:

- **A MySonicWALL account**—allows you to manage your Dell SonicWALL products and purchase licenses for various services. Creating a MySonicWALL account is fast, simple, and free. Simply complete an online registration form directly from your Dell SonicWALL security appliance management interface. Your MySonicWALL account is also accessible at <https://www.mysonicwall.com> from any Internet connection with a Web browser. After you have an account, you can purchase Dell SonicWALL Analyzer and other licenses for your registered Dell SonicWALL security appliances.
- **A registered Dell SonicWALL security appliance with active Internet connection**—you need to register your Dell SonicWALL security appliance to activate Analyzer. Registering your Dell SonicWALL security appliance is a simple procedure done directly from the management interface. After your Dell SonicWALL security appliance is registered, you can activate Dell SonicWALL Analyzer by using an activation key or by synchronizing with [mysonicwall.com](https://www.mysonicwall.com).



Note MySonicWALL registration information is not sold or shared with any other company.

To register and license Analyzer Software on a server, complete the following steps:

- 
- Step 1 Double-click the Dell SonicWALL Universal Management Suite desktop icon or open a Web browser and enter **<http://localhost/>** to launch the UMH system interface.



Note If you specified a custom port (a port other than the default port 80), modify the URL as follows: <http://localhost:<port>/>

For example, if you specified port 8080, the URL would be: <http://localhost:8080/>.

---

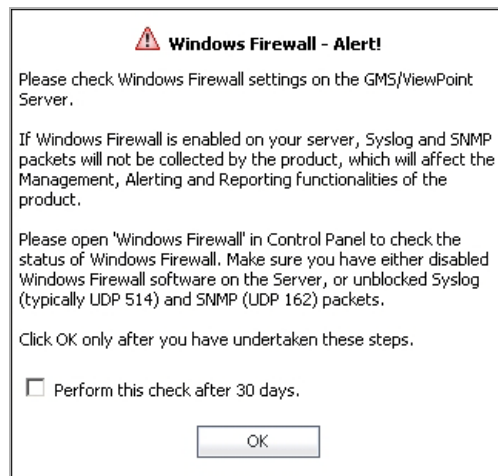
- Step 2 The login page loads by default in English, type *admin* in the **User** field, and *password* in the **Password** field and then click **Submit**.

Analyzer Software includes language support for English, Japanese, Simplified Chinese, Traditional Chinese. Click the language of your choice at the bottom of this page.

- Step 3 The Login page reloads to force a password change. Type a new password into both the **New Password** and **Confirm New Password** fields, and then click **Submit**.

- Step 4 If the software detects that the Windows Firewall is enabled on the system, a warning dialog box is displayed on top of the **System > Status** page. To receive syslog and SNMP packets, either disable the Windows Firewall or configure it to open these ports (default syslog port is UDP 514 and default SNMP port is UDP 162). When ready, click **OK**.

Optionally, you can select **Perform this check after 30 days** if you do not plan to disable the Windows Firewall immediately, and do not wish to see this warning every time you login. The check for Windows Firewall cannot be disabled completely, and if you leave it running you will see this alert after the 30-day delay. You can repeat the delay as many times as needed.



- Step 5 On the **System > Status** page, the **Registration Pending** notification across the top of the screen indicates that the system is not registered, the Serial Number status is **UNKNOWN**, and the License status displays **Not Licensed**. To begin registration, click **Register** in the top, right corner.
- Step 6 On the License Management page, type your MySonicWALL user name and password into the appropriate fields and then click **Submit**.



**Note** If you do not have a MySonicWALL account, you must create one before continuing.

- Step 7 In the next License Management page, type *ANALYZER* (all capital letters) into the **Serial Number** field and leave the **Authentication Code** fields blank.

- Step 8 Type a friendly name for the system into the **Friendly Name** field. The friendly name is displayed on MySonicWALL to more easily identify the installation on this system.

- Step 9 Click **Submit**, the License Management page displays a completion screen.

- Step 10 Click **Continue**, the License Management page displays license summary information.

When registration is complete, the **Deployment > Roles** page is displayed. Although there is only one possible role for a Analyzer Software deployment, you must still configure certain fields on this page and then click **Update** to fully activate the application. For instructions on configuring these settings, see the [Configuring UMH Deployment Options](#) on page 20.

# Chapter 5

## Configuring UMH Deployment Options

The Analyzer single server configuration (default) is an All in One role and is the only role available for Analyzer. All services of Analyzer run on a single server, including the MySQL database. The role assigned to your Dell SonicWALL Analyzer Software defines the Dell SonicWALL Universal Management Suite services that it provides. The following Dell SonicWALL Universal Management Suite services run in the Analyzer “All in One” system:

- Database
- Reports Database
- Reports Scheduler
- Reports Summarizer
- Scheduler
- Syslog Collector
- Update Manager
- Web Server

## Configuring the Deployment Role

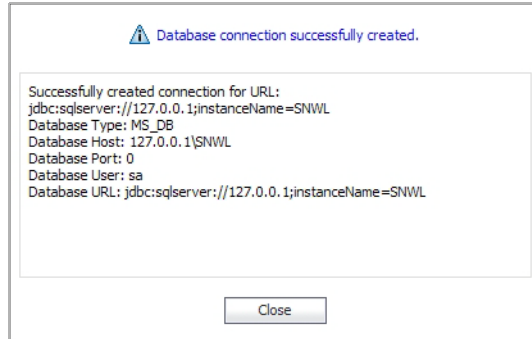
In a Analyzer Software installation, the **Deployment > Roles** page provides a way to configure the syslog port and the database settings, and to test database connectivity.

The screenshot shows the 'Host Role Configuration' page. On the left, a navigation menu has 'Roles' selected. The main content area is titled 'Host Role Configuration' and contains a 'Single Server Configuration' section. In this section, the 'Analyzer' role is selected, and the 'Syslog Server Port' is set to 3003. Below this is the 'Database Configuration' section, which includes fields for 'Database Type' (MySQL), 'Database Host' (localhost), 'Database Port' (3306), 'Database User' (gmsadm), 'Database Password' (empty), 'Confirm Database Password' (empty), 'Database Driver' (com.mysql.jdbc.Driver), and 'Database URL' (jdbc:mysql://localhost:3306). There are buttons for 'Test Connectivity', 'Update', and 'Reset'.

To configure the deployment role, complete the following:

- Step 1 To set the syslog port, enter the port number into the **Syslog Server Port** field.
- Step 2 Under Database Configuration, to provide credentials with which Analyzer Software accesses the database, enter the account user name into the **Database User** field

- Step 3 Enter the account password into both the **Database Password** and **Confirm Database Password** fields.
- Step 4 Additionally, you can enter a **Database Driver** file name and the **Database URL** for an explicit directory path location.
- Step 5 To test connectivity to the database server, click **Test Connectivity**. A pop-up message displays the database connectivity status.



- Step 6 When finished, click **Update** to apply the changes. To revert the fields on the page to their default settings, click **Reset**.

## Configuring Deployment Settings

This section describes the UMH/UMA **Deployment > Settings** page, used for Web port, SMTP, and SSL access configuration.

The **Deployment > Settings** page is identical in both the UMH and UMA management interfaces, except for the left navigation pane that shows the Network menu item on the UMA.

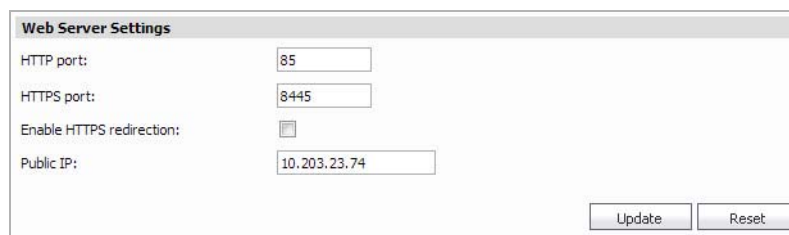
See the following sections:

- [Configuring Web Server Settings](#) on page 22
- [Configuring SMTP Settings](#) on page 23
- [Configuring SSL Access](#) on page 24

# Configuring Web Server Settings

Web Server Settings configuration is largely the same on any role:

- Step 1 Navigate to **Deployment > Settings > Web Server Settings** in the /appliance management interface.



The screenshot shows the 'Web Server Settings' configuration window. It contains four input fields: 'HTTP port:' with the value '85', 'HTTPS port:' with the value '8445', 'Enable HTTPS redirection:' with an unchecked checkbox, and 'Public IP:' with the value '10.203.23.74'. At the bottom right, there are two buttons: 'Update' and 'Reset'.

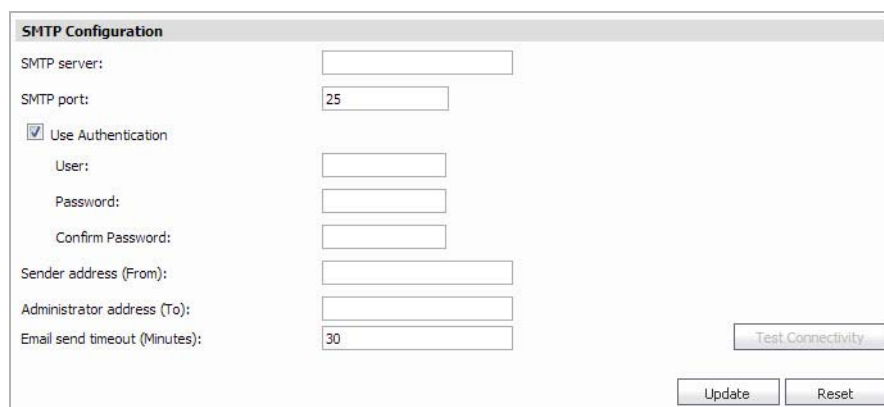
- Step 2 To use a different port for HTTP access to the Dell SonicWALL Analyzer Software, type the port number into the **HTTP Port** field. The default port is 80.
- Step 3 If you enter another port in this field, the port number must be specified when accessing the appliance management interface or Analyzer Software management interface. For example, if port 8080 is entered here, the appliance management interface would be accessed with the URL: `http://<IP Address>:8080/appliance/`.
- Step 4 To use a different port for HTTPS access to the Dell SonicWALL Analyzer Software, type the port number into the **HTTPS Port** field. The default port is 443.
- Step 5 If you enter another port in this field, the port number must be specified when accessing the appliance management interface or Analyzer Software management interface. For example, if port 4430 is entered here, the appliance management interface would be accessed with the URL: `https://<IP Address>:4430/appliance/`.
- Step 6 Click **Enable HTTPS Redirection** to redirect HTTP to HTTPS when accessing the Analyzer management interface.
- Step 7 In the **Public IP** text-field, enter the public IP or FQDN of the outside web services.
- Step 8 When you are finished configuring the Web Server Settings, click **Update**.

# Configuring SMTP Settings

The SMTP Configuration section allows you to configure an SMTP server name or IP address, a sender email address, and an administrator email address. You can test connectivity to the configured server.

To configure SMTP settings:

- Step 1 Navigate to the **Deployment > Settings** page under the **SMTP Configuration** section.



The screenshot shows the 'SMTP Configuration' form. It includes fields for 'SMTP server:', 'SMTP port:' (with '25' entered), 'Use Authentication' (checked), 'User:', 'Password:', 'Confirm Password:', 'Sender address (From):', 'Administrator address (To):', and 'Email send timeout (Minutes):' (with '30' entered). There are 'Test Connectivity', 'Update', and 'Reset' buttons at the bottom right.

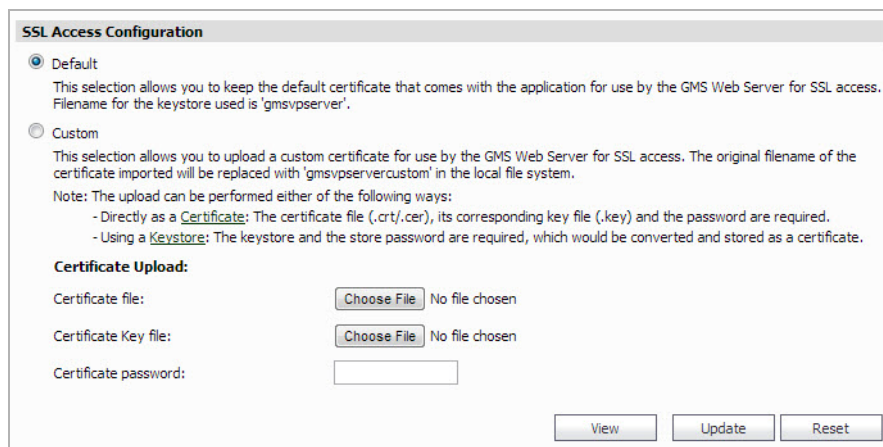
- Step 2 Type the FQDN or IP address of the SMTP server into the **SMTP server** field.
- Step 3 If the SMTP server in your deployment is set to use authentication, click **Use Authentication**. This option is necessary for all outgoing Analyzer emails to properly send to the intended recipients. Enter the username in the **User** field, and enter/confirm the password in the **Password** and **Confirm Password** fields. This is the username/password that is used to authenticate against the SMTP server.
- Step 4 Type the email address from which mail is sent into the **Sender address** field.
- Step 5 Type the email address of the system administrator into the **Administrator address** field.
- Step 6 In the **Email send timeout** field, enter a timeout interval (in minutes). If the server does not respond within the specified interval, the Email send action is stopped and an error is reported.
- Step 7 To test connectivity to the SMTP server, click **Test Connectivity**.
- Step 8 To apply your changes, click **Update**.

# Configuring SSL Access

The SSL Access Configuration section allows you to configure and upload a custom Keystore/Certificate file for SSL access to the GMS appliance, or select the default local keystore.

To configure SSL access:

- Step 1 Navigate to the **Deployment > Settings** page under **SSL Access Configuration** section.



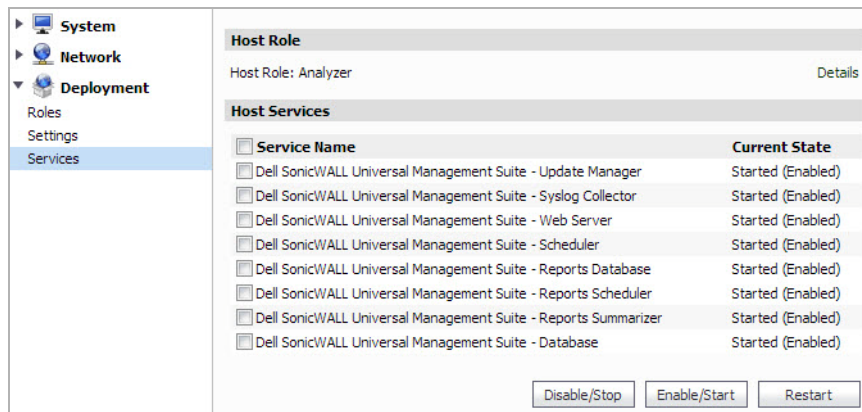
The screenshot shows the 'SSL Access Configuration' web page. It has a title bar 'SSL Access Configuration'. Below it, there are two radio buttons: 'Default' (selected) and 'Custom'. The 'Default' option has a description: 'This selection allows you to keep the default certificate that comes with the application for use by the GMS Web Server for SSL access. Filename for the keystore used is 'gmsvpserver''. The 'Custom' option has a description: 'This selection allows you to upload a custom certificate for use by the GMS Web Server for SSL access. The original filename of the certificate imported will be replaced with 'gmsvpservercustom' in the local file system.' Below the descriptions, there is a 'Note' section: 'Note: The upload can be performed either of the following ways: - Directly as a Certificate: The certificate file (.crt/.cer), its corresponding key file (.key) and the password are required. - Using a Keystore: The keystore and the store password are required, which would be converted and stored as a certificate.' Below the note, there is a 'Certificate Upload:' section. It contains three fields: 'Certificate file:' with a 'Choose File' button and 'No file chosen' text; 'Certificate Key file:' with a 'Choose File' button and 'No file chosen' text; and 'Certificate password:' with a text input field. At the bottom right, there are three buttons: 'View', 'Update', and 'Reset'.

- Step 2 Select **Default** to keep, or revert to, the default settings, where the default GMS Web Server certificate with 'gmsvpserverks' keystore is used.
- Step 3 Select **Custom** to upload a custom keystore certificate for GMS SSL access.
- Step 4 In the **Certificate file** field, click **Choose File** to select your certificate file.
- Step 5 In the **Certificate Key file** field, click **Choose File** to select your certificate key file.
- Step 6 Type the password for the certificate into the **Certificate password** field.
- Step 7 Click **View** to display details about your certificate.
- Step 8 Click **Update** to submit your changes.



# Controlling Deployment Services

The **Deployment > Services** page provides a list of the services that are running on your system as part of Analyzer Software. It also provides a way to stop or start any of the services.



To stop a service that is currently Enabled, select the checkbox for that service and then click **Disable/Stop**.

To start a service that is currently Disabled, select the checkbox for that service and then click **Enable/Start**.

To restart a service that is either Enabled or Disabled, select the checkbox for that service and then click **Restart**.

# Chapter 6

## Provisioning and Adding Units

After installation, registration, and role configuration, the next steps in setting up your Dell SonicWALL Analyzer Software are provisioning Dell SonicWALL appliances to support Analyzer and adding them to the Dell SonicWALL Analyzer. All Dell SonicWALL appliances must be provisioned before adding them to the Dell SonicWALL Analyzer. Make sure the provisioned Dell SonicWALL appliances have a valid Analyzer license, one Analyzer license for each Dell SonicWALL appliance.

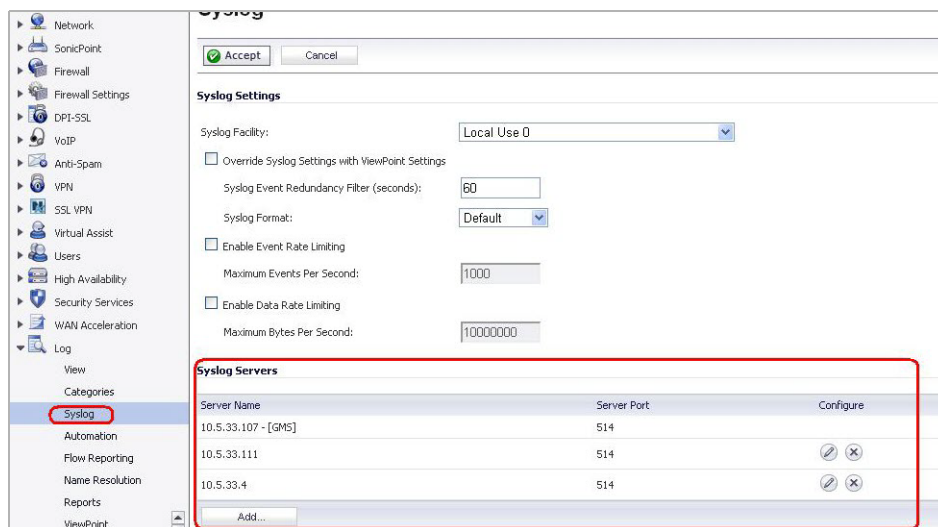
This chapter contains the following sections:

- [Provisioning a Dell SonicWALL Firewall Appliance](#) on page 26
- [Provisioning a Dell SonicWALL SRA SMB Appliance](#) on page 27
- [Provisioning a Dell SonicWALL E-Class SRA Series Appliance](#) on page 28
- [Provisioning a Dell SonicWALL CDP Appliance](#) on page 28
- [Adding Dell SonicWALL Appliances](#) on page 29

## Provisioning a Dell SonicWALL Firewall Appliance

To provision a Dell SonicWALL firewall appliance to support Analyzer, do the following:

- Step 1 Log in to the firewall appliance. Navigate to the **Log > Syslog** page.
- Step 2 In Syslog Servers, click **Add**.
- Step 3 Enter the Analyzer IP address to start sending syslogs. The Analyzer service should be activated. Set the log in UTC format and log category.



Step 4 Navigate to the **System > Time** page, and enable **Display UTC in logs (instead of local time)**.



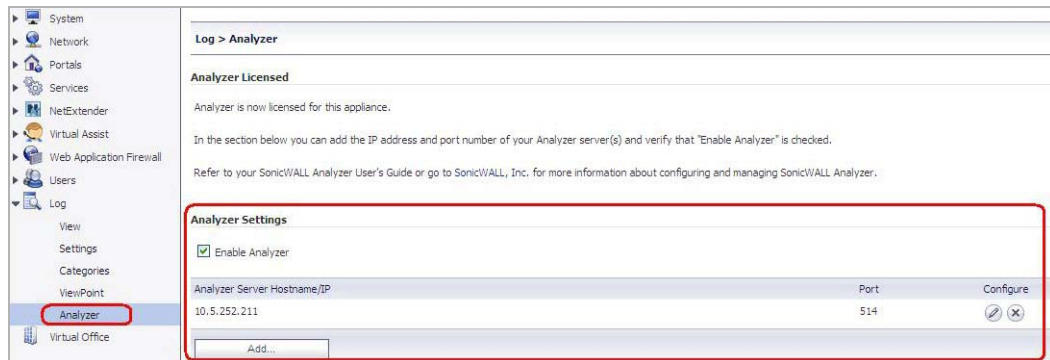
## Provisioning a Dell SonicWALL SRA SMB Appliance

To provision a Dell SonicWALL SRA SMB appliance for Dell SonicWALL Analyzer, do the following:

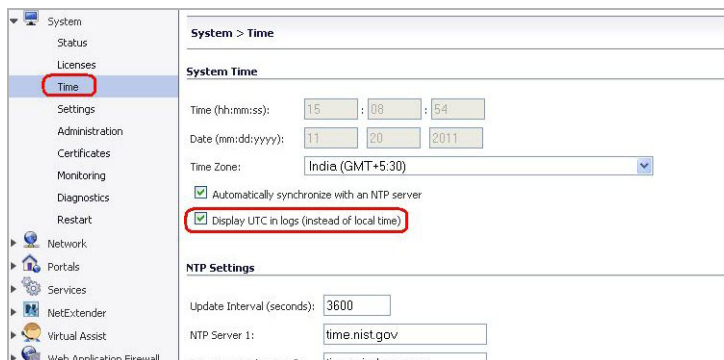
Step 1 Log in to the SRA SMB appliance. Navigate to the **Log > Analyzer** page.

Step 2 In Analyzer Settings, click **Enable Analyzer**.

Step 3 Click **Add** to add the Analyzer IP address, this starts sending syslogs.



Step 4 Navigate to the **System > Time** page, and enable **Display UTC in logs (instead of local time)**.



# Provisioning a Dell SonicWALL E-Class SRA Series Appliance

Currently there is no Analyzer settings implementation in SonicWALL E-Class SRA series appliances. To add Analyzer reporting support, use the **Additional ViewPoint** settings in the **General Settings > Configure Centralized Management** screen, and enter the Analyzer IP address and port number to start sending syslog.

**Security Administration**  
Access Control  
Resources  
Users & Groups  
**User Access**  
Realms  
Aventail WorkPlace  
Agent Configuration  
End Point Control  
**System Configuration**  
General Settings  
Network Settings  
SSL Settings  
Authentication Servers  
Services  
Virtual Assist  
Maintenance  
**Monitoring**  
User Sessions  
System Status  
Logging  
Troubleshooting

**Configure Centralized Management** [General Settings > Configure Centralized Management](#)

Configure this appliance for use with a Global Management System (GMS) server and/or a ViewPoint reporting server.

**GMS/ViewPoint server settings**

☒ Enable GMS/ViewPoint

GMS/ViewPoint server address:\*

GMS/ViewPoint server port:\*

Heartbeat interval:\*  seconds

Options: ☐ Send only heartbeat status messages  
Note: Choosing this option will disable syslog required for reporting

**Additional ViewPoint server**

☒ Enable additional ViewPoint server

ViewPoint server address:\*

ViewPoint server port:\*

**GMS/ViewPoint credentials**

Password:\*

Confirm password:\*

Options: ☒ Enable single sign-on for AMC configuration

On the GMS/ViewPoint Add Unit screen, add this appliance by entering "GMS" as the login name and this value as the password.

# Provisioning a Dell SonicWALL CDP Appliance

Currently there is no Analyzer settings implementation in Dell SonicWALL CDP appliances. To add Analyzer reporting support, use the **Analyzer** settings in the **Settings > SMB** screen. In Active Report, select **Enable**. And enter the Analyzer IP address and port number to start sending CDP syslog.

[Log out](#)

Your Device: CDP 2440i  
Status: Registered

**System**  
Status  
**Settings**  
Administration  
Diagnostics  
Registration/Licenses  
Activity Progress

**System > Settings**

Password | Time | NTP | Mail | Alert | Email Reports | **GMS** | Offsite | Import/Export

**Heartbeat Syslog**

☒ Enable

Name/IP Address:

Port:

Interval (Sec):

Minimum Syslog Priority:

**Activity Report**

☒ Enable

Name/IP Address:

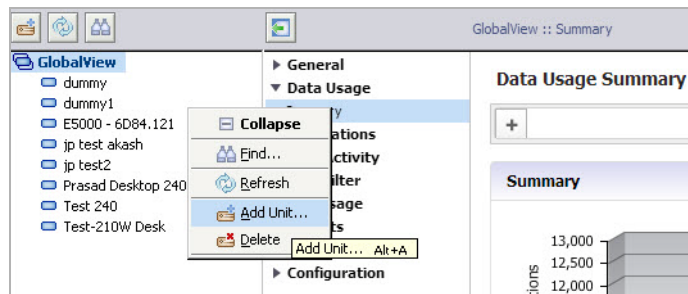
Port:

# Adding Dell SonicWALL Appliances

This section describes how to add Dell SonicWALL appliances to the Dell SonicWALL Analyzer. Analyzer Software checks with the Dell SonicWALL licensing server when you add an appliance, so it is important that Dell SonicWALL Analyzer has Internet access to the server. Analyzer Software can communicate with Dell SonicWALL appliances through HTTP or HTTPS.

To add a Dell SonicWALL appliance using the Analyzer Software management interface, do the following:

- 
- Step 1 Click the appliance tab that corresponds to the type of appliance that you want to add:
- **Firewall**
  - **SRA**
  - **CDP**
- Step 2 Expand the Analyzer Software tree and select the group to which you are adding the Dell SonicWALL appliance. Then, right-click the group and select **Add Unit** from the pop-up menu. To not specify a group, right-click an open area in the left pane (TreeControl pane) of the Analyzer Software management interface and select **Add Unit** or click the **Add Unit** icon in the tool bar.



The Add Unit dialog box appears:

A screenshot of the 'Add Unit' dialog box. It has a title bar with a close button. The dialog contains several input fields: 'Unit Name:', 'Serial Number:', 'IP Address:', 'Login Name:' (with 'admin' entered), 'Password:', 'Access Mode:' (with 'Use Secure login (HTTPS)' selected), and 'Management Port:' (with '443' entered). At the bottom, there are 'OK' and 'Cancel' buttons.

- Step 3 Enter a descriptive name for the Dell SonicWALL appliance in the **Unit Name** field. Do not enter the single quote character (') in the **Unit Name** field.
- Step 4 Enter the serial number of the Dell SonicWALL appliance in the **Serial Number** field.
- Step 5 Enter the IP address of the Dell SonicWALL appliance in the **IP Address** field.
- Step 6 Enter the administrator login name for the Dell SonicWALL appliance in the **Login Name** field.

- Step 7 Enter the password used to access the Dell SonicWALL appliance in the **Password** field.
- Step 8 For Access **Mode**, select from the following:
- Step 9 The Dell SonicWALL appliance is connected with HTTPS by default.
- Step 10 Enter the port used to connect to the Dell SonicWALL appliance in the **Management Port** field (default port for is HTTPS: 443).
- Step 11 Click **OK**. The new Dell SonicWALL appliance appears in the Analyzer management interface. It has a yellow icon that indicates it has not yet been successfully acquired.
- Step 12 Analyzer then attempts to set up an HTTPS connection to access the appliance. Analyzer then reads the appliance configuration and acquires the Dell SonicWALL appliance for reporting. This takes a few minutes.



---

**Note** After the Dell SonicWALL appliance is successfully acquired, its icon turns blue, its configuration settings are displayed at the unit level, and its settings are saved to the database.

---

# Chapter 7

## Support

## Related Technical Documentation

Dell SonicWALL reference documentation is available at the Dell SonicWALL Technical Documentation Online Library:

<https://support.software.dell.com/>

Dell SonicWALL Analyzer video training is available from the Analyzer Development Team:

<http://software.sonicwall.com/gmsvp/Dev-Training/>

The Dell SonicWALL Analyzer 7.2 documentation set includes the following:

- Dell SonicWALL Analyzer 7.2 Release Notes
- Dell SonicWALL Analyzer 7.2 Software Getting Started Guide
- Dell SonicWALL Analyzer 7.2 Virtual Appliance Getting Started Guide
- Dell SonicWALL Analyzer 7.2 Administrator's Guide

The screenshot shows the Dell SonicWALL Product Support page for the Analyzer product. The page has a blue header with the Dell logo and navigation links: Products, Solutions, How to Buy, Support, Sign In, and Register. A search bar is located in the top right corner. The main content area is titled "Product Support" and "Analyzer". Below the title, there are social media links for Facebook, LinkedIn, and Twitter. The page is divided into two main sections: "Support Documents" and "Knowledge Base". Under "Support Documents", there is a "List View Options" section with a filter to focus on items of interest. Below this, there are "Categories" with checkboxes for Video Tutorials, Product Guides, Technical Notes, Release Notes, and Support Data Sheets. The "Product Guides" section shows a list of 5 guides, including "Dell SonicWALL Analyzer 7.1 Administrator's Guide" (6 May 2013), "Dell SonicWALL Analyzer 7.1 Virtual Appliance Getting Started Guide" (6 May 2013), "Dell SonicWALL Analyzer 7.1 Software Getting Started Guide" (5 Mar 2013), "SonicWALL Analyzer 7.0 Administrator's Guide" (10 Sep 2012), and "SonicWALL Analyzer Virtual Appliance 7.0 Getting Started Guide" (21 Feb 2012). The "Technical Notes" section shows 1 of 1 note: "SonicWALL GMS 7.0 ConnectWise Integration Technote" (31 May 2012).

**Support**

Overview

Product Documentation

Network Security

SSL VPN Secure Remote Access

Email Security Appliances and Software

Management & Reporting

Global Management System

UMA Series

Scrutinizer

**Analyzer**

ViewPoint Software

Content Security Management

Client Software

Legacy Products

Self-Help Resources

Support Services

Professional Services

Guidelines & Policies

Product Lifecycle

Contact Support

Report a Vulnerability

Training / Certification

**Product Support**

**Analyzer**

Like Share Tweet

**Support Documents** Knowledge Base

**List View Options**

Adjust the filters below to focus the resource list on items of the most interest.

**Categories**

☐ Video Tutorials

☒ Product Guides

☒ Technical Notes

☒ Release Notes

☒ Support Data Sheets

**Product Guides**

5 of 5

Dell SonicWALL Analyzer 7.1 Administrator's Guide 6 May 2013

Dell SonicWALL Analyzer 7.1 Virtual Appliance Getting Started Guide 6 May 2013

Dell SonicWALL Analyzer 7.1 Software Getting Started Guide 5 Mar 2013

SonicWALL Analyzer 7.0 Administrator's Guide 10 Sep 2012

SonicWALL Analyzer Virtual Appliance 7.0 Getting Started Guide 21 Feb 2012

5 of 5

**Technical Notes**

1 of 1

SonicWALL GMS 7.0 ConnectWise Integration Technote 31 May 2012

1 of 1

# Live Product Demos

Get the most out of your Analyzer with the complete line of Dell SonicWALL products. The Dell SonicWALL Live Demo Site provides free test drives of Dell SonicWALL security products and services through interactive live product installations:

- UTM/Firewall/VPN
- Continuous Data Protection
- SSL VPN Secure Remote Access
- Content Filtering
- Email Security
- GMS and Analyzer

For further information, visit:

<http://livedemo.sonicwall.com/>

