

# Dell™ Secure Mobile Access 11.2

Central Management Server (CMS)  
Administration Guide



**© 2015 Dell Inc.  
ALL RIGHTS RESERVED.**

This guide contains proprietary information protected by copyright. The software described in this guide is furnished under a software license or nondisclosure agreement. This software may be used or copied only in accordance with the terms of the applicable agreement. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of Dell Inc.

The information in this document is provided in connection with Dell products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of Dell products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, DELL ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL DELL BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF DELL HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Dell makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. Dell does not make any commitment to update the information contained in this document.

If you have any questions regarding your potential use of this material, contact:

Dell Inc.  
Attn: LEGAL Dept  
5 Polaris Way  
Aliso Viejo, CA 92656

Refer to our website ([software.dell.com](http://software.dell.com)) for regional and international office information.

**Patents**

For more information, go to <http://software.dell.com/legal/patents.aspx>.

**Trademarks**

Dell, the Dell logo, and are trademarks of Dell Inc. Other trademarks and trade names may be used in this document to refer to either the entities claiming the marks and names or their products. Dell disclaims any proprietary interest in the marks and names of others.

**Legend**

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

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

 **IMPORTANT NOTE, NOTE, TIP, MOBILE, or VIDEO:** An information icon indicates supporting information.

Dell SMA 11.2 Central Management Server (CMS)  
Updated - May 2015  
Software Version - Release 11.2  
232-002859-00 Rev B

# Contents

## Part 1. Introduction

<b>Overview</b> .....	6
The Central Management Server .....	7
CMS Access to Other Services .....	8
The Central Management Console .....	8
Managed Appliances .....	8
GMS and CMS .....	8
HA, FIPS, and CMS .....	9
Pooled Licenses .....	9
Getting Started in Four Steps .....	9
Contents of this Guide .....	9
Guide Conventions .....	10

## Part 2. Installation and Configuration

<b>Installing/Configuring the Central Management Server (CMS)</b> .....	12
Overview .....	12
Supported Platforms for CMS .....	12
Hardware Resource Requirements .....	13
Installation Files .....	13
Setting up a CMS .....	14
<b>Configuring Appliances for Central Management</b> .....	21
Overview .....	21
Firmware Compatibility with the CMS .....	21
Enabling Central Management and Registering an SMA Appliance with the CMS .....	22
Previously Configured Appliances .....	23

## Part 3. Dashboard and Menus

<b>Using the CMC Dashboard</b> .....	25
Overview .....	25
Viewing the CMS Dashboard .....	25
Using the Alerts Pane .....	26
Using the Appliance Pane .....	27
Using the Geographic View .....	28
Using the Current Users Pane .....	29
Using the License Usage Pane .....	29
Using the About Pane .....	30
<b>Using the CMC Menus</b> .....	31
Using the Management Server Menus .....	31

Using the Dashboard . . . . .	32
Using Alerts . . . . .	32
Configuring the CMS . . . . .	37
Monitoring the CMS . . . . .	46
Maintaining the CMS . . . . .	47
Using the Managed Appliances Menu . . . . .	48
Defining a Collection of Managed Appliances . . . . .	49
Configuring a Managed Appliance . . . . .	50
Monitoring a Managed Appliance . . . . .	53
Maintaining a Managed Appliance . . . . .	55

## Part 4. Licensing and Alerts

Pooled Licensing . . . . .	57
Overview . . . . .	57
How CMS Pooled Licenses Work . . . . .	57
Types of Licenses . . . . .	59
Alerts and SNMP . . . . .	60
Overview . . . . .	60
Pre-Configured Alerts . . . . .	61
Configuring SNMP . . . . .	63
About Dell . . . . .	64
Contacting Dell . . . . .	64
Technical Support Resources . . . . .	64

# Part 1

## Introduction

- [Overview](#)

# Overview

This section contains an introduction to the Central Management Server (CMS) and important concepts associated with it. The section contains the following:

- [The Central Management Server](#) on page 7
- [The Central Management Console](#) on page 8
- [Managed Appliances](#) on page 8
- [GMS and CMS](#) on page 8
- [HA, FIPS, and CMS](#) on page 9
- [Pooled Licenses](#) on page 9
- [Getting Started in Four Steps](#) on page 9
- [Contents of this Guide](#) on page 9
- [Guide Conventions](#) on page 10

Central Management is an add-on product for managing multiple Dell Secure Mobile Access (SMA) VPN appliances. It gives companies with multiple appliances a single administrative user interface from where they can manage all their VPN appliances. The Central Management Server (CMS) is a virtual machine used to interact with all their managed VPN appliances. The CMS reduces the total cost of operation and simplifies the management of multiple VPN appliances for enterprise companies.

The VPN Administrator uses the Central Management Console (CMC) of the CMS to manage all the VPN appliances regardless of location in the world. There is close integration between the CMS and the managed appliances through a secure tunnel with native communications.

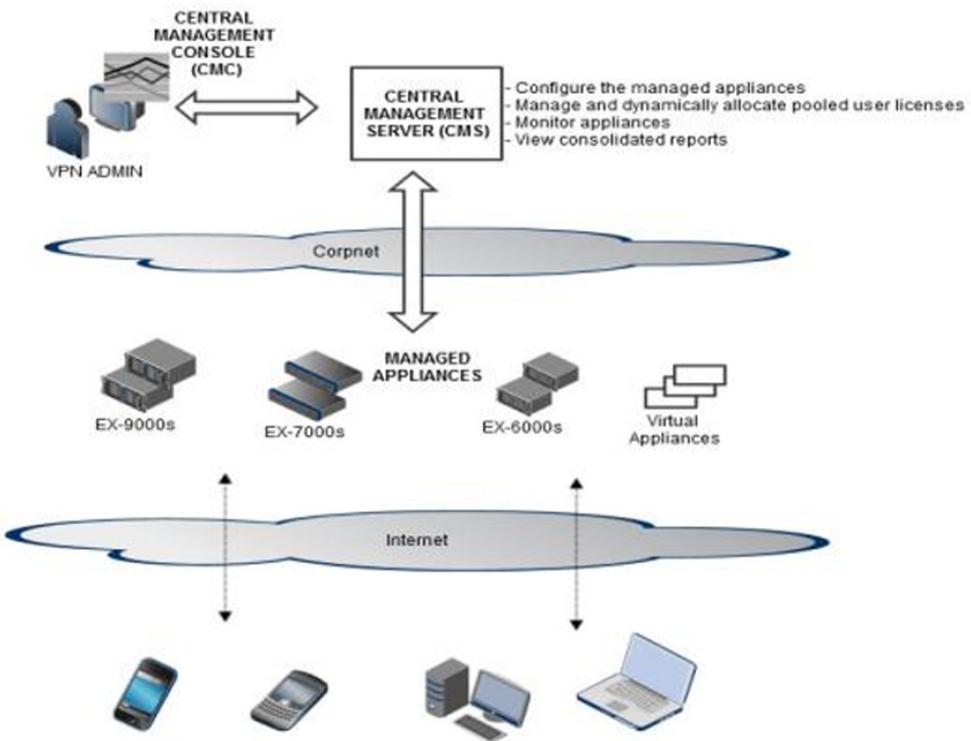
## Central Management:

- Provides enterprise customers a single plane of glass (the Dashboard) to manage their distributed VPN infrastructure.
- Reduces Total Cost of Operation (TCO) and operator errors associated with the management of multiple appliances.
- Provides a Central Management Console (CMC) to configure, maintain and monitor appliances.
- Simplifies license management with a centralized license that eliminates the need for separate appliance licenses.
- Optimizes license usage, that is, licenses are dynamically allocated to appliances based on user load.
- Facilitates centralized alerts via the console dashboard and SNMP traps.
- Requires no dedicated appliance or hardware (The Central Management Server is a virtual machine.)

This dashboard view in the CMC gives the Administrator a summarized view of all managed appliances.

Administrators can apply a common configuration to managed appliances from the CMC. Consolidated monitoring and reporting gives the Administrator an overview of all the appliances that are being managed.

An administrator can click on a single appliance in the CMS to launch the Appliance Management Console (AMC) for that appliance because of a single-sign on system.



## The Central Management Server

The Central Management Server (CMS) is only available as a virtual machine and supports the following VM host environments:

- VMWare ESXi 4.0 Update 1 (Build 208167) and newer
- VMWare ESX 4.0 Update 1 (Build 208167) and newer
- VMWare ESXi 5.0 (and newer)
- Windows Server 2012 R2 Hyper-V (and newer)

A CMS can manage up to 100 appliances (physical and virtual appliances), but before an appliance can be managed it must be registered with CMS.

The CMS communicates with each managed appliance over a secure SSL tunnel to receive:

- Data on the Control channel for configuring, licensing, maintaining appliances.
- Periodic health and status information from managed appliances.

The CMS also becomes an NTP server for managed appliances.

The CMS periodically communicates with MySonicWall for license validation. This ensures correct system wide timing and use of licenses.

## CMS Access to Other Services

The CMS requires access to the following two online services:

### SonicWall Licensing Server:

FQDN: software.sonicwall.com

IP: 204.212.170.115

217.149.45.76

ports 80, 443

### SonicWall Geo Server:

FQDN: geows.global.sonicwall.com

IP: 208.17.117.116

Ports: 80, 443

## The Central Management Console

The Central Management Console (CMC) provides the user with a single screen (called the Dashboard) to show Active alerts, Appliance status, License status, and Geographic View of all appliances on a map of the world. The Dashboard also allows you, from a single point to:

- Configure appliances (using push configuration settings).
- Maintain appliances, that is, Upgrade/hotfix, EPC update, and Restart.
- Use a one-click (single sign-on) to the AMC of managed appliance.
- View health history and reports for all appliances.
- Configure alerts, manage alert notifications for appliances or CMS.
- Configure user licenses and spike licenses (Start/Pause) on managed appliances.

## Managed Appliances

Managed appliances are SMA appliances that are registered with the CMS so that they can be centrally managed.

Each managed appliance must be an SMA Version 11.2 (or later) VPN appliance, but can be any combination of physical or virtual appliances, such as EX6000, EX7000, EX9000, SMA 6200, SMA 7200, and SMA-Virtual appliances.

Each appliance, when configured to do so, accepts configurations pushed from the CMS. Each appliance also accepts dynamically allocated leased licenses from the CMS (based on the number of user connections).

Managed appliances maintain a secure communication channel with the CMS to accept configuration and maintenance commands, and send health and status information.

## GMS and CMS

In the 11.2.0 release, SMA appliances can be managed by either the Dell Global Management System (GMS) or by the Dell Central Management Server (CMS), but not by both. Once an appliance registers with CMS, all GMS related functions are not available. CMS does not interact with GMS. SMA support for GMS is being deprecated. After the 11.2.0 release, GMS will no longer be supported.

# HA, FIPS, and CMS

CMS does not run in High Availability (HA) Cluster mode.

- You cannot use CMS to manage HA pairs.

CMS is not FIPS compliant.

- You cannot use CMS to manage a FIPS appliance.
- A FIPS appliance cannot be configured to be centrally managed.
- A FIPS appliance configuration cannot be imported into the CMS.

## Pooled Licenses

CMS supports a new pooled licensing model that allows user licenses to be centralized on the CMS and distributed and reallocated dynamically among the managed appliances, based on demand. User licenses no longer have to be applied to individual VPN appliances. Companies with appliances that are globally distributed can benefit from the fluctuating demands for user licenses due to time differences. The CMS reallocates licenses to managed appliances where user demands have peaked from appliances where usage has fallen due to off-work/night hours. Companies with appliances that are behind load balancers can also benefit from the dynamic distribution of licenses across managed appliances since the load balancer distributes connection requests across the managed appliances. For more information, refer to [Pooled Licensing](#) on page 57.

## Getting Started in Four Steps

- 1 Install and configure the CMS and apply the CMS license.  
Refer to [Installing/Configuring the Central Management Server \(CMS\)](#) on page 12.
- 2 Setup the VPN appliances to be managed.  
Refer to [Configuring Appliances for Central Management](#) on page 21.
- 3 Define the collection of managed appliances.  
Refer to [Defining a Collection of Managed Appliances](#) on page 49.
- 4 Monitor and manage appliances from the CMC Dashboard.  
Refer to [Using the CMC Dashboard](#) on page 25.

## Contents of this Guide

This *CMS System Administrator Guide* contains installation procedures and configuration guidelines for deploying Dell's Central Management Server (CMS) for Secure Mobile Access (SMA) appliances and additional descriptive information in the following sections:

- **Section 1 Introduction:** This section describes the concept of Central Management, Managed Appliances and Pooled Licenses.
- **Section 2 Installing/Configuring the Central Management Server:** This section includes procedures for setting up and installing the CMS, setting up VPN appliances to be managed, defining the collection of managed appliances, and monitoring appliances from the CMS Dashboard.
- **Section 3. Configuring Appliances for Central Management:** This section includes information about configuring appliances for central management.
- **Section 4. Using The CMC Dashboard:** This section includes definitions of the major panes and views of the Dashboard, that is, Alerts pane, Appliances pane, Table view and Geographic view, Current users pane, Per Appliance view and Pie Chart view, License usage view, About window.

- **Section 5. Using the CMS Menus:** This section explains the choices available with the CMS menus for operating and controlling the CMS and Managed Appliances. This includes information about Alerts, Configuration, Monitoring, and Maintenance.
- **Section 6. Pooled Licensing:** This section includes information about the following: Pooled licensing concepts, a CMS License, a CMS Spike license, a Leased license.
- **Section 7. Alerts and SNMP:** This section contains information about how the CMS provides a new SNMP MIB that queries the CMS and managed appliances to get health and metrics data associated with the CMS as well as generating SNMP traps for critical alerts.
- **About Dell:** Information about contacting Dell technical support.

## Guide Conventions

The following conventions are used in this guide.

**Table 1. Guide Conventions**

Convention	Use
Bold Text	Highlights field, button, and tab names. Also highlights window, dialog box, and screen names. Also used for file names and text or values you are being instructed to type into the interface.
Italic Text	Indicates the name of a technical manual, emphasis on certain words in a sentence, or the first instance of a significant term or concept.
Menu Item > Menu Item	Indicates a multiple step Management Interface menu choice. For example, <b>System &gt; Status</b> means select the <b>Status</b> page under the <b>System</b> menu.

## Part 2

# Installation and Configuration

- [Installing/Configuring the Central Management Server \(CMS\)](#)
- [Configuring Appliances for Central Management](#)

# Installing/Configuring the Central Management Server (CMS)

This section contains the following sections:

- [Overview on page 12](#)
- [Supported Platforms for CMS on page 12](#)
- [Hardware Resource Requirements on page 13](#)
- [Installation Files on page 13](#)
- [Setting up a CMS on page 14](#)

## Overview

A CMS is located inside a corporation's intranet. CMS requires a new type of license called a CMS License that is issued by Dell.

The CMS runs as a virtual machine that can be hosted on VMware ESX/ESXi or Microsoft Hyper-V. CMS is not designed to run on custom hardware such as VPN appliances.

Core CMS provides the following features:

- Central Management Console (CMC) to monitor, maintain, and configure Dell SMA appliances.
- Simplified license management with a centralized license that eliminates the need for individual appliance licenses.
- Centralized alerts via the console dashboard and SNMP traps.

## Supported Platforms for CMS

CMS runs as a virtual machine on the following hypervisor platforms:

**Table 1. Supported Platforms**

VMWare	Microsoft
ESXi 5 and newer	Windows Server 2012 R2 Hyper-V and newer
ESXi 4.0 Update 1 (Build 208167) and newer	
ESX 4.0 Update 1 (Build 208167) and newer	

# Hardware Resource Requirements

The virtual instance of CMS requires the following hardware resources:

- 2 GB RAM
- 2 CPU
- 64 GB HDD

If you are managing more than 50 appliances, the virtual instance of CMS requires the following hardware resources:

- 4 GB RAM
- 2 CPU
- 100 GB HDD

## Installation Files

Central Management is supported on Version 11.2 and later of Dell's Secure Mobile Access (SMA) firmware.

- To install on VMware hypervisors, the Open Virtual Appliance (.OVA) file with the following file name format is available for import and deployment to your ESX/ESXi server: ex\_sra\_vm\_11.2.x-xxx.ova
- To install in a Microsoft Hyper-V environment, use an International Organization for Standardization (.ISO) file such as: 11.2.0-xxx.iso.

The 11.2.x indicates the release version and x's represent a build number.

 **NOTE:** The same firmware is used for both the CMS and the SMA-Virtual appliance. The Central Management feature is enabled during the setup process.

For information on installing SMA-Virtual appliances, refer to the *Dell SMA-Virtual Getting Started Guide*.

# Setting up a CMS

**To setup a Centrally Managed VPN infrastructure:**

- 1 Setup a virtual instance (ESX or Hyper-V) of the release firmware.
- 2 Start the virtual machine and wait for a login prompt to appear.
- 3 Login as "root" (no password is required). A display similar to the following appears.

```
Hint: Num Lock on
DellSMAAppliance-00155d0ae445 login: root
=====
* Dell SMA Setup
* (c) 2014, Dell, Inc.
*
=====
Welcome to Dell Secure Mobile Access!

The following prompts will guide you through the initial setup of the
Dell SMA appliance. The network information you provide here will
enable you to connect to the Administration & Management Console (AMC)
and continue configuring the appliance.

When you're prompted with a question, press "y" for Yes or "n" for No.
To quit, press "q" at any prompt.

[Press any key to proceed]
```

- 4 Press any key.

```
INTERNAL INTERFACE CONFIGURATION

Please enter network settings for the internal interface (labeled
"2" on the appliance). If you are on the same network as the appliance,
press ENTER when prompted for a gateway.

IP address: 192.168.0.20
Subnet mask: 255.255.255.0
Gateway: 192.168.0.1

CLUSTERING CONFIGURATION

This appliance can be configured standalone or as a node in a cluster.
If this appliance is to be installed in a cluster, it must be given
the active or standby role.

Install node in a cluster? (n)

Please review the information you provided. Press ENTER to accept the
current value, otherwise enter a new value.

IP address [192.168.0.20]:
```

- 5 Configure the internal interface settings and save the configuration settings.

- 6 Continue until instructed to access the console from a browser at <https://<Internal-IP-Address>:8443>.  
The following screen appears.

Welcome

License Agreement

Basic Settings

Network Settings

Routing

Name Resolution

User Access

Completion

## Welcome to Dell Secure Mobile Access

This Setup Wizard guides you through a series of required and optional settings for getting the appliance up and running quickly:

**Basic Settings:** Set the password you'll use to administer the appliance, and the date and time.

**Network Settings:** Set the name of the appliance, which is used in log files, and the IP address and subnet mask for the internal and external network interfaces.

**Routing:** Configure the gateways for internal and external network traffic.

**Name Resolution:** Configure the domain name of the network to which the appliance will be connected and the internal DNS.

**User Access:** Create a basic security policy. You can change it later in the Appliance Management Console (AMC).

After you complete the Setup Wizard:

- You will be redirected to AMC. To log in, type "admin" in the Username box, and enter the administrator password that you set on the Basic Settings page.
- Register your appliance on MySonicWALL ([www.mysonicwall.com](http://www.mysonicwall.com)). Registration gives you access to essential resources, such as your license file and updates. In order to register, you need both the serial number for your appliance, and its authentication code, which is visible on the General Settings page in AMC.

 Secure Mobile Access

< Back Next > Cancel

- 7 Read and if appropriate, accept the EULA and click **Next**. The **Basic Settings** page appears.

**Welcome**

**License Agreement**

**Basic Settings** (selected)

**Network Settings**

**Routing**

**Name Resolution**

**User Access**

**Completion**

## Basic Settings

### Central Management

This appliance can manage the licensing and configuration of up to 100 appliances.

Install this appliance as the central management server for a pool of appliances

### Cluster settings

This appliance can be installed as a standalone appliance, or in a high-availability cluster. In a cluster this appliance can be either the active (node 1) or standby (node 2) node.

Install this appliance as a node in a cluster

This appliance will be the active node (node 1) The active node is responsible for configuring and managing the cluster.

This appliance will be the standby node (node 2)

### Administrator password

Specify the password you will use to access the Appliance Management Console (AMC). Your password must be at least eight characters long.

Enter password: \*

Confirm password: \*

### Date and time

Please select a time zone below. To set the current time, click **Change**. If you wish to synchronize the time with an NTP server, it can be configured later in AMC.

Time zone:

Current time: Tue Apr 7 2015 14:38:23 GMT [Change](#)

Secure Mobile Access

< Back **Next >** Cancel

- 8 Configure the virtual computer as a Central Management Server using the check-box circled in red above.
- 9 Configure the Shared Secret and Locale.

**Welcome**

**License Agreement**

**Basic Settings**

**Network Settings**

**Routing**

**Name Resolution**

**Central Management** (selected)

**Completion**

## Central Management

This server manages the licensing and configuration for a collection of appliances.

### Shared secret

Every appliance in the pool must be configured with this shared secret. The secret is set on each appliance's Central Management page under Maintenance.

Shared secret: \*  Must be at least 8 characters long.

Confirm secret: \*

### Locale

Country:

Location:   
Example: Seattle, WA

### Policy Synchronization

Enable pushing policy configuration from this server to managed appliances.

Secure Mobile Access

< Back **Next >** Cancel

- 10 Make additional configuration selections, as required.
- 11 Upon successful completion, click **Next**. The **Completion** page appears.

The screenshot shows the 'Completion' page of the Dell SMA Setup Wizard. On the left, a vertical navigation bar lists steps: Welcome, License Agreement, Basic Settings, Network Settings, Routing, Name Resolution, Central Management, and Completion, with 'Completion' highlighted. The main area has a title 'Completion' and a message: 'You have successfully completed the Setup Wizard. To apply your settings, click **Finish**. After your settings have been applied, you will be directed to AMC where you can log in using the password you supplied earlier.' Below this is a section titled 'Appliance Settings' containing a table of configuration details:

Date and time:	Tue Apr 7 2015 14:58:41 GMT
Central management server:	Yes
Clustered:	No
Appliance name:	CMS-192-168-0-10
Internal interface:	192.168.0.10 / 255.255.255.0
External interface:	Disabled
Routing:	Default gateway (192.168.0.1)
Default domain:	hypervbox.com
DNS server:	8.8.8.8
Full network access:	OnDemand Tunnel disabled
Access policy:	Unknown

At the bottom right are buttons: '< Back', 'Finish' (highlighted with a dotted border), and 'Cancel'.

- 12 Click **Finish**. The configuration changes are applied and a **Logon** screen appears.

The screenshot shows the 'Please log in' screen of the Dell SMA Central Management Console. It features the Dell logo and the text 'Secure Mobile Access | Central Management Console'. The login form includes fields for 'Username' (empty), 'Password' (empty), and 'Log in using' (set to 'Management Console'). Below the form are 'Login' and 'Clear' buttons.

- 13 Login with username "admin" and the password that you just configured. The **Central Management Console (CMC) Dashboard** Page appears.

The screenshot shows the CMS-110 Dashboard. On the left, a sidebar lists 'Management Server' (Dashboard, Alerts, Configure, Monitor, Maintain) and 'Managed Appliances' (Define collection, Configure, Monitor, Maintain). The main area has a title 'CMS-110 Dashboard'. It features three main sections: 'Alerts' (with two critical alerts: 'CMS-110: High user license usage 99%' and 'Seattle-111: Critically high appliance license usage 98%'), a table of managed appliances (Seattle-111, Shanghai-113, Bangalore-112), and three gauge charts for 'Current users' (Seattle-111 at 4.9k, Shanghai-113 at 3.8k, Bangalore-112 at 2.2k) and a 'License usage' chart (Peak Usage 02/06/15, 9.9k users). At the bottom right is an 'About' section with system details: Model: Dell SMA CMS, Hypervisor platform: Microsoft HyperV, Version: 11.2.0-192, Hotfixes: None, System time: Tue Apr 07 05:53:18 PDT 2015, Uptime: 66 days 20 hours 36 mins, License: 5 appliances, 10000 users.

- 14 Download a CMS license from [MySonicWall.com](http://MySonicWall.com)  
 15 On the menu selection **Management Server > Configure > Licensing** page, apply the downloaded CMS license to the CMS.

- 16 From the menu on the left side of the screen, select **Management Server > Configure**. The **Configure Server** page appears.

The screenshot shows the Dell Secure Mobile Access Central Management Console interface. The left sidebar contains navigation links for 'Management Server' (Dashboard, Alerts, Configure, Monitor, Maintain) and 'Managed Appliances' (Define collection, Configure, Monitor, Maintain). The main content area is titled 'Configure Server' and includes several configuration sections:

- Central Management Settings:** Change shared secret, managed address pool, enable/disable policy synchronization.
- Licensing:** Displays license holder (Dell Engineering), maximum users (5000), maximum appliances (100), appliance serial number (VirtualCMSMain11.2.0-182), and authentication code (VirtualCMSMain11.2.0-182).
- General options:** Client security (720 minutes credential lifetime), Date and time (Current time: Tue Jan 27 2015 12:29:20 PST, Time zone: GMT-08:00 Pacific Standard Time (US/Pacific)).
- Administration:** Define administrators and authentication servers for managing the central management server.
- Network Settings:** Modify server IP address, routing, and name resolution.
- Network Services:** Modify settings for server services NTP, SSH, SNMP, and SMTP.
- SSL Settings:** Modify the management console certificate and SSL settings.

17 Click Central Management Settings. The Central Management Settings page appears.

The screenshot shows the Dell Secure Mobile Access Central Management Console. The left sidebar has sections for Management Server (Dashboard, Alerts, Configure, Monitor, Maintain) and Managed Appliances (Define collection, Configure, Monitor, Maintain). The main content area is titled 'Central Management Settings' under 'Configure Server > CMS Settings'. It contains the following fields:

- Shared secret**: A field where 'Shared secret:' is followed by a masked input field containing '\*\*\*\*\*' and a note: 'The shared secret must be at least 8 characters long.'
- Address Pool**: A section for IP address allocation with fields for 'IP address range\*' (172.16.254.154-254) and 'Subnet mask' (255.255.255.0).
- Locale**: Fields for 'Country' (United States) and 'Location' (Seattle, WA), with a note: 'Geographic server can't be accessed now. You can only change central management server's location by dragging it on dashboard.'
- Policy Synchronization**: A checked checkbox for 'Enable pushing policy configuration from this server to managed appliances.' A note below says: 'By default, configuration data on the destination nodes will be overwritten. To preserve certain settings on the destination, specify exclusions here.'
- Authentication servers**: Radio buttons for 'Nodes in the collection share centralized authentication servers' (selected) and 'Each node has its own authentication server'. A note says: 'Overwrites the authentication server settings on the destination nodes.' Another note says: 'Retains authentication settings on the destination nodes, except in the case of a PKI server: trusted CA certificates cannot be retained.'

At the bottom are 'Save' and 'Cancel' buttons.

18 Configure your CMS from this page follows:

- Review the range of 100 IP addresses that will be used to communicate with managed appliances. In most cases the defaults work, so this is only necessary if the private address space that is filled in overlaps with existing addresses.

The administrator can configure the private address space (IP address pool) for the CMS tunnel so that it does not overlap or conflict with the IP addresses of resources in the private corporate network (such as host, IP range, or subnet).

**NOTE:** The CMC and the AMC do not check for private IP address range overlaps or conflicts.

19 Enable the **Policy Synchronization** option by clicking the check box. Use this option ONLY if you want to transfer settings from the CMS to the managed appliance and overwrite the appliance's current configuration settings. Use this option if your appliances have the same configuration settings, and you plan to manage the appliance configuration centrally. You can change this option later.

20 Select whether the managed appliances will use the same authentication servers, by selecting either the **Nodes in the collection share centralized authentication servers** option or the **Each node has its own authentication server** option.

21 Click Save.

# Configuring Appliances for Central Management

This section explains how to configure appliance for central management, that so they become managed appliances. The section contains the following topics:

- [Overview](#) on page 21
- [Firmware Compatibility with the CMS](#) on page 21
- [Enabling Central Management and Registering an SMA Appliance with the CMS](#) on page 22
- [Previously Configured Appliances](#) on page 23

## Overview

A CMS can manage up to 100 appliances. Managed Appliances can be any combination of physical and virtual appliances (for example, EX6000, EX7000, EX9000, SMA 6200, SMA 7200, and SMA-Virtual). High Availability (HA) pairs cannot be managed by CMS.

A Shared Secret is used to bootstrap a secure communication channel between the CMS and the appliance. Once a secure SSL tunnel is established, all subsequent communications between the appliances and CMS take place through the tunnel.

## Firmware Compatibility with the CMS

Managed Appliances must be running firmware that is compatible with CMS.

**Table 1. Firmware Compatibility**

Appliance Type	CMS Version 11.2
SRA Appliance Version 10.x	Not Supported
SMA Appliance Version 11.1	Not Supported
SMA Appliance Version 11.2	Supported

# Enabling Central Management and Registering an SMA Appliance with the CMS

Before an appliance can be registered with the CMS, it must first be enabled for Central Management. In addition, the CMS must have an unused appliance license (obtained from the CMS license) before an SMA Appliance can be registered. The administrator must enable Central Management and type the shared password into the console of the SMA appliance. In addition the administrator must register the appliance with the CMS.

The shared password is used to bootstrap the secure tunnel, and all subsequent communications go through the secure tunnel. The appliance uploads its information (model, version, serial#) to the CMS. The CMS pushes a Leased License to the appliance, and then (if configured), pushes the configuration settings to the appliance.

The managed appliance is now online and ready to accept VPN connections.

## **To enable central management:**

- 1 Access the AMC console of the appliance to be registered.
- 2 Select **System Configuration > Maintenance**.

Secure Mobile Access | Management Console

**Maintenance**   **Scheduler**

**Product:** SonicWALL SRA EX-Virtual  
**Version:** 11.2.0-074  
**Time since last reboot:** 5 Days 18 Hours 26 Minutes 59 Seconds  
**Number of current users:** 0  
**Last replication:** N/A

**Restart....** Restart the appliance.   **Shutdown....** Turn off the appliance.   **Reset....** Reset the system software.

**System configuration**

**Import or export** — Import configuration data from another system or from backup, or export the current configuration for replication or backup.   **Configure...**

**Replicate** — Push configuration data to other appliances, or configure this appliance to receive data.

**Central Management** — Include this appliance in a pool of appliances that is licensed and managed by a central management server.   **Configure...**

**System software updates**

**Update** — Install a system upgrade or hotfix on the appliance.   **Configure...**

**Rollback** — Restore a previous version of the system software or remove a hotfix.   **Rollback...**

- 3 Click **Configure** in the **Central Management** panel. The **Configure Central Management** page appears.

The screenshot shows the Dell Secure Mobile Access Management Console interface. On the left, there is a navigation sidebar with several categories: Security Administration, User Access, System Configuration, Monitoring, and Troubleshooting. Under Security Administration, 'Access Control', 'Resources', and 'Users & Groups' are listed. Under User Access, 'Realms', 'WorkPlace', 'Agent Configuration', and 'End Point Control' are listed. Under System Configuration, 'General Settings', 'Network Settings', 'SSL Settings', 'Authentication Servers', 'Services', 'Virtual Assist', and 'Maintenance' are listed. Under Monitoring, 'User Sessions', 'System Status', 'Logging', and 'Troubleshooting' are listed. The main content area is titled 'Configure Central Management' and has a sub-header 'Maintenance > Configure Central Management'. It contains a note: 'Include this appliance in a pool of appliances that is licensed and managed by a central management server.' Below this is a checkbox labeled 'Enable central management' which is checked. There are two input fields: 'Shared secret:' and 'Confirm shared secret:', both containing the value '\*\*\*\*\*'. A note next to the fields says 'The shared secret must be at least 8 characters long.' At the bottom of the form are 'Save' and 'Cancel' buttons.

- 4 Click **Enable central management**.
- 5 Click **Save** to apply pending changes.
- 6 Ensure that the appliance has a network connection.
- 7 Enter the Shared Secret that you entered on the CMC and then enter it again to confirm it.  
① | **NOTE:** The appliance must next be registered with the CMS.
- 8 Click **Save**.

## Previously Configured Appliances

Standalone appliances that were originally configured from their AMC can be registered with a CMS without affecting the appliance's policy settings.

For information on how to synchronize (or not) policy on an appliance from the CMS, refer to [Configuring a Managed Appliance](#) on page 50.

## Part 3

# Dashboard and Menus

- [Using the CMC Dashboard](#)
- [Using the CMC Menus](#)

# Using the CMC Dashboard

This section explains how to use the CMS Dashboard. It contains the following topics:

- [Overview](#) on page 25
- [Viewing the CMS Dashboard](#) on page 25
- [Using the Alerts Pane](#) on page 26
- [Using the Appliance Pane](#) on page 27
- [Using the Current Users Pane](#) on page 29
- [Using the License Usage Pane](#) on page 29
- [Using the About Pane](#) on page 30

## Overview

A VPN administrator uses the Central Management Console (CMC) of the CMS to manage all registered VPN appliances. The CMC gives Administrators a single screen from where they can configure and monitor all their managed appliances. The CMC provides the following capabilities:

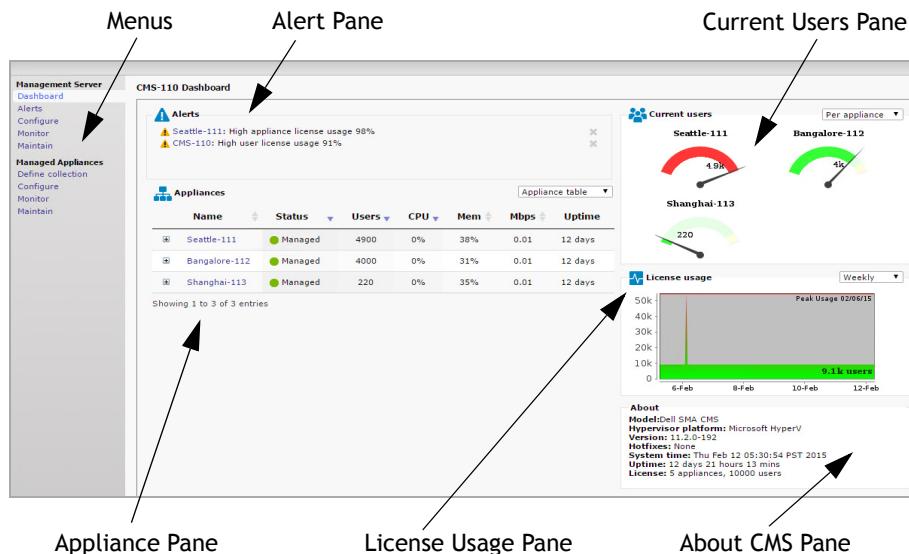
- A dashboard view of the VPN infrastructure.  
Refer to [Viewing the CMS Dashboard](#) on page 25.
- Enroll, maintain, configure and monitor managed appliances.  
Refer to [Using the Appliance Pane](#) on page 27.
- Monitor license usage and consolidated user sessions.  
Refer to [Monitoring a Managed Appliance](#) on page 53.
- Manage appliance configuration/policy settings.  
Refer to [Using the Appliance Pane](#) on page 27.
- Configure the CMS.  
Refer to [Configuring the CMS](#) on page 37.

## Viewing the CMS Dashboard

Use the dashboard to review system statistics and use the menus on the left to configure and maintain your system.

The **Dashboard** page is the first screen that appears after you log in. You can also access it anytime by clicking **Management Server > Dashboard** from the menus.

The Dashboard is divided into the sections illustrated and explained below.



This Dashboard contains the following areas:

- **Menu selections** - Click a selection under one of the two main categories:
  - **Management Server** - Contains the following selections: Dashboard, Alerts, Configure, Monitor, Maintain.
  - **Managed Appliances** - Contains the following selections: Define collection, Configure, Monitor, Maintain.
- **Alert Pane** - Contains a list of currently active alerts. Click an Alert to view information about alerts.
- **Appliance Pane** - Shows all online appliances. Select a managed appliance to view information about it. Appliances are sorted starting with the appliance with the most users.
- **Current Users Pane** - Displays the activity on current users
- **License Usage Pane** - Displays information about license usage.
- **About Pane** - Displays CMS Information consisting of Model, Hypervisor platform, Version, Hotfixes, System Time, Uptime, License.

Each pane is independently refreshed with updated information/status.

Dashboard panes use the following color codes: Green (OKAY), Yellow (WARNING), and Red (ERROR).

## Using the Alerts Pane

The Alerts Pane shows all currently active alerts that have not been acknowledged by the administrator. When specific alert thresholds are met, a Warning or an Error alert is shown on the CMC dashboard.



The Alerts pane gives an administrator a consolidated view of all Errors and Warnings across the VPN infrastructure. It contains Error and Warning messages (that is appliance offline, license consumption greater than 75%, and so on). Refer to [Pre-Configured Alerts](#) on page 61 for more information about alerts and their parameters. The Alerts pane consists of a table with the following columns:

- Colored icon representing the severity of the Alert
  - Red – Critical
  - Yellow – Warning
- Description of the Alert

An acknowledged alert will re-appear if the state changes. Error alerts are listed first, followed by Warnings. Alerts are sorted by time (most recent on top) within the categories. If there are no active alerts, a "No Alerts" message is displayed in the pane.

Alerts can be acknowledged by the Administrator by clicking on the X to the right of the alert. An acknowledged alert will no longer appear in the dashboard, but can be seen in the Alerts section.

An acknowledged alert will re-appear if the state changes (on to off to on). Alerts are automatically removed if the cause of the alert ceases, for example if an appliance that was Offline starts communicating with the CMS, the error alert is no longer valid and is removed from the Alert pane.

To view an individual alert, click on the Alert.

For more information about this area, refer to [Alerts and SNMP](#) on page 60.

To view and configure all alerts, select **Management Server > Alerts**. Refer to [Using Alerts](#) on page 32.

## Using the Appliance Pane

The Appliance Pane displays real-time, online, managed appliances with data in the following columns: Name, Status, Users, CPU usage, Memory usage, Mbps, Uptime. This gives a quick overview of the appliance managed.

On the top of the pane, on the right side is a drop down menu with the following selections:

- Appliance Table: This is the default view and is the one shown here.
- Geographic View: This shows the geographic location of each appliance on a separate display. Refer to [Geographic View](#)

Appliances								Appliance table ▾
Name	Status	Users	CPU	Mem	Mbps	Uptime		
Seattle-111	Managed	4900	0%	38%	0	12 days		
Bangalore-112	Managed	4000	0%	32%	0.01	12 days		
Shanghai-113	Managed	220	1%	35%	0.01	12 days		

Click the + at the beginning of each line to display the following information about the appliance: Host, Platform, Serial Number, Version, Hotfixes.

To directly start the AMC for an appliance (without entering credentials), click the name of the appliance.

# Using the Geographic View

This view of the appliances managed by the CMS, is accessed from the Geographic view drop-down menu on the title bar of the Appliances pane (shown here with an arrow).

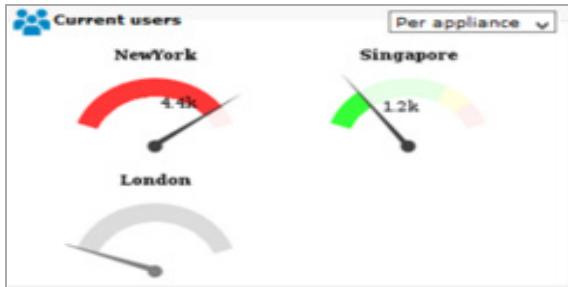
The screenshot shows the CMS-110 Dashboard. On the left, there's a sidebar with 'Management Server' and 'Managed Appliances' sections. The main area has a 'CMS-110 Dashboard' title. It includes an 'Alerts' section with two yellow warning icons: 'Seattle-111: High appliance license usage 98%' and 'CMS-110: High user license usage 91%'. Below that is an 'Appliances' section with a world map showing appliance locations. A red arrow points to a dropdown menu next to the map that says 'Geographic view ▾'. To the right of the map are three cards: 'Current users' (Seattle-111, Bangalore-112, Shanghai-113), 'License usage' (a weekly chart peaking at 9.1k users on 02/06/15), and an 'About' section with system details. The map itself has zoom controls (+ and -) and a copyright notice: 'Copyright: 2010 ESRI, AND, TANA, ES...'.

This selection changes the list of managed appliances into a geographic representation of the devices. An appliance is located on the map based on its city/country obtained during configuration. You can reposition the icon for an appliance on the map by dragging and dropping the icon. You may need to do this if the icon for an appliance is not correctly positioned on the map, or if multiple appliance icons are positioned too close to each other. You can drag the appliance to locate it in a different location on the map. Move your cursor across the colored icons on the map and information about that equipment appears:

- A blue icon represent the CMS Server and displays Host name and address.
- A green icon represents a selected managed appliance that is online and displays Host, Status, Users, CPU, Memory, Bandwidth.
- A red icon represents an appliance that is offline.
- Zoom (+) and UnZoom (-) buttons allow the map view to be changed. The last map viewed is saved.

# Using the Current Users Pane

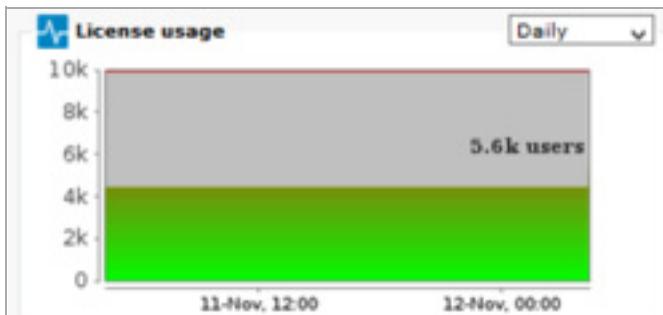
This pane displays the current distribution of all the connected users across the managed appliances. It also indicates how appliances are loaded relative to their maximum configured license settings.



- The drop-down menu at the top of this pane lets you choose to display the data in either of the following two ways:
  - Appliance dial gauge view
  - Pie chart view
- Red indicates that the managed appliance license usage is close to the maximum configured license setting for the appliance.
- Yellow is a warning.
- Green indicates okay.
- The number shows the number of users connected through the appliance.

# Using the License Usage Pane

This pane displays the history of CMS user license consumption relative to the maximum license capacity.

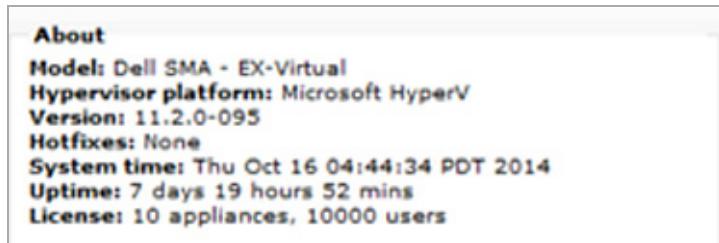


- A drop-down menu allows you to change the display to show usage Now, Hourly, Daily, Weekly, Monthly, Quarterly.
- The graph displays number of users as a function of time.
- The actual number of users (based on the number allowed by the number of licenses) is represented by the bar graph and indicated on the x axis of the graph.
- Colors: Green indicates that the CMS license usage is running within the pooled licensed capacity. If it gets to 75% (default warning alert setting for CMS license usage warning) it turns yellow. If it gets to 90% (default alert setting for CMS license usage) it turns red.

# Using the About Pane

This pane displays the following information about an individual Appliance highlighted from the list in the Appliance Pane:

- Model
- Hypervisor platform
- Version
- Hotfixes
- System time
- Uptime
- License



# Using the CMC Menus

A VPN Administrator uses the Central Management Console (CMC) of the CMS to manage all the VPN appliances. This section contains information about the menus of the CMC.

- [Using the Management Server Menus on page 31](#)
  - [Using the Dashboard on page 32](#)
  - [Using Alerts on page 32](#)
  - [Configuring the CMS on page 37](#)
  - [Monitoring the CMS on page 46](#)
  - [Maintaining the CMS on page 47](#)
- [Using the Managed Appliances Menu on page 48](#)
  - [Defining a Collection of Managed Appliances on page 49](#)
  - [Configuring a Managed Appliance on page 50](#)
  - [Monitoring a Managed Appliance on page 53](#)
  - [Maintaining a Managed Appliance on page 55](#)

## Using the Management Server Menus

This section provides the following information:

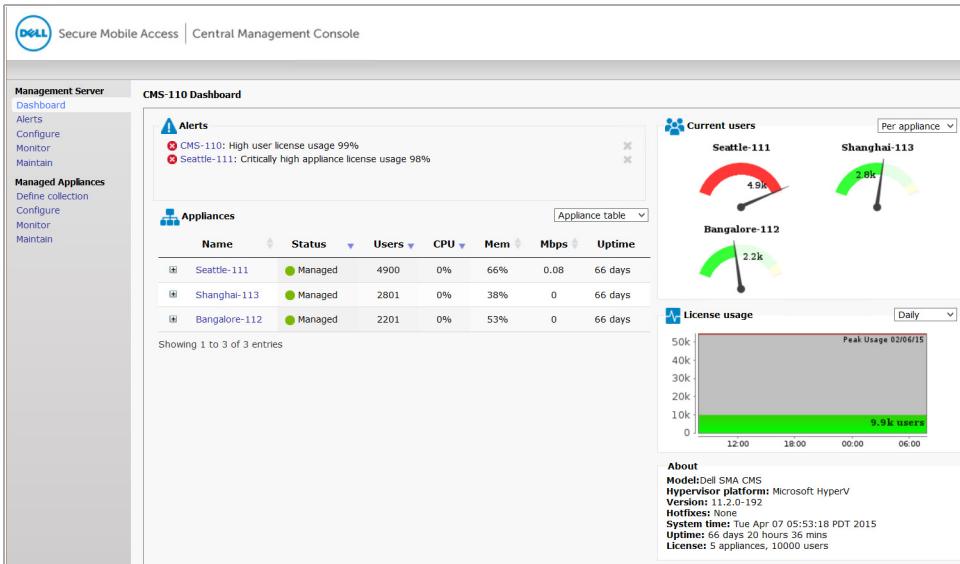
- [Using the Dashboard](#)
- [Using Alerts](#)
- [Configuring the CMS](#)
- [Monitoring the CMS](#)
- [Maintaining the CMS](#)

# Using the Dashboard

For detailed information about the dashboard, refer to [Viewing the CMS Dashboard](#) on page 25.

## To view the Dashboard:

- Select **Management Server > Dashboard**:  
The CMS Dashboard appears.

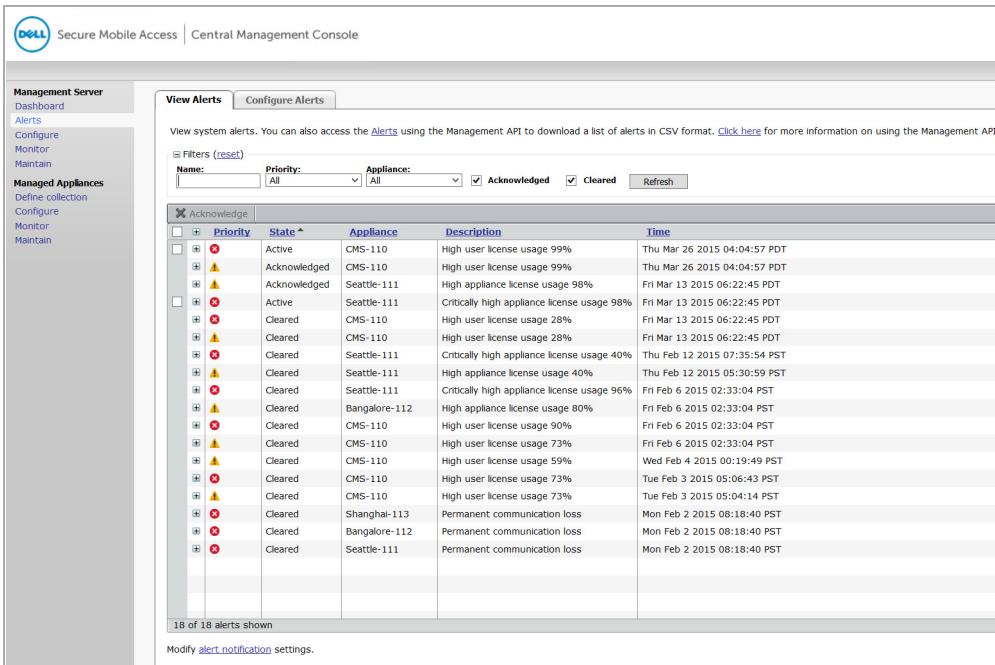


# Using Alerts

For detailed information about the type of Alerts, refer to [Alerts and SNMP](#) on page 60.

## To view and configure alerts:

- Select **Management Server > Alerts**. This page has two tabs: **View Alerts** and **Configure Alerts**.



## Viewing Alerts

The View Alerts tab provides a way to determine the type of information that you want to view:

- You can filter the alerts that are displayed by Name, Priority and Appliance.
- Alerts that were acknowledged from the dashboard can be viewed by checking the **Acknowledged alerts** checkbox.
- Alerts that cleared (by the alert condition going away) can be viewed by checking the **Cleared alerts** check box.

**Configuration Alert Notification**      [Configure Alerts > Configuration Alert Notification](#)

Configure settings for alert notification

Notify recipients of:

Critical alerts  
 Warning alerts  
 Acknowledged alerts  
 Cleared alerts

**Email settings**

Email messages will be sent for the above events.

From address:  Alert notifications use the [SMTP settings](#) to send email messages.

Send email to the following recipients:

<input type="checkbox"/>	Name	Address	Enabled
<input type="checkbox"/>			<input type="checkbox"/>
<input type="checkbox"/>			<input type="checkbox"/>
<input type="checkbox"/>			<input type="checkbox"/>

**Buttons:**

**To view alerts:**

- 1 Go to the **Management Server > Alerts** page.
- 2 Click the **View Alerts** tab.

	Priority	State	Appliance	Description	Time
<input type="checkbox"/>	<span style="color: red;">●</span>	Active	CMS-110	High user license usage 99%	Thu Mar 26 2015 04:04:57 PDT
<input type="checkbox"/>	<span style="color: yellow;">▲</span>	Acknowledged	CMS-110	High user license usage 99%	Thu Mar 26 2015 04:04:57 PDT
<input type="checkbox"/>	<span style="color: yellow;">▲</span>	Acknowledged	Seattle-111	High appliance license usage 98%	Fri Mar 13 2015 06:22:45 PDT
<input type="checkbox"/>	<span style="color: green;">●</span>	Active	Seattle-111	Critically high appliance license usage 98%	Fri Mar 13 2015 06:22:45 PDT
<input type="checkbox"/>	<span style="color: green;">●</span>	Cleared	CMS-110	High user license usage 28%	Fri Mar 13 2015 06:22:45 PDT
<input type="checkbox"/>	<span style="color: yellow;">▲</span>	Cleared	CMS-110	High user license usage 28%	Fri Mar 13 2015 06:22:45 PDT
<input type="checkbox"/>	<span style="color: green;">●</span>	Cleared	Seattle-111	Critically high appliance license usage 40%	Thu Feb 12 2015 07:35:54 PST
<input type="checkbox"/>	<span style="color: yellow;">▲</span>	Cleared	Seattle-111	High appliance license usage 40%	Thu Feb 12 2015 05:30:59 PST
<input type="checkbox"/>	<span style="color: green;">●</span>	Cleared	Seattle-111	Critically high appliance license usage 96%	Fri Feb 6 2015 02:33:04 PST
<input type="checkbox"/>	<span style="color: yellow;">▲</span>	Cleared	Bangalore-112	High appliance license usage 80%	Fri Feb 6 2015 02:33:04 PST
<input type="checkbox"/>	<span style="color: green;">●</span>	Cleared	CMS-110	High user license usage 90%	Fri Feb 6 2015 02:33:04 PST
<input type="checkbox"/>	<span style="color: yellow;">▲</span>	Cleared	CMS-110	High user license usage 73%	Fri Feb 6 2015 02:33:04 PST
<input type="checkbox"/>	<span style="color: yellow;">▲</span>	Cleared	CMS-110	High user license usage 59%	Wed Feb 4 2015 00:19:49 PST
<input type="checkbox"/>	<span style="color: green;">●</span>	Cleared	CMS-110	High user license usage 73%	Tue Feb 3 2015 05:06:43 PST
<input type="checkbox"/>	<span style="color: yellow;">▲</span>	Cleared	CMS-110	High user license usage 73%	Tue Feb 3 2015 05:04:14 PST
<input type="checkbox"/>	<span style="color: green;">●</span>	Cleared	Shanghai-113	Permanent communication loss	Mon Feb 2 2015 08:18:40 PST
<input type="checkbox"/>	<span style="color: green;">●</span>	Cleared	Bangalore-112	Permanent communication loss	Mon Feb 2 2015 08:18:40 PST
<input type="checkbox"/>	<span style="color: green;">●</span>	Cleared	Seattle-111	Permanent communication loss	Mon Feb 2 2015 08:18:40 PST

18 of 18 alerts shown  
Modify alert notification settings.

# Configuring Alerts

**To add an alert trigger:**

- 1 Go to the Configure Alerts tab
- 2 Click the green plus mark. The Add Alert Trigger dialog appears.

Pri	Name	Measurement	Condition
0	Unable to communicate with MySonicWALL	CMS connection to MySonicWALL	Connection is lost for 10080 minutes
0	Unable to communicate with MySonicWALL	CMS connection to MySonicWALL	Connection is lost for 4320 minutes
1	Temporary communication loss	Managed appliance connection to CMS	Connection is temporarily lost
0	Permanent communication loss	Managed appliance connection to CMS	Connection is permanently lost
0	High user license usage	CMS license usage	Value is over 95 percent
0	High user license usage	CMS license usage	Value is over 75 percent
0	High swap usage	Swap usage	Value is over 5 percent
0	High memory usage	Memory usage	Value is over 95 percent for 5 minutes
0	High disk usage	Disk usage	Value is over 95 percent
0	High CPU usage	CPU usage	Value is over 95 percent for 5 minutes
0	High appliance license usage	Appliance license usage	Value is over 89 percent
0	Critically high memory usage	Memory usage	Value is over 95 percent for 5 minutes
0	Critically high CPU usage	CPU usage	Value is over 95 percent for 5 minutes
0	Critically high appliance license usage	Appliance license usage	Value is over 98 percent
0	Certificate expired	Time until certificate expires	Value is under 0 days
0	Certificate about to expire	Time until certificate expires	Value is under 30 days

- 3 Fill in the required information and click Save.

**To configure alerts:**

- 1 Go to the Management Server > Alerts page.
- 2 Click the Configure Alerts tab.

Pri	Name	Measurement	Condition
0	Unable to communicate with MySonicWALL	CMS connection to MySonicWALL	Connection is lost for 10080 minutes
0	Unable to communicate with MySonicWALL	CMS connection to MySonicWALL	Connection is lost for 4320 minutes
1	Temporary communication loss	Managed appliance connection to CMS	Connection is temporarily lost
0	Permanent communication loss	Managed appliance connection to CMS	Connection is permanently lost
0	High user license usage	CMS license usage	Value is over 95 percent
0	High user license usage	CMS license usage	Value is over 75 percent
0	High swap usage	Swap usage	Value is over 5 percent
0	High memory usage	Memory usage	Value is over 95 percent for 5 minutes
0	High disk usage	Disk usage	Value is over 95 percent
0	High CPU usage	CPU usage	Value is over 95 percent for 5 minutes
0	High appliance license usage	Appliance license usage	Value is over 89 percent
0	Critically high memory usage	Memory usage	Value is over 95 percent for 5 minutes
0	Critically high CPU usage	CPU usage	Value is over 95 percent for 5 minutes
0	Critically high appliance license usage	Appliance license usage	Value is over 98 percent
0	Certificate expired	Time until certificate expires	Value is under 0 days
0	Certificate about to expire	Time until certificate expires	Value is under 30 days

The **Configure Alerts** tab provides a way to configure the type of information that you want:

- Click the +/- to the left of Filters. This displays/hides a field for Name, Measurement, Priority (a drop-down for All, Warning, Critical, Appliance (All, Enable, Disabled)).
- Use the check box on the left-hand side to select an Alarm.
- Information is displayed in the following columns: Priority, Measurement, Condition. Use the check box to Check all items and the +/- box to Expand all items.

**To modify Alert notification settings:**

- 1 Click alert notification and the bottom of the page. The **Configure Alert Notification** appears.

The screenshot shows the Dell Secure Mobile Access Central Management Console interface. On the left, there is a navigation sidebar with sections for Management Server (Dashboard, Alerts, Configure, Monitor, Maintain) and Managed Appliances (Define collection, Configure, Monitor, Maintain). The main content area is titled "Configuration Alert Notification" and includes a sub-header "Configure Alerts > Configuration Alert Notification". The page contains several configuration fields:

- "Notify recipients of:"
  - Critical alerts
  - Warning alerts
  - Acknowledged alerts
  - Cleared alerts
- "Email settings":
  - Email messages will be sent for the above events.
  - "From address": A text input field with the placeholder "Alert notifications use the [SMTP settings](#) to send email messages."
- "Send email to the following recipients": A grid-based table for managing recipient addresses.

<input type="checkbox"/>	Name	Address	Enabled
<input type="checkbox"/>			

- 2 Fill in the required information and click **Save**.

# Configuring the CMS

**To configure the CMS:**

- Select Managed Server > Configure.

This page provides the following information and activities as shown below:

- [Central Management Settings Page](#)
- [Licensing Pages](#)
- [General Options Page](#)
- [Administration Page](#)
- [Network Settings Page](#)
- [Network Services Page](#)
- [SSL Settings Page](#)

The screenshot shows the Dell Secure Mobile Access Central Management Console. The left sidebar has a grey background with navigation links: Management Server (Dashboard, Alerts, **Configure**, Monitor, Maintain), Managed Appliances (Define collection, Configure, Monitor, Maintain), and a search bar. The main content area has a white background with a title 'Configure Server' and a sub-section 'Central Management Settings' with a gear icon. It says 'Change shared secret, managed address pool, enable/disable policy synchronization'. Below it is a 'Licensing' section with a lock icon, showing details: License holder: Dell Engineering, Maximum users: 5000, Maximum appliances: 300, Appliance serial number: CMSSeattleVM01, Authentication code: CMSSeattleVM01. Further down are sections for 'General options' (Client security: 720 minutes credential lifetime, Date and time: Current time: Thu Jan 22 2015 15:04:51 PST, Time zone: GMT-08:00 Pacific Standard Time (US/Pacific)), 'Administration' (Define administrators and authentication servers for managing the central management server), 'Network Settings' (Modify server IP address, routing, and name resolution), 'Network Services' (Modify settings for server services NTP, SSH, SNMP, and SMTP), and 'SSL Settings' (Modify the management console certificate and SSL settings).

# Central Management Settings Page

**To access the Central Management Settings page:**

- 1 Select Management Server > Configure > Central Management Settings.  
The Central Management Settings page appears.

The screenshot shows the Dell Secure Mobile Access Central Management Console. The left sidebar has two main sections: 'Management Server' (Dashboard, Alerts, Configure, Monitor, Maintain) and 'Managed Appliances' (Define collection, Configure, Monitor, Maintain). The main content area is titled 'Central Management Settings' with a sub-link 'Configure Server > CMS Settings'. It contains several configuration sections: 'Shared secret' (a field with masked input and a note about length), 'Address Pool' (IP address range 172.16.254.154-254 and subnet mask 255.255.255.0), 'Locale' (Country: United States, Location: Seattle, WA), 'Policy Synchronization' (checkbox checked for enabling policy pushing), and 'Authentication servers' (radio button selected for 'Nodes in the collection share centralized authentication servers'). At the bottom are 'Save' and 'Cancel' buttons.

- 2 Make the desired changes.
- 3 Click **Save**.

# Licensing Pages

**To manage your licenses for CMS:**

- 1 Go to the Management Server > Configure > Licensing page.  
The Manage Licenses page appears.

The screenshot shows the Dell SMA Central Management Console interface. The top navigation bar includes the Dell logo, 'Secure Mobile Access', and 'Central Management Console'. On the left, a sidebar menu lists 'Management Server' (Dashboard, Alerts, Configure, Monitor, Maintain) and 'Managed Appliances' (Define collection, Configure, Monitor, Maintain). The main content area is titled 'Manage Licenses' (with a 'License Distribution' tab). It displays software license information for an appliance, including the product (SonicWALL SRA EX-Virtual), license holder (Dell Engineering), maximum concurrent users (5000), maximum appliances (100), appliance serial number (VirtualCMSMain11.2.0-182), and authentication code (VirtualCMSMain11.2.0-182). Below this is a table of components and their license types:

Component	License Type
Advanced End Point Control	Evaluation - expires Sat Jan 23 2016
Connect Tunnel	Evaluation - expires Sat Jan 23 2016
Graphical terminal agents	Evaluation - expires Sat Jan 23 2016
Cache Cleaner	Evaluation - expires Sat Jan 23 2016
FIPS	Evaluation - expires Sat Jan 23 2016
Virtual Assist 5000 technicians	Evaluation - expires Sat Jan 23 2016
Central Management	Evaluation - expires Sat Jan 23 2016
Base license	Evaluation - expires Sat Jan 23 2016

At the bottom of the page are 'Import License...' and 'Cancel' buttons.

- 2 Select the desired License(s).
- 3 Click Import Licence....

4 Click the License Distribution tab.

This page allows you to set the minimum and maximum number of leased licenses that should be distributed to each managed appliance. The default settings for Max Licenses are based on the appliance model.

The screenshot shows the Dell SMA Central Management Console interface. On the left, there's a sidebar with 'Management Server' and 'Managed Appliances' sections. The main area has tabs for 'Manage Licenses' and 'License Distribution'. A warning message says: 'Modifying these settings is not recommended. Licenses are automatically distributed to appliances as needed.' Below it, a note states: 'Licenses are distributed to managed appliances as needed, requiring no attention from the administrator. However, the minimum and maximum license distributions can be set for each appliance if desired.' A table lists two appliances: KADUBU and Seafood.eng.sonicwali.com. The table columns are Name, Distributed, Consumed, Min Licenses, Max Licenses, and Capacity. Both appliances have a capacity of 5000. The 'Max Licenses' field for both is set to 5000. At the bottom are 'Save', 'Cancel', and 'Reset Defaults' buttons.

Name	Distributed	Consumed	Min Licenses	Max Licenses	Capacity
KADUBU	2499	0	5	5000	5000
Seafood.eng.sonicwali.com	2501	1	5	5000	5000

5 Click Save, Cancel, or Reset Defaults.

CMS will attempt to distribute all user licenses between the managed appliances and will not hold on to any user licenses. It uses criteria like Min and Max settings, number of users connected in order to determine how to distribute the licenses.

You can also see the actual number of leased licenses that have been distributed at any time to each appliance on this screen.

# General Options Page

*To access the General Options page:*

- 1 Select Management Server > Configure > General Options.  
The Configure General Options page appears.

Secure Mobile Access | Central Management Console

**Management Server**

- Dashboard
- Alerts
- Configure
- Monitor
- Maintain

**Managed Appliances**

- Define collection
- Configure
- Monitor
- Maintain

**Configure General Options**

[Configure Server > General Options](#)

**Client security settings**

Control security settings for users. You can also enhance security using [End Point Control](#) (EPC).

Credential lifetime: \*  minutes

If the length of a session exceeds the time specified, the user is prompted to reauthenticate.

**Date/time**

To set the time zone referenced on the appliance and in the system logs, select a time zone, click **Save**, and then apply your change. To set the current time, click **Change** to set the time manually, or [click here](#) to configure the appliance to synchronize with one or more NTP servers.

Current system time: Tue Jan 27 2015 12:35:30 PST [Change](#)

Time zone:

**Save** **Cancel**

- 2 Make the desired changes.

- 3 Click **Save**.

# Administration Page

**To configure the settings for Administrators, Authentication servers, or Users & Groups:**

- 1 Select Management Server > Configure > Administration.  
The Administration page appears.

The screenshot shows the Dell Secure Mobile Access Central Management Console. The left sidebar has two main sections: 'Management Server' (Dashboard, Alerts, Configure, Monitor, Maintain) and 'Managed Appliances' (Define collection, Configure, Monitor, Maintain). The main content area is titled 'Central Management Administration' and includes a note: 'This configuration applies to central management server administrators. It is also pushed to managed appliances during policy synchronization.' Below this are three sections: 'Administrators' (listing Primary Admin: admin, Super Admin: Jeff Kauffman, Super Admin: John Thekkethala, Read Only: Seattle\_Engineering, Read Only: IT Services, Read Only: SMA-Engineering, Super Admin: Stephen Hailes), 'Authentication servers' (describing an authentication server used for CMS administrators), and 'Users & Groups' (noting that an administrator role is assigned to a user or group).

- 2 Select any of the three items: **Administrators**, **Authentication servers**, and **Users & Groups**.
- 3 Make the changes you want.
- 4 When finished, click **Save**.

# Network Settings Page

**To configure the Basic, Routing, or Name resolution network settings:**

- 1 Select Management Server > Configure > Network Settings.  
The Network Settings page appears.

The screenshot shows the 'Network Settings' page within the 'Configure Server > Network Settings' section of the Dell SMA Central Management Console. The left sidebar lists 'Management Server' and 'Managed Appliances' options. The main content area is titled 'Network Settings' and contains three tabs: 'Basic', 'Routing', and 'Name resolution'.  
**Basic Tab:**  
Single interface, single node  
Appliance name: CMS-VM-001-Main  
Appliance public domain: sea.eng.sonicwall.com  
Private address: 10.4.4.100  
ICMP pings: Enabled  
FQDNs: 3 FQDNs defined  
Custom Ports: 0 custom ports defined  
**Routing Tab:**  
Routing mode: Default gateway  
Default gateway: 10.4.4.1  
Static routes: 0 routes defined  
**Name resolution Tab:**  
Private search domains: sea.eng.sonicwall.com; sv.us.sonicwall.com; eng.sonicwall.com; sonicwall.com  
DNS servers: 10.4.2.22  
10.4.2.50  
WINS servers: N/A  
Windows domain: N/A

- 2 Click **Edit** to configure any of the **Basic**, **Routing**, or **Name resolution** settings.
- 3 When finished, click **Save**.

# Network Services Page

To configure NTP, SSH, SNMP, or SMTP:

- 1 Select Management Server > Configure > Network Services.  
The Network Services page appears.

The screenshot shows the Dell SMA Central Management Console interface. At the top, there's a header with the Dell logo, 'Secure Mobile Access', and 'Central Management Console'. On the left, a sidebar menu includes 'Management Server' (Dashboard, Alerts, Configure, Monitor, Maintain) and 'Managed Appliances' (Define collection, Configure, Monitor, Maintain). The main content area is titled 'Network Services'. It contains four sections: 'NTP' (Configure, Status: Enabled), 'SSH' (Configure, Status: Enabled), 'SNMP' (Configure, Status: Enabled), and 'SMTP' (Configure, Status: Disabled). Each section has a brief description and a 'Configure' link.

- 2 Click **Configure** for the item you want to configure: NTP, SSH, SNMP, or SMTP.
- 3 Make the desired changes.
- 4 When finished click **Save**.

# SSL Settings Page

*To configure SSL certificates or SSL encryption:*

- 1 Select Management Server > Configure > SSL Settings.  
The SSL Settings page appears.

The screenshot shows the Dell Secure Mobile Access Central Management Console interface. At the top left is the Dell logo and the text "Secure Mobile Access | Central Management Console". At the top right is the link "Configure Server > SSL Settings". On the left, there's a sidebar with two main sections: "Management Server" (containing Dashboard, Alerts, Configure, Monitor, Maintain) and "Managed Appliances" (containing Define collection, Configure, Monitor, Maintain). The main content area is titled "SSL Settings". It contains two sections: "SSL certificates" and "SSL encryption". Under "SSL certificates", it shows the "Management console certificate (CMC)" which is self-signed (192.168.0.10) and valid until Jan 22, 2020. It also lists "Virtual hosting certificates for WorkPlace sites and URL resources" with IP addresses 10.4.4.100 and 192.168.0.10. Under "SSL encryption", it specifies "Protocols: Any TLS version" and "Ciphers: Compression: disabled, DES: Triple DES with SHA-1, AES: 256 or 128 bit with SHA-256, 256 or 128 bit with SHA-1, RC4: 128-bit with MD5 or SHA-1".

- 2 Click **Edit** for the item you want to edit: **SSL certificates** or **SSL encryption**.
- 3 Make the desired changes.
- 4 When finished, click **Save**.

# Monitoring the CMS

## To monitor the CMS:

- 1 Select Management Server > Monitor.
- 2 The Monitor Server page appears. From the Monitor Server page, you can select to view and edit the settings for Logging, System Status, and Troubleshooting.

The screenshot shows the Dell Secure Mobile Access Central Management Console (CMS) interface. At the top left is the Dell logo and the text "Secure Mobile Access | Central Management Console". On the left side, there is a navigation sidebar with two main sections: "Management Server" and "Managed Appliances". Under "Management Server", the "Monitor" option is selected and highlighted in grey. Under "Managed Appliances", the "Monitor" option is also listed. The main content area is titled "Monitor Server". It contains three sections: "Logging", "System Status", and "Troubleshooting". Each section has a small icon, a title, and a brief description. The "Logging" section says "View logs and modify logging settings for the central management server". The "System Status" section says "View health metrics and system information for the central management server". The "Troubleshooting" section says "Ping, lookup, routes, network traffic, and snapshot troubleshooting tools".

- 3 To view or edit logging settings for the CMS, click **Logging**.
  - a Make the changes you want and click **Save**.
- 4 To view health metrics and system information for the CMS, click **System Status**.
  - a Make the changes you want and click **Save**.
- 5 To ping, lookup, view network traffic or use snapshot troubleshooting tools, click **Troubleshooting**.
  - a Make the changes you want and click **Save**.

# Maintaining the CMS

**To maintain the CMS:**

- 1 Select **Management Server > Maintain**.

This page has two tabs: **Maintain Server** and **Maintenance Tasks**.

The screenshot shows the Dell SMA Central Management Console interface. The top navigation bar includes the Dell logo, 'Secure Mobile Access', and 'Central Management Console'. On the left, a sidebar lists 'Management Server' (Dashboard, Alerts, Configure, Monitor, Maintain) and 'Managed Appliances' (Define collection, Configure, Monitor, Maintain). The main content area has two tabs: 'Maintain Server' (selected) and 'Maintenance Tasks'. Under 'Maintain Server', product information is displayed: Product: SonicWALL SRA EX-Virtual, Version: 11.2.0-182, and Time since last reboot: 4 Days 1 Hours 31 Minutes 45 Seconds. Below this are three buttons: 'Restart....' (blue icon), 'Shutdown....' (orange icon), and 'Reset....' (green icon). A 'System configuration' section contains an 'Import or export' link and a 'Import/Export...' button. A 'System software updates' section contains 'Update' and 'Rollback' links, each with a corresponding button ('Update...' and 'Rollback...').

- 2 Do any of the following:

- a To restart the CMS, click **Restart**.
  - b To shutdown the CMS, click **Shutdown**.
  - c To reset the CMS, click **Reset**.
- a To import or export a system configuration file, click **Import/Export**
  - a Enter the path name for the system configuration file.
- a To update the system software to a newer version, click the **Update** button.
  - a To rollback the system software to a previous version, click the **Rollback** button.

- 6 Click the **Maintenance Tasks** tab.

The screenshot shows the Dell SMA Central Management Console interface. On the left, there is a navigation sidebar with sections for Management Server (Dashboard, Alerts, Configure, Monitor, Maintain) and Managed Appliances (Define collection, Configure, Monitor, Maintain). The main content area has tabs for 'Maintain Server' and 'Maintenance Tasks'. The 'Maintenance Tasks' tab is selected. A message at the top says 'View, reschedule or delete maintenance tasks. All times are in the server time zone PDT.' Below this is a 'Task log' section with a table header: Time, Task, Run at, Status, Message. There are no rows in the table. Underneath is a 'Scheduled Tasks' section with a table header: Run at, Scheduled by, Task. There are no rows in this table either. At the bottom of the task log section, there is a note: '\*This task will restart the CMS after running.' followed by three buttons: Delete, Run now, and Reschedule.

- 7 In the **Task log** panel, you can view the tasks that are scheduled.  
8 In the **Scheduled Tasks** panel, you can select a task and **Delete**, **Run now**, or **Reschedule** that task.

## Using the Managed Appliances Menu

This section describes the following procedures:

- [Defining a Collection of Managed Appliances](#)
- [Configuring a Managed Appliance](#)
- [Monitoring a Managed Appliance](#)
- [Maintaining a Managed Appliance](#)

# Defining a Collection of Managed Appliances

**To define a collection of managed appliances:**

- Select **Managed Appliances > Define collection**.

This page displays all appliances currently managed by the CMS, and allows you to add or delete new appliances.

Name	Host or IP address	Country	Location
CMS-VM-001-Main	10.4.4.100	United States	Seattle, WA
KADUBU	192.168.144.27	India	Bangalore
Seafood.eng.sonicwall.com	10.4.4.94	United States	Seattle, WA

**To add a new appliance:**

- 1 Click the **New** button with the green plus sign.  
The **Add Appliance** dialog appears.
- 2 Enter the appropriate information in the required fields.
- 3 Click **OK**.
- 4 Click **Save** at bottom of the **Define Managed Appliances** page.

**To Delete a current appliance:**

- 1 Select the appliance you want to delete.
- 2 Click the **Delete** button.
- 3 Click **OK**.
- 4 Click **Save** at the bottom of the **Define Managed Appliances** page.

# Configuring a Managed Appliance

An administrator can import policies from an existing appliance and define configurations. Policies can be applied to all (or a collection) of appliances. Services do not need to be restarted after this configuration.

An existing managed appliance configuration may be partially imported into the CMS to startup the CMS global configuration.

The first time the CMS synchronizes a policy with an appliance, it overwrites the policy on the appliance. This is equivalent to the appliance partially importing the CMS configuration. After the initial policy synchronization, further policy synchronizations replicate the CMS configuration onto the appliance.

Also, after the initial policy synchronization, the administrator can manually modify the address pools of the appliance and the authentication servers. The administrator changes are not overwritten during subsequent CMS policy synchronizations.

The policy settings that are replicated during synchronization are:

- Security policy, including access control rules and EPC configuration
- Network resources
- Users and groups
- Realms
- Authentication servers (the authentication server names should match those on the sending node, even if the IP addresses do not).

When you define a collection of appliances, you have the option of either overwriting authentication server settings (which would be typical in a deployment where there is a shared, central server), or excluding server settings from being overwritten during replication.

- WorkPlace shortcuts
- CA certificates
- Certificate revocation lists downloaded from a remote CDP (CRL distribution point)
- Agent configuration, including graphical terminal agents (Citrix and Windows Terminal Server) and Web browser profiles
- Local user accounts
- Single sign-on profiles

The policy settings that are not replicated during synchronization are:

- Network settings, including IP addresses, routing information, name resolution settings (DNS and WINS), and the settings for the network services (NTP, SSH and SNMP)
- If you have configured fallback servers for your Connect Tunnel users, each appliance has a unique list that is not replicated on the other servers
- License files
- SSL certificates
- WorkPlace configuration data (customized templates)
- Administrator user accounts and role definitions
- (Optional) You can exclude authentication server settings from being overwritten during replication, which is typical for a deployment where each appliance has its own authentication server.

**To configure a managed appliance:**

- 1 Go to the **Managed Appliance > Configure** page.

The **Define policy** tab provides access to the **Security Administration**, **User Access**, and **System Configuration** policy pages:

The screenshot shows the Dell Secure Mobile Access Central Management Console interface. On the left, there is a navigation sidebar with options like Management Server, Dashboard, Alerts, Monitor, Maintain, Managed Appliances (with sub-options Define collection, Configure, Monitor, Maintain), and User Access. The main content area has tabs for 'Define policy' and 'Synchronize policy'. The 'Define policy' tab is active and displays three main sections: 'Security Administration', 'User Access', and 'System Configuration'. Each section contains various configuration options and descriptions. For example, under 'Security Administration', there are sections for Access Control, Resources, and Users & Groups. Under 'User Access', there are sections for Realms, Network Tunnel Service, Web Proxy Service, WorkPlace, Agent Configuration, and End Point Control. Under 'System Configuration', there are sections for Administrators, Authentication Servers, CA certificates, and OCSP.

- 2 Click **Security Administration** to define access control, resources (web, file, group and variables), users and groups.
- 3 Click **User Access** to define realms, network tunnel service, WorkPlace, agent configuration, and end point control.
- 4 Click **System Configuration** to define administrators, authentication servers, CA certificates, and Online Certificate Status Protocol (OSCP).
- 5 When you are finished defining a policy, click **Save** or **OK**.

6 Click the **Synchronize policy** tab.

Use this page to push policy data to selected appliances.

The screenshot shows the Dell Secure Mobile Access Central Management Console interface. On the left, there's a sidebar with 'Management Server' and 'Managed Appliances' sections. The main area has tabs for 'Define policy' and 'Synchronize policy', with 'Synchronize policy' being active. A sub-header says 'Push policy data to the selected appliance(s.)'. Below this is a table with two rows:

Name	Status
KADUBU	<b>Policy import required</b> - the appliance policy (users, auth servers, resources, etc) will be overwritten and user connections will be closed.
Seafood.eng.sonicwall.com	<b>Policy import required</b> - the appliance policy (users, auth servers, resources, etc) will be overwritten and user connections will be closed.

Below the table is an 'Advanced' panel with the following options:

- Force selected appliances to import the CMS policy
- Synchronize configuration:
  - Now
  - At [14] : [30] PST on [01/27/2015 today]

At the bottom are 'Synchronize' and 'Cancel' buttons.

7 Click **Advanced** to open the **Advanced** panel.

8 Select the **Force selected appliance to import the CMS policy** checkbox.

This triggers the next synchronization (or scheduled sync) to overwrite the policies of the selected appliances with the CMS policy (just as the initial policy synchronization would). This is a way to reset appliance policy to the baseline CMS policy.

9 Select **Now** if you want to synchronize immediately.

or

Select **At** and choose the time and date from the drop-down menus when you want the synchronization to take place.

10 Click **Synchronize**.

Replicating a policy does not usually terminate existing user sessions. If the next sync will terminate user sessions an appropriate warning message is displayed for that appliance on the Sync Policy page.

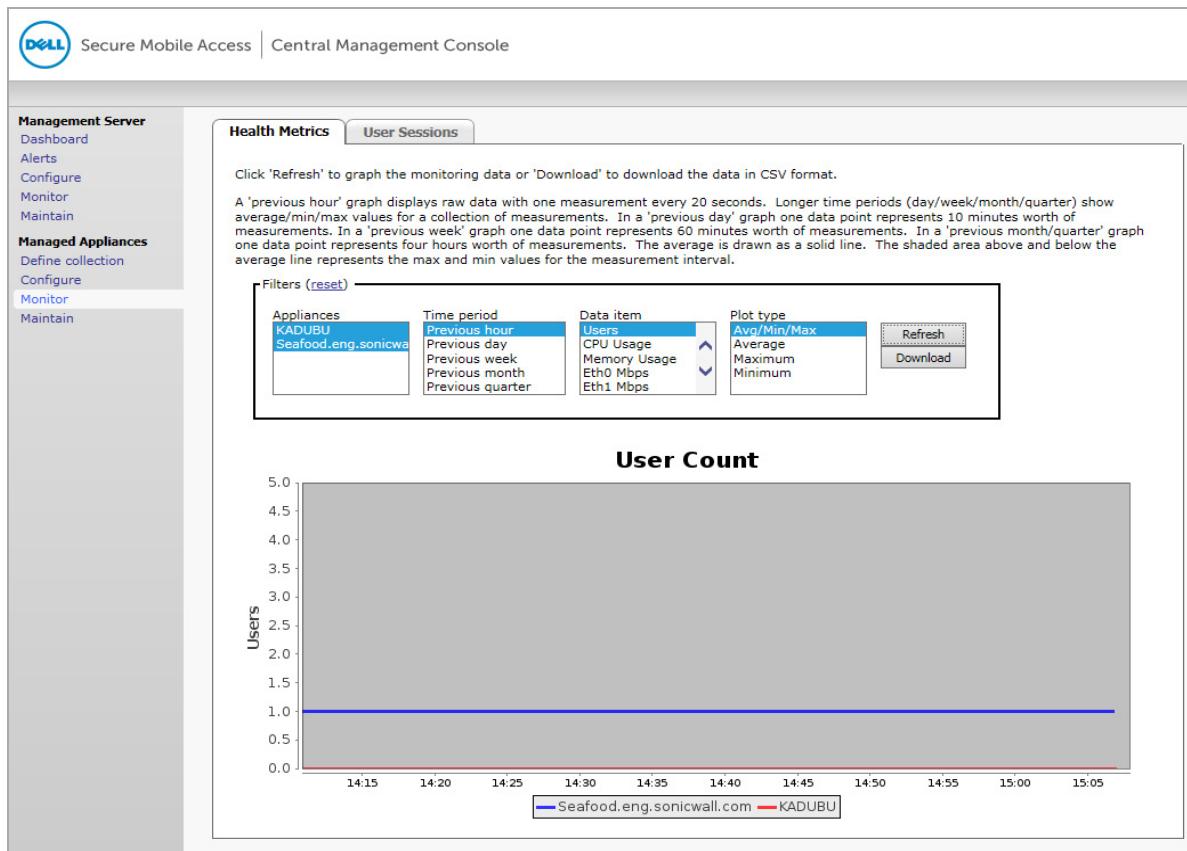
# Monitoring a Managed Appliance

Each managed appliance streams monitoring events to the CMS and the CMC provides a view of aggregated events from managed appliances on the Dashboard. The Dashboard also provides a view of VPN infrastructure. It displays key CMS/appliance parameters such as license usage, CPU, memory, bandwidth, swap activity, and disk activity.

## To monitor a managed appliance:

- 1 Go to the **Managed Appliances > Monitor** page.

This page provides two tabs: **Health Metrics** and **User Sessions**. From this page, you can monitor the health metrics on a graph that charts users against time.



- 2 From the **Appliances** menu, select the appliance you want to graph.
- 3 From the **Time period** menu, select the time period you want the graph to display.
- 4 From the **Data item** menu, select the data you want the graph to display.
- 5 From the **Plot type** menu, select the type of graph you want to plot.

# User Sessions

On the **User Sessions** page, you can view current and past user sessions and terminate current sessions.

If you select a session and then select the **Terminate session-restrict logins** option, it temporarily disables the user's access for up to 10 minutes.

## To view and manage user sessions:

- 1 Go to the **Managed Appliances > Monitor** page.
- 2 Click the **User Sessions** tab.
- 3 From the drop-down menus, select the items you want to view or manage.

The screenshot shows the 'User Sessions' tab selected within the 'Health Metrics' section of the Dell Secure Mobile Access Central Management Console. The interface includes a sidebar with 'Management Server' and 'Managed Appliances' sections. The main area displays a table of user sessions with columns for User, Appliance, Started, Ended, Elapsed, Avg bytes/min, and Total bytes. One session is listed: kmott@sv.us.sonicwall.com, connected to Seafood.eng.sonicwall.com, started at 01/27/2015 08:16 PST, and has been active for 0 days, 6:52, averaging 694 KB/min and totaling 171 MB. Buttons for 'Terminate session' and 'Terminate session - restrict logins' are visible above the table. A status bar at the bottom indicates '1 of 1 sessions shown, 1 currently active' and the date '01/27/2015 15:09'.

# Maintaining a Managed Appliance

**To maintain a managed appliance:**

- 1 Go to the **Managed Appliances > Maintain** page.  
This page has two tabs: **Maintain Appliances** and **Maintenance Tasks**.

Name	Host	Platform	Version	Hotfixes	EPC version	Pending Changes
Shanghai-113	192.168.0.113	EX-Virtual	11.2.0-192	None	14.12.31.00	No
Seattle-111	192.168.0.111	EX-Virtual	11.2.0-192	None	14.12.31.00	No
Bangalore-112	192.168.0.112	EX-Virtual	11.2.0-192	None	14.12.31.00	No

- 2 Under the **Maintain Appliances** tab, select the checkbox for an appliance and use the top buttons to perform any of the following tasks: **Restart**, **EPC Update**, **Upgrade/Hotfix**.
- 3 Select the **Maintenance Tasks** tab.

Time	Task	Run at	Status	Message
04/08/2015 02:02:48	New! Restart Shanghai-113	04/10/2015 02:00 PDT	Scheduled	scheduled by admin
04/08/2015 02:01:18	Restart Seattle-111	04/08/2015 02:01 PDT	Executing	

- 4 In the **Task log** panel, you can view the tasks that are scheduled.
- 5 In the **Scheduled Tasks** panel, you can select a task and **Delete**, **Run now**, or **Reschedule** that task.

## Part 4

# Licensing and Alerts

- Pooled Licensing
- Alerts and SNMP

# Pooled Licensing

This section contains information about pooled licensing and the CMS in the following sections:

- [Overview on page 57](#)
- [Types of Licenses on page 59](#)
- [Types of Licenses on page 59](#)

## Overview

Appliances that are globally located have fluctuating demands for user licenses due to time differences.

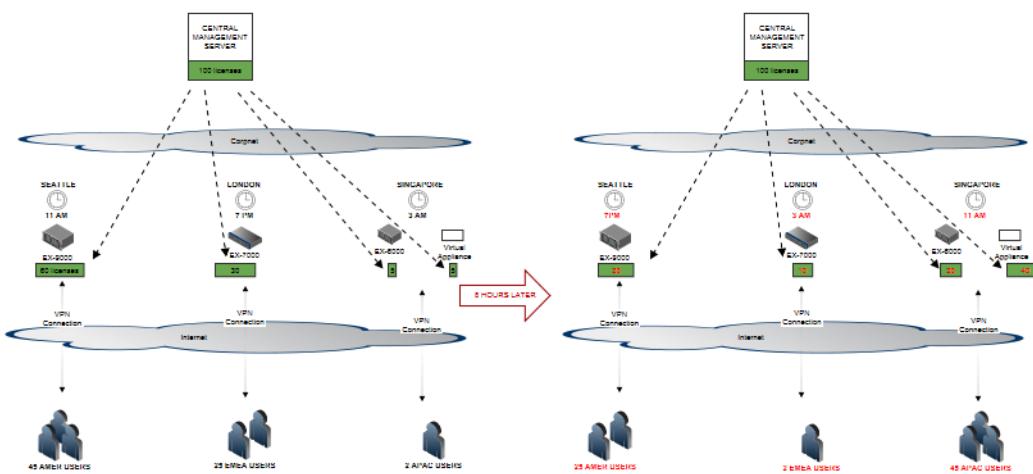
A Central Management Server (CMS) can manage a pool of user licenses and dynamically allocate them among managed appliances. Managed appliances do not have their own user licenses and use the allocated licenses. The CMS distributes the pool of licenses between the managed appliances based on demand. The CMS requires a CMS license in order to be functional.

Each CMS license permits the management of up to 3 managed appliances (default). Customers may choose to purchase additional licenses for managed appliances.

## How CMS Pooled Licenses Work

User licenses no longer have to be applied to individual VPN appliances. A new central licensing model allows CMS licenses for users to be distributed and reallocated dynamically among the managed appliances based on user demand. Customers with appliances that are globally distributed can benefit from the fluctuating demands for user licenses due to time differences. The CMS reallocates licenses to managed appliances where user demands have peaked from appliances in a different geographic area where usage has fallen due to off-work/night hours. Customers with appliances that are behind load balancers can benefit from the dynamic distribution of licenses across managed appliances as the load balancer distributes connection requests across the managed appliances.

The following drawing illustrates centrally managed licenses for globally located VPN appliances.



CMS creates "leased licenses" for a number of users based upon usage demand. The administrator defines the maximum and minimum for each managed appliance. CMS redistributes the leased license periodically based on usage, thereby changing the number of licensed users allowed for each managed appliance.

- i **NOTE:** The configured maximum number of user licenses is not a hard limit. A small percentage of additional connections to a managed appliance are allowed. When the number of connections to a managed appliance exceeds the configured maximum, the number of consumed licenses that is shown on the CMC license distribution page can be up to 10% higher than the number of distributed licenses. Alerts may also report license usage up to 110%.

CMS attempts to allocate all available user licenses. Leased licenses have a validity of 7 days.

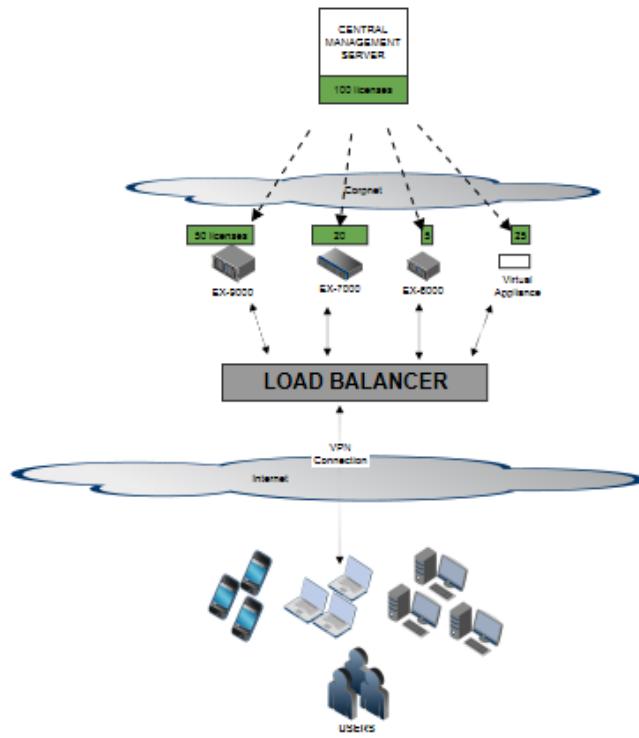
CMS Spike licenses are stackable user licenses obtained from MySonicWALL and are commonly valid for 10 to 30 days. Spikes license add to the license pool and are redistributed based on user demand. They can be started and paused from the CMC.

In the event of a **communication loss between CMS and a Managed Appliance**:

- Appliance: Continues with a leased license until the lease expires (7 days) or communications are re-established.
- CMS: Recovers lost licenses after 24 hours.

In the event of a **communications loss between the CMS and MySonicWall**: The CMS continues to generate leased licenses for up to 30 days.

The following drawing shows centrally managed licenses for VPN appliances behind a load balancer.



## Types of Licenses

There are two types of license:

- **CMS License** - A new type of license issued from MySonicWall.com that gets applied to the CMS. It has two dimensions - user licenses and appliance licenses.
- **CMS Spike License** - A spike license that is issued from MySonicWall.com and can be applied to the CMS. A CMS Spike license consists of stackable (adds to the pool) user licenses that can be added to currently existing licenses in the pool and distributed automatically based on demand. The license can be paused or stopped from the CMC. After a 24 hour period of no activity, the CMS recovers the Spike license and reassigns it to a different appliance.

# Alerts and SNMP

This section contains detailed information about alerts and the use of SNMP in the CMS. It consists of the following topics:

- [Overview on page 60](#)
- [Pre-Configured Alerts on page 61](#)
- [Configuring SNMP on page 63](#)

## Overview

The CMS generates alerts that are either Warnings or Errors. Alerts are displayed prominently on the CMS dashboard. Alerts can originate from a condition that occurs on the CMS, or from a managed appliance.

Alerts can be configured to generate SNMP traps that are monitored by any IT infrastructure Network Management System (NMS).

# Pre-Configured Alerts

The Table of Pre-Configured Alerts below has a fixed set of conditions that can trigger alerts.

 **NOTE:** The Priority symbols represent a Warning  or an Error .

**Table 1. Table of Pre-Configured Alerts**

Priority	Name	Measurement	Condition
	Unable to communicate with MySonicWall	CMS connection to MySonicWALL	Connection is lost for 10080 minutes
	Unable to communicate with MySonicWall	CMS connection to MySonicWALL	Connection is lost for 4320 minutes
	Temporary communication loss	Manage appliance connection to CMS	Connection is temporarily lost
	Pertmanent communication loss	Managed appliance connection to CMS	Connection is permanently lost
	High user license usage	CMS license usage	Value is over 95 percent
	High user license usage	CMS license usage	Value is over 75 percent
	High swap usage	Swap usage	Value is over 5 percent
	High memory usage	Memory usage	Value is over 85 percent for 5 minutes
	High disk usage	Disk usage	Value is over 95 percent
	High CPU usage	CPU usage	Value is over 85 percent for 5 minutes
	High appliance license usage	Appliance license usage	Value is over 89 percent
	Critically high memory usage	Memory usage	Value is over 95 percent for 5 minutes
	Critically high CPU usage	CPU usage	Value is over 95 percent for 5 minutes
	Critically high appliance license usage	Appliance license usage	Value is over 98 percent
	Certificate expired	Time until certificate expires	Value is under 0 days
	Certificate about to expire	Time until certificate expires	Value is under 30 days

The administrator can edit the pre-configured alerts as follows:

- Modify or customize these pre-configured default alerts.
- Disable them
- Make changes to the threshold, duration and message.
- Configure additional alerts. The Table of Alerts lists all the conditions that can be used to configure Alerts.

For these activities, use the following guidelines:

- When an appliance-related alert is configured, it applies to all the managed appliance, that is, alerts cannot be individually configured/tailored for a specific appliance.
- The maximum number of alerts that can be configured by the Administrator on a CMS is 100.

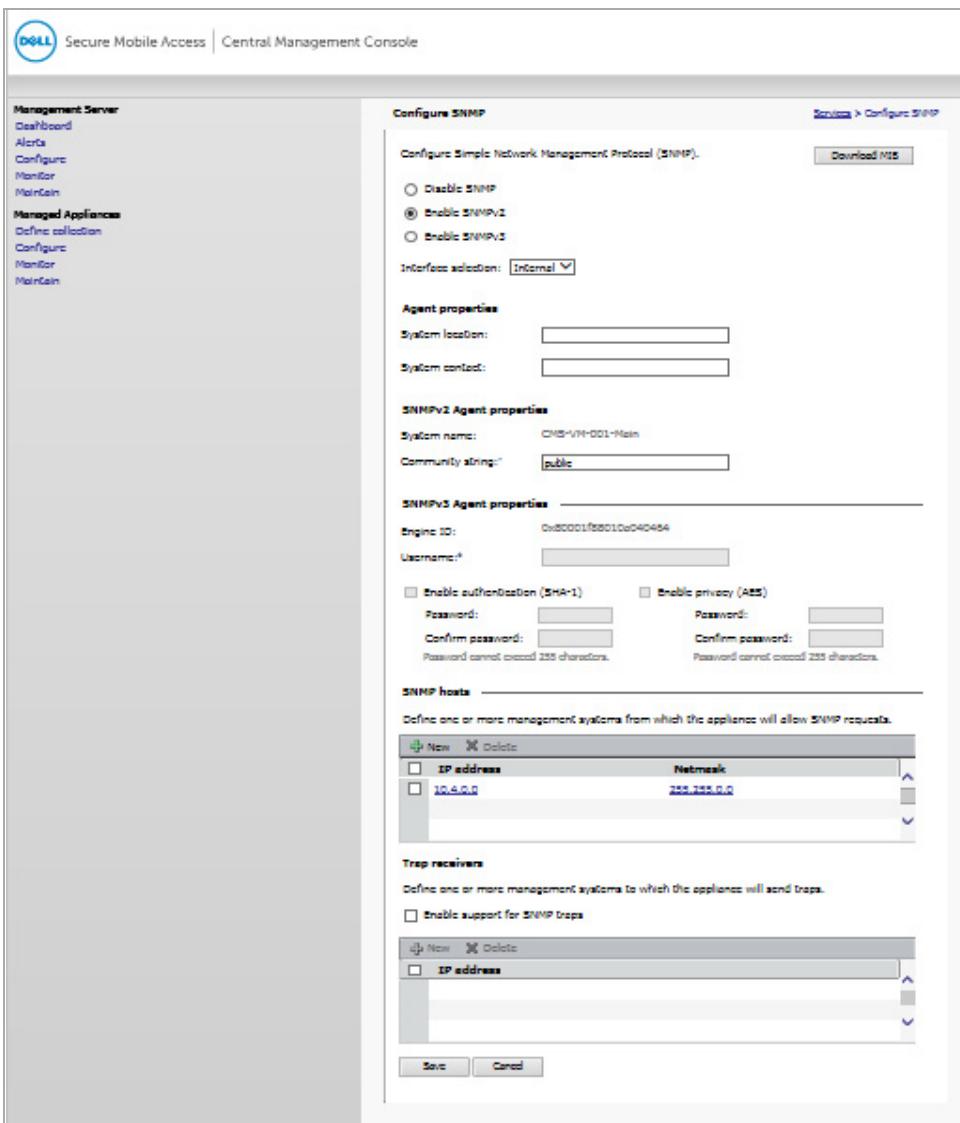
Alerts shown on the dashboard can be dismissed by the Administrator. Dismissed alerts will no longer be displayed in the dashboard view, but can be seen in the Alerts page. If the alert condition toggles (ON->OFF->ON), a new alert for the same condition will be raised in the dashboard.

All alerts are stored in the Alerts Database. A rolling history of 90 days worth of alerts are retained in the Alerts Database. An Alerts View allows the Administrator to see all Alerts in the past Day, Week, Month or Quarter.

# Configuring SNMP

**To enable SNMP:**

- 1 Click Management Server > Configure > Network Services.
- 2 Under SNMP, click Configure.



- 3 Enter the information you want in the appropriate fields.
- 4 Click Save.

## Contacting Dell

Dell listens to customers and delivers worldwide innovative technology, business solutions and services they trust and value. For more information, visit [www.software.dell.com](http://www.software.dell.com).

**Technical support:**

[Online support](#)

**Product questions and sales:**

(800) 306-9329

**Email:**

[info@software.dell.com](mailto:info@software.dell.com)

## Technical Support Resources

Technical support is available to customers who have purchased Dell software with a valid maintenance contract and to customers who have trial versions. To access the Support Portal, go to <https://support.software.dell.com/>.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. In addition, the portal provides direct access to product support engineers through an online Service Request system.

The site enables you to:

- Create, update, and manage Service Requests (cases)
- View Knowledge Base articles
- Obtain product notifications
- Download software. For trial software, go to [Trial Downloads](#).
- View how-to videos
- Engage in community discussions

Chat with a support engineer