

Release Notes for Cisco Smart Storage Open Web Analytics PKG Package Version 1.3.1

November 2010

These Release Notes provide information for the Open Web Analytics PKG Package version 1.3.1 for the Cisco NSS 300 Series Smart Storage.

Contents

This document includes the following topics:

- **Introduction**
- **Description**
- **Prerequisites**
- **Firmware Requirements**
- **Downloading and Upgrading the Firmware**
- **PKG Package Installation**
- **Caveats**
- **Enable Web Server**
- **Enable MySQL Server**
- **Configure SMTP Server**
- **Additional Resources**

Introduction

Your NSS 300 Series Smart Storage comes with built-in applications and the ability to add new applications. Add-on applications add new functionality to your Smart Storage device. Add-on applications are downloaded from Cisco.com via a PKG package or PKG plugin installation file.

Description

Open Web Analytics (OWA) is an open source web analytics software that you can use to track and analyze how people use your websites and applications. OWA also comes with built-in support for tracking websites created with popular content management software, such as WordPress and MediaWiki.

For more information about the OWA features and installation, see:

- OWA Documentation Wiki—<http://wiki.openwebanalytics.com>
- OWA Demo and Examples—<http://demo.openwebanalytics.com>

Prerequisites

Prior to running the OWA software PKG package, the Web server and MySQL server need to be enabled on the Cisco NSS 300 Series Smart Storage (NAS) device. In addition, the OWA software PKG package requires an email server. See [Enable Web Server, page 6](#), [Enable MySQL Server, page 7](#) and [Configure SMTP Server, page 7](#).

It is strongly recommended to create a dedicated database for OWA to make the database easier to manage and avoid the risk of overwriting data. To configure MySQL, you can use either phpMyAdmin or the command-line environment. If you are not familiar with using the command-line or the SQL language, it is recommended to use phpMyAdmin.

NOTE During the initial installation of the NAS, phpMyAdmin is pre-installed in Applications > PKG Plugins > PKG Installed.

To create a database using phpMyAdmin:

STEP 1 Choose **Applications > PKG Plugins > Installation** from the Navigation menu. The *PKG Plugins INSTALLATION* window appears.

STEP 2 Click the graphical phpMyAdmin icon to open the application.

STEP 3 To log into phpMyAdmin, enter the default username **root** and the default password **admin**.

NOTE When you are configuring a PKG package, if you are prompted to enter the database default username and password, enter **root** for username and **admin** for password. If the password has been changed, enter the root's password account.

STEP 4 In the *Create a new database* field, enter the name for the new database.

STEP 5 Click **Create**. The database is created and you are ready to install the PKG package.

NOTE When you are configuring the PKG package and prompted to enter the database name, enter the database name exactly as it was created in phpMyAdmin.

If you are prompted for "database server" or "database host," use **localhost**. Localhost will sometimes automatically display as the default.

Firmware Requirements

The Cisco NSS 300 Series Smart Storage device should be running firmware version 1.0.0 or higher. To update your firmware see, [Downloading and Upgrading the Firmware](#).

Downloading and Upgrading the Firmware

This procedure describes how to upgrade the firmware on the NSS 300 Series Smart Storage devices from the Network Attached Storage (NAS) interface.

Release Notes



CAUTION As a precautionary measure, back up the NAS system configuration before upgrading the firmware.



CAUTION Do not upgrade the firmware over a WAN or Wi-Fi link since an interruption in service can lead to corruption of the firmware upgrade process.

From the *Administration > Firmware Upgrade* window, you can view the current firmware version and update the firmware on the NAS. The current NAS settings will not change while performing the firmware version update.

To upgrade the firmware:

-
- STEP 1** Click **Administration > Firmware Upgrade** from the Navigation menu. The *Firmware Upgrade* window appears. The current firmware version is displayed.
 - STEP 2** Click **Browse** to locate the correct firmware file for the system update. Before updating the system, verify that the product model and firmware version you are going to update is correct.
 - STEP 3** Click **Update The System**.

Within 15 seconds, a MD5 checksum result window will display to confirm the integrity of the system. After the successful integrity check of the NAS, click **OK** for the new firmware file to upload to the NAS. After this has completed, a message displays and asks you to reboot the system. Please wait patiently. A system log in window will automatically display after the successful update to the new firmware.

The MD5 verification window does not perform any processing on the NAS or the candidate firmware for installation. Once the target firmware has been selected, the MD5 verification allows the user to validate the checksum calculated by the NAS against the provided checksum value found in a separate file that was provided alongside the firmware download. Mismatched checksums indicate firmware integrity has been compromised.

PKG Package Installation

From the *Applications > PKG Plugins* window, you can install PKG packages to add more functions to the NAS. Before you install the packages, make sure the files are correct, read the instructions carefully, and back up all important data on the NAS. Download the software package that you want to install on NAS to your computer.

To install a new PKG package:

-
- STEP 1** Choose **Applications > PKG Plugins > Installation** from the Navigation menu. The *PKG Plugins INSTALLATION* window appears.
 - STEP 2** Click **Browse** to locate and select the owa_1.3.1.pkg file.
 - STEP 3** Click **Install**. The OWA PKG Plugin is installed to the NAS.
- NOTE** To verify the PKG is installed, choose **Applications > PKG Plugins > PKG Installed**. A graphical icon appears in the window, indicating that the PKG is installed on the NAS system.
-

To open the OWA application:

-
- STEP 1** Choose **Applications > PKG Plugins > PKG Installed** from the Navigation menu. The *PKG Plugins PKG INSTALLED* window appears.
 - STEP 2** Click the graphical OWA icon to open the application.
 - STEP 3** Click the link next to the Web Page.
 - STEP 4** Enter the OWA administrator account to access the application.
- NOTE** This account information is received at the end of the OWA installation.
-

To remove a OWA PKG package:

-
- STEP 1** Choose **Applications > PKG Plugins > PKG Installed** from the Navigation menu. The *PKG Plugins PKG INSTALLED* window appears.
 - STEP 2** Click on the OWA icon. The OWA application window appears.
 - STEP 3** Click **Remove**. The OWA PKG package is removed from the NAS.
-

Caveats

Information regarding any known caveats with OWA can be accessed from the OWA website:

http://wiki.openwebanalytics.com/index.php?title=Category:Release_Notes

Enable Web Server

To enable the web server network service:

- STEP 1** Choose **Network Services > Web Server** from the Navigation menu. The *Web Server* window opens.
- STEP 2** Click **Enable Web Server** to enable the web server.
- STEP 3** Enter the value for the Port Number for the web server. Default value is 80 but you can enter another port number. Note that port 8080 is already being used for the admin web server.
- STEP 4** Enable or disable register_globals by clicking **On** (enable) or **Off** (disable). The setting is disabled by default. When the web program asks to enable PHP register_globals, enable register_globals. However, for system security concerns, it is recommended that this option be disabled when possible.
- STEP 5** Enable SSL if a secure connection is needed by clicking **Enable Secure Connection (SSL)**. After enabling this option, users can access websites which are hosted on the NAS over SSL. The concept of HTTPS is a combination of the HTTP with the SSL/TLS to create a secure channel over the network.
- STEP 6** Enable WebDAV (Web-based Distributed Authoring and Versioning) if needed by clicking **Enable WebDAV**. WebDAV is a set of extensions to HTTP that allows users to edit and manage files collaboratively on remote World Wide Web servers. After enabling this function, you can access shared folders remotely through a client application.

NOTE Go to **Access Right Management > Share Folders** for detailed privilege settings.
- STEP 7** Enable php.ini if necessary by clicking **php.ini Maintenance**. The php.ini file is the system configuration file for the Web Server. After enabling this function, you can edit, upload or restore this file. It is recommended that you use the system default setting.

STEP 8 Click **Apply**. Your web server settings are updated to the NAS.

Enable MySQL Server

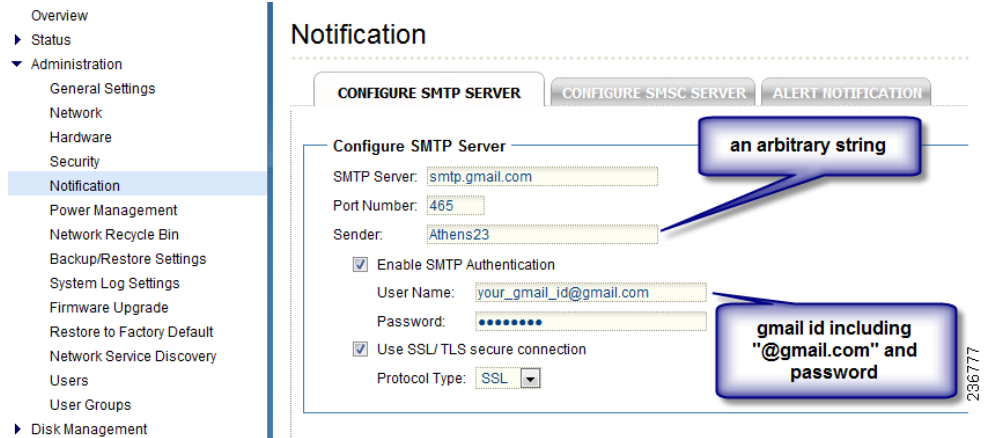
To enable MySQL server application:

-
- STEP 1** Choose **Applications > MySQL Server** from the Navigation menu. The *MySQL Server* window opens.
- STEP 2** Click **Enable MySQL Server** to enable MySQL Server.
- STEP 3** To enable TCP/IP Networking, click **Enable TCP/IP Networking** and specify a port number. The default port is 3306.
- STEP 4** Click **Apply**. Your MySQL Server settings are updated to the NAS.
-

Configure SMTP Server

For the OWA application, you might need to perform a password reset for the OWA user. OWA requires a mail server to send the password reset URL command to your personal email address. When the email is received, it includes a URL link. You must open this URL link for the password reset.

On the NAS device, you can configure the Simple Mail Transfer Protocol (SMTP) server by using an external server, such as Gmail server. An example of using Gmail as the SMTP server is shown.



To configure the SMTP server:

STEP 1 Choose **Administration > Notification > Configure SMTP Server** from the Navigation menu. The *Configure SMTP Server* window opens.

STEP 2 Enter the parameters according to the mail server configuration:

- **SMTP Server**—Enter the name of the SMTP server. For example: smtp.gmail.com.
- **Port Number**—Enter the port number used by the SMTP server. The default port number is 25. If you are running a mail server at home, verify that port number 25 is not blocked by your ISP.
- **Sender**—Enter the email address that you want to appear in the from: field of the email header of each email alert.
- **Enable SMTP Authentication**—Enables SMTP authentication. If enabled, the system will request authentication of the mail server before the message is sent. A user name and password must be specified. This is optional.
 - **User Name**—Enter your email account user name.
 - **Password**—Enter your email account password.
- **Use SSL/TLS secure connection**—Enables Secure Sockets Layer (SSL) / Transport Level Security (TLS) connections. This is optional.

STEP 3 Click **Apply** to save the settings.

Additional Resources

Support for the add-on applications is available via open source online community support resources.

Cisco Resources	URL
Cisco PKG Add-on Application Downloads	http://www.cisco.com/go/smartstorage
Cisco Smart Storage Application Support	http://www.cisco.com/go/smartstorage-apps
Cisco Smart Storage Documentation, Application Notes, and Video Application Notes	http://www.cisco.com/go/smallbizsmartstorage
Open Web Analytics Resources	URL
OWA Website	http://www.openwebanalytics.com
Wiki Documentation	http://wiki.openwebanalytics.com
Demo and Examples	http://demo.openwebanalytics.com

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

© 2010 Cisco Systems, Inc. All rights reserved.

OL-23727-01