



Dell Protected Workspace Management Server



Installation and Configuration Guide

Dell Protected Workspace Management Server v2.2.2

Created and Maintained by Invincea, Inc.

Proprietary – For Customer Use Only

Contents

<i>Purpose and Intended Audience</i>	5
<i>System Requirements</i>	5
DPWMS Sizing Recommendations	6
<i>Dell Protected Workspace Management Server Features</i>	7
Threats Module	7
Configuration Module	7
Admin Module	7
<i>Installation on VMware vSphere 4.x or later</i>	8
Installing VMware Tools for DPWMS running in a vSphere Environment	14
Upgrading the network adapter to VMXNET3 for DPWMS running in a vSphere Environment	16
Conversion of files for VMware Workstation 7 or 8	21
<i>Installing DPWMS on VMware Workstation 7.1.x or later</i>	22
<i>Installing the DPWMS on Custom Hardware or a custom Virtual Machine</i>	24
Installing the DPWMS and prerequisites.....	24
Configuring the DPWMS SYSV startup script.....	25
Configuring the DPWMS configuration file	27
[server].....	27
[license].....	28
[mysql]	28
[logging]	28
<i>Applying New Updates via the UI</i>	29
<i>Manual Upgrade from via SSH/Console</i>	31
<i>Merging configuration file (ims.conf) changes after upgrade</i>	32
<i>Configuring Secure Protocol for Client Connections</i>	32
<i>Configuring the Dell Protected Workspace Management Server for Basic Operation – Pre-Built Virtual Machine Only</i>	33
Obtaining the DHCP Address of the System	33
Accessing the WebUI	34
Changing the time or time zone.....	35
Network Configuration	38
Self-Signed Certificate Creation	42
Changing the root and ims_admin passwords.....	45

<i>Additional Administrative Tasks</i>	46
Modifying the default Firewall	46
Installing Linux Updates	47
Generating a new self-signed certificate after initial configuration is complete	49
Installing a Trusted SSL certificate	49
Generating a CSR.....	49
Importing Signed Certificate and Key.....	51
Configuring the Dell Protected Workspace Management Server for SYSLOG	52
Testing SYSLOG connection from DPWMS.....	53
Configuring the Threats Module with the Correct SYSLOG format.....	54
<i>Operational Notes for the Dell Protected Workspace Management Server</i>	55
Security Restrictions/Features	55
Logging into the Appliance Remotely via SSH	55
<i>Configuring Dell Protected Workspace to work with the Dell Protected Workspace Management Server – Configuration Management Module</i>	56
<i>Configuring Dell Protected Workspace to work with the Dell Protected Workspace Management Server – Threat Data Module</i>	57
<i>Dell Protected Workspace Management Server Administrative Tasks</i>	58
Acquiring the temporary administrator password for DPWMS UI	58
Logging into the Dell Protected Workspace Management Server Console	59
Entering the DPWMS License Key	60
DPWMS UI Method.....	60
DPWMS Configuration File Method.....	62
Modules	63
Admin Module.....	64
Users Tab	64
Adding a new DPWMS User	65
Deleting a user from the DPWMS	66
Activity Tab	67
Backup Tab.....	67
Create a Database Backup.....	68
Recovering from a Database Backup File	68
Errors Tab.....	69
Upgrades Tab.....	70
Upgrading the DPWMS.....	70
Restarting the DPWMS Process.....	71
Platform Tab	72
Dell Protected Workspace Home Module.....	73
Home Tab.....	74
Threat Data Section	74
Configuration Management Section	75

Administration Section	76
Threats Module	77
Settings and Plugins	78
Threat Data Module Settings	78
Plugin Settings	79
Overview Tab	80
Detections by Date	80
Detections by Category	80
Top Users and Top Sources	81
Detections Tab	82
Threat Categories	83
Report Overview Page	85
Statistics	85
Configuration	86
Applications	87
Threat Report Analysis Tab	88
Threat Report Event Tree Tab	89
Threat Report Timeline Tab	91
Threat Report Geography Tab	92
Threat Report Plugin Tabs	92
Threat Report Actions:	93
Configuration Module	94
Hosts	94
Groups	94
Packages	94
Accessing the Configuration Module	95
Configuration Module Interface	95
Packages Tab	95
Adding a Package to the DPWMS	96
Viewing package details	97
Entering the Client Software Activation Key	100
Additional Global Package Settings	101
Groups Tab	102
Creating a New Group	103
Renaming a Group	103
Group Details View	104
Set Installation Method	109
Adjust Preferences	111
Adding Custom Preferences / Attributes	113
Manage Unprotected Sites	115
Customize App Settings	118
Hosts Tab	122
Audit Tab	127
Contacting Dell Support	129

Purpose and Intended Audience

This document is intended to provide instructions for installing and configuring the Dell Protected Workspace Management Server. It is intended for IT administrators that will be completing the initial deployment and configuration and/or will be managing the Dell Protected Workspace Management Server.

System Requirements

- One of the following Host Platforms
 - VMware Workstation 7.1 or later
 - VMware ESX or ESXi 4 or later
- 2GB of available RAM for the Virtual Machine (for pre-built template)
- 40GB of available disk for the Virtual Machine (for pre-built template)
- 1 Network connection for the Virtual Machine
- 1 IP address to assign to the system
- 1 DNS System Name to assign to the system
- External internet connectivity (for activation and OS updates)
- Compatible web browser to access the system
 - Internet Explorer 9+
 - Google Chrome 30+
 - Mozilla Firefox 20+

IMPORTANT NOTE: The Dell Protected Workspace Management Server requires an internet connection to allow activation of the server.

The virtual machine can also be run in a Citrix or Microsoft virtual environment; however installation instructions are not included for those environments. The provided VMware image will also need to be converted to support these other platforms before deployment. Post-installation configuration steps will remain the same.

DPWMS Sizing Recommendations

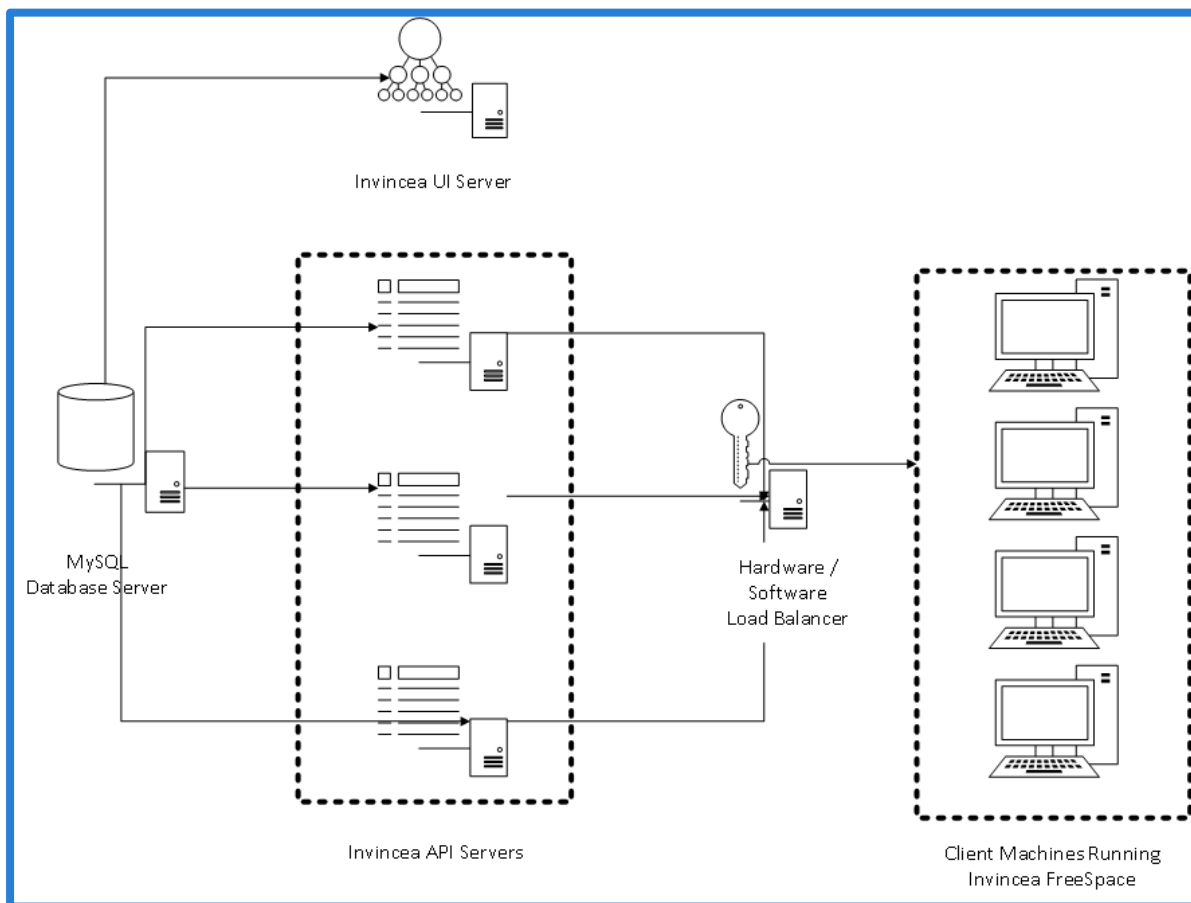
The following table outlines the recommended VM configuration based on number of clients that will connect to the DPWMS:

# of Client Systems	# of DPWMS API Systems	Memory per system	vCPU per system
Up to 1000	1	2GB	1vCPU
1000 – 2000*	1	4GB	2 vCPU
2000+	multiple	2GB	1 vCPU

*This number can be increased if heartbeats are set to daily, this is based on an hourly heartbeat setting

Note: for environments that require multiple API servers, a dedicated MySQL VM, a dedicated DPWMS UI VM and a dedicated load balancer VM are all recommended.

The following graphic provides a basic overview of a multi-API environment, as recommended for larger installation bases.



Dell Protected Workspace Management Server Features

The Dell Protected Workspace Management Server is a modular system that allows for multiple Dell Protected Workspace applications to run on a single appliance. Each module is licensed individually and will only be available with a valid license key.

Threats Module

The Threats Module allows Dell Protected Workspace clients to view Threat Report details. The module receives the reports from the Enterprise client software and displays them for review by the security analysts. This feature set was previously found in the Dell Protected Workspace Threat Data Server.

Configuration Module

The Configuration Module allows for centralized management of the Dell Protected Workspace clients, managing both configuration files and software updates. This feature set was previously found in the Dell Protected Workspace Configuration Management Server.

Admin Module

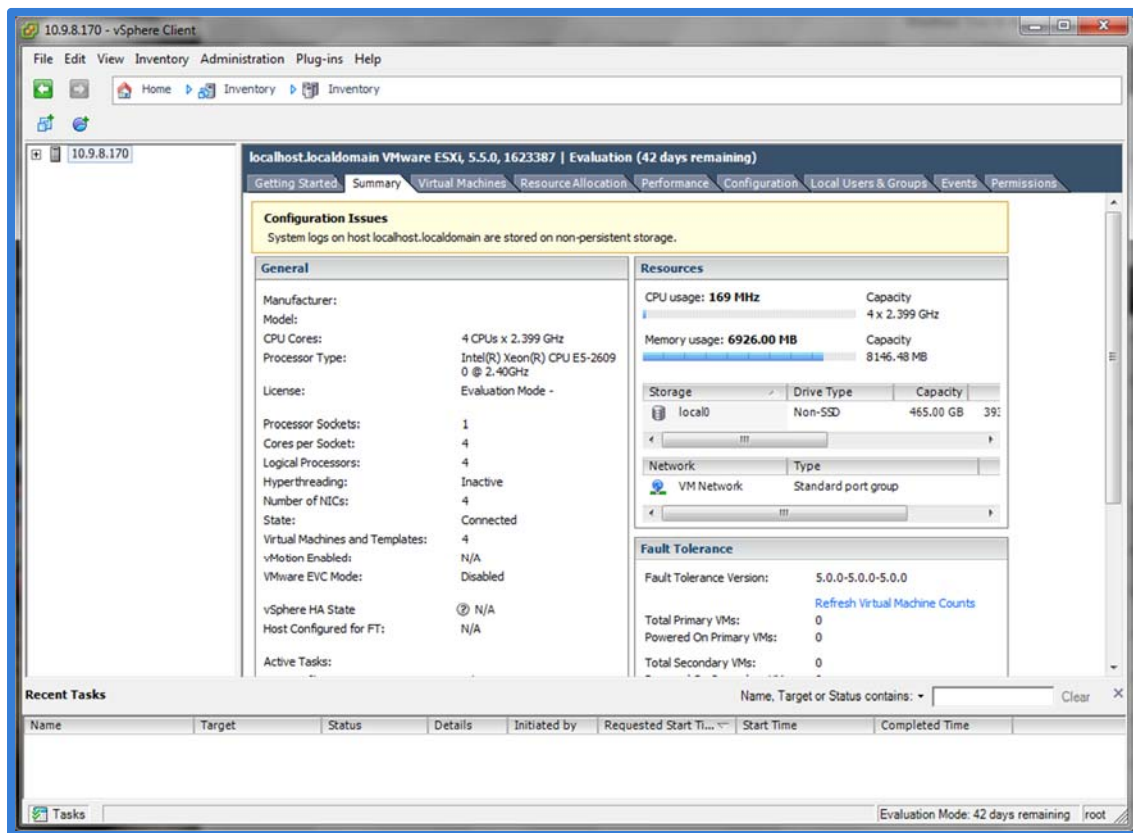
The Admin Module allows for administrative management of the Dell Protected Workspace Management Server, including managing user accounts, applying DPWMS upgrades, viewing error logs and creating backups of the database.

Installing the Dell Protected Workspace Management Server

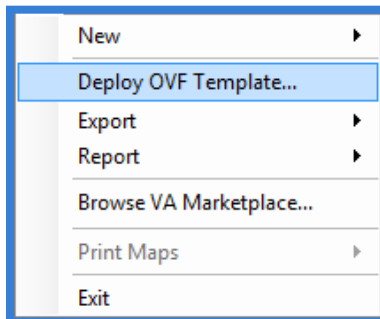
The Dell Protected Workspace Management Server is delivered as a virtual machine, in the VMware OVF template format. The following instructions outline how to install the DPWMS on either VMware vSphere 4.x or later or VMware Workstation 7.1.x or later. Some steps may differ slightly based on the version being used. The following instructions assume that the latest DPWMS template has been downloaded from the Dell.

Installation on VMware vSphere 4.x or later

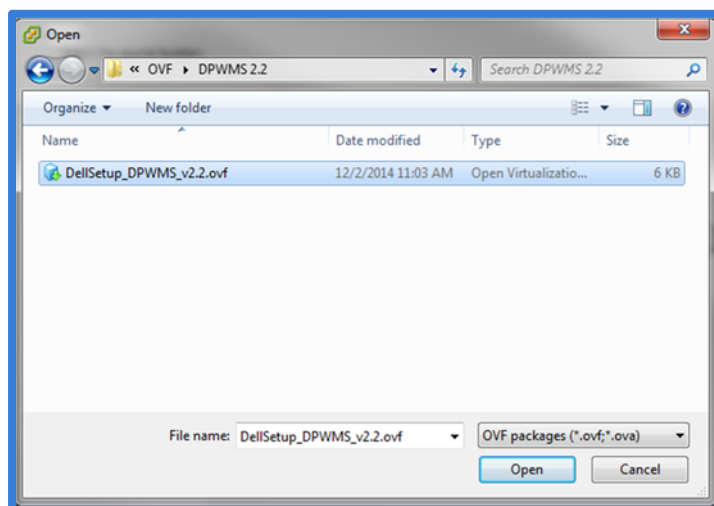
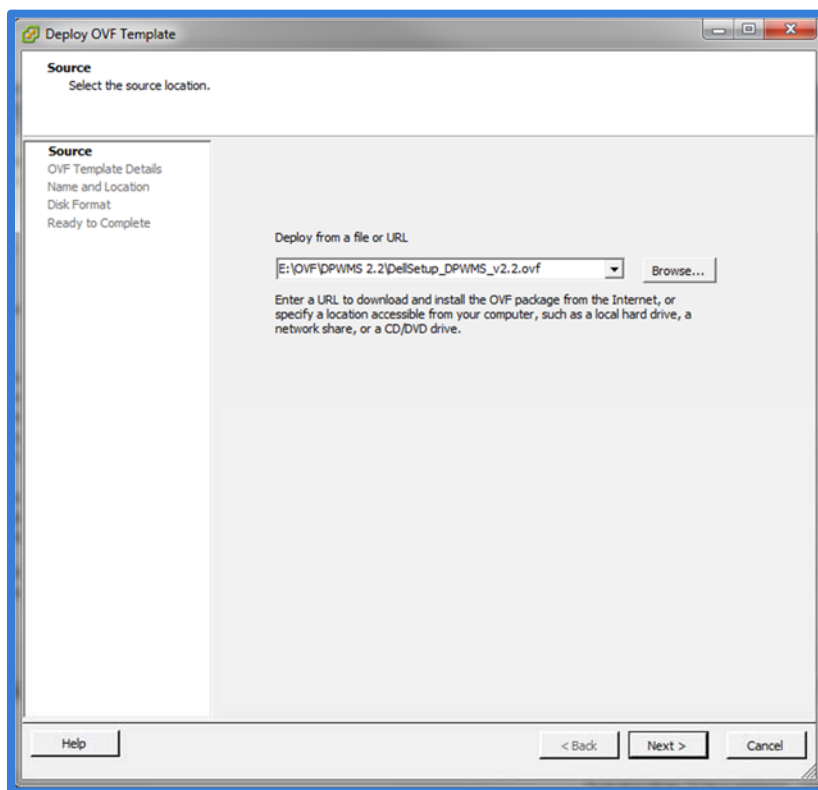
1. Open the VMware vSphere Client and connect to the ESX(i) or vCenter system that the DPWMS will be installed on.



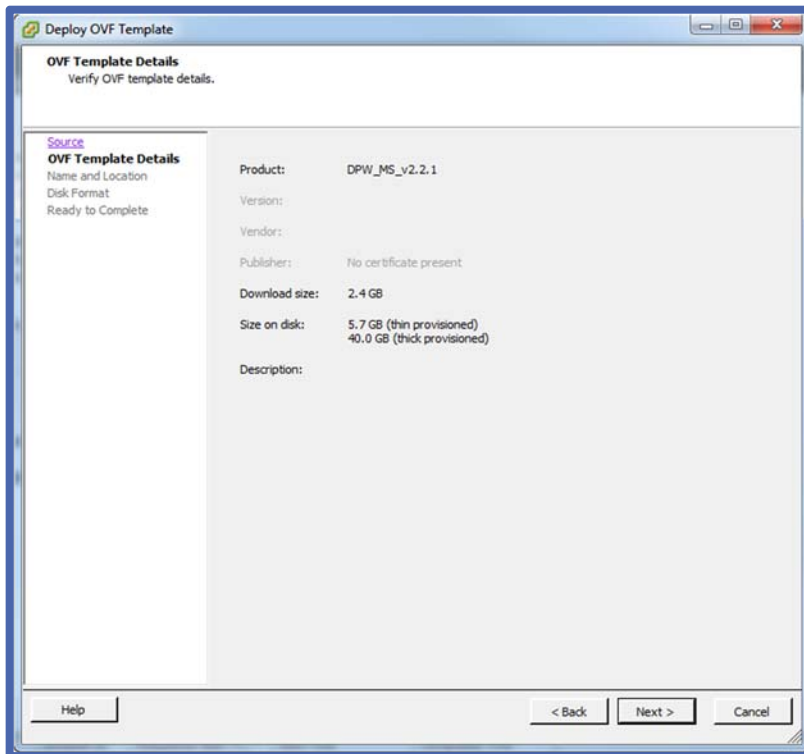
2. Select the File menu and choose “Deploy OVF Template...”



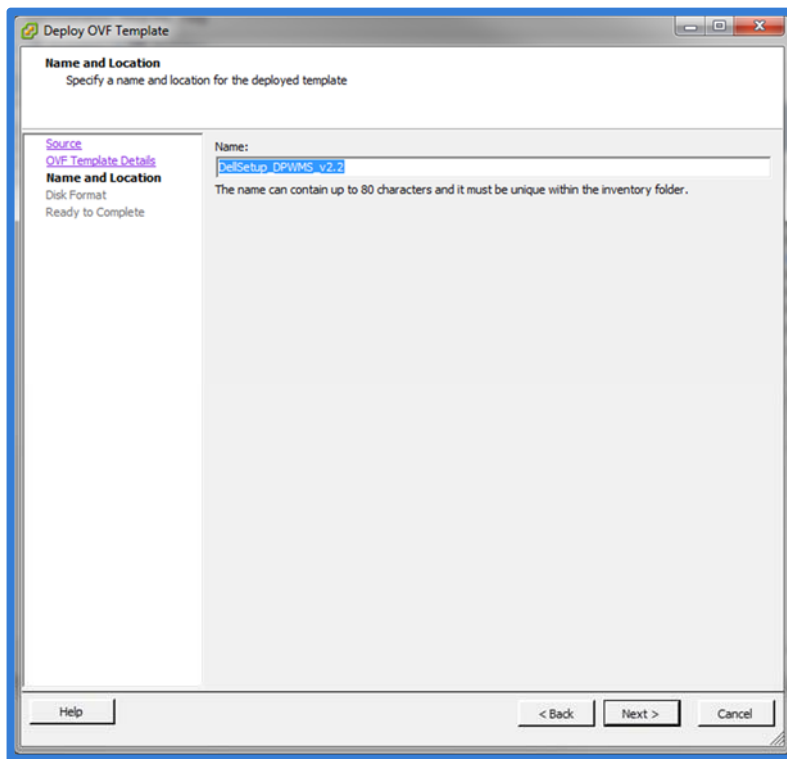
3. Choose the file location of the OVF template (the download must be unzipped before this step). Press the “Next” button.



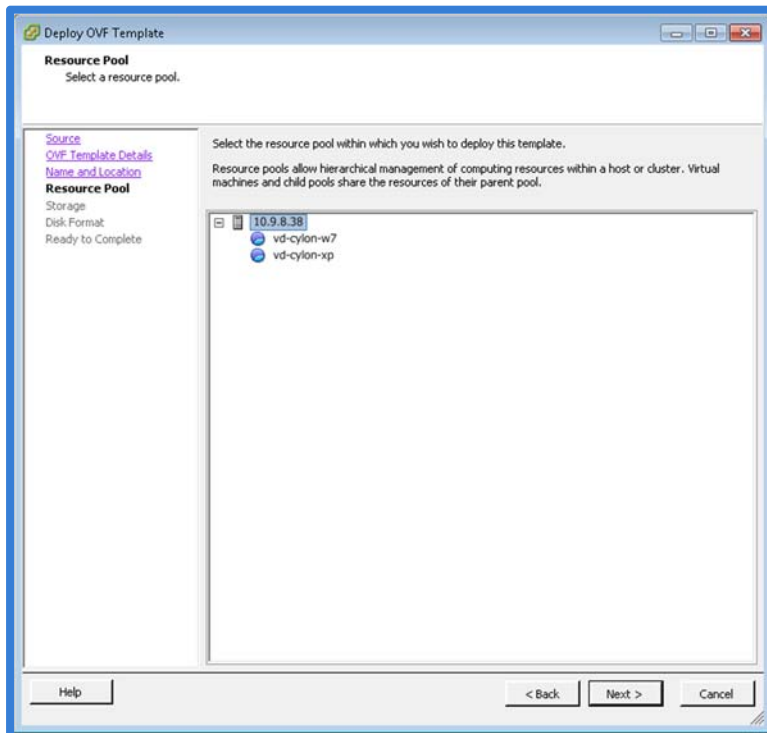
- Review the OVF information. Press the “Next” button.



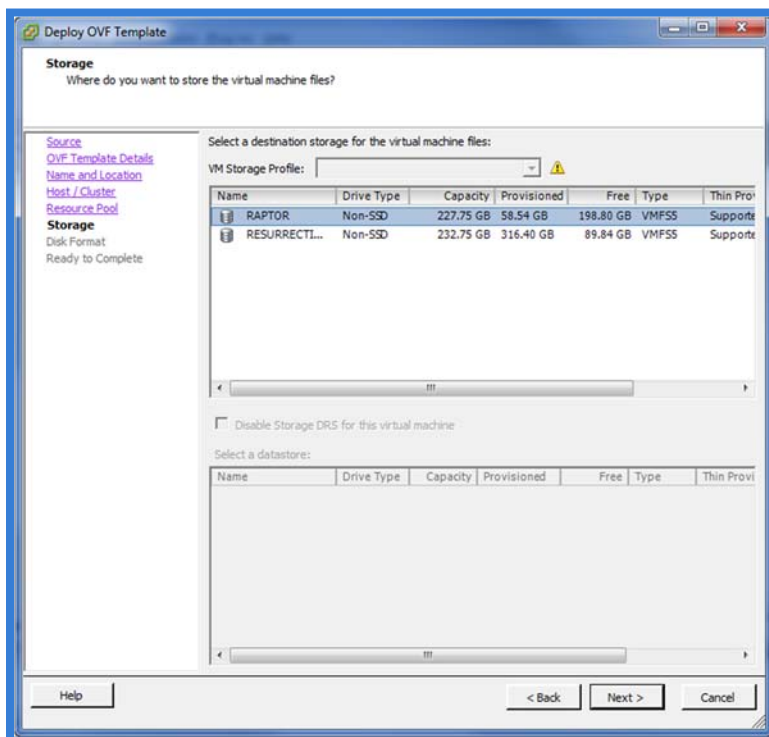
- Give the virtual machine a name (or use the default one provided). Choose which datacenter/folder the VM will be deployed to (if applicable). Press the “Next” button.



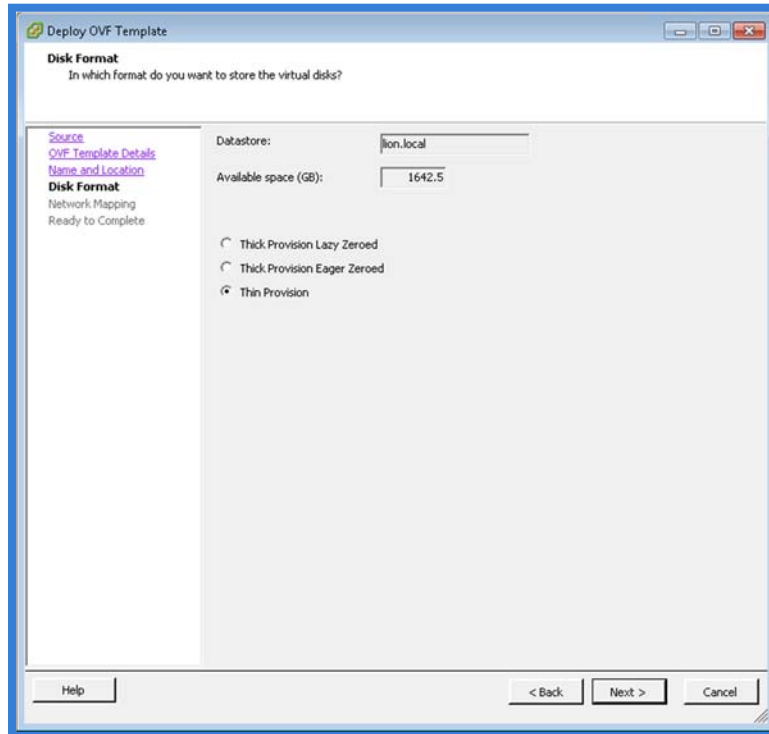
- For clustered systems, choose which cluster/host the VM will be deployed on. Press the “Next” button.



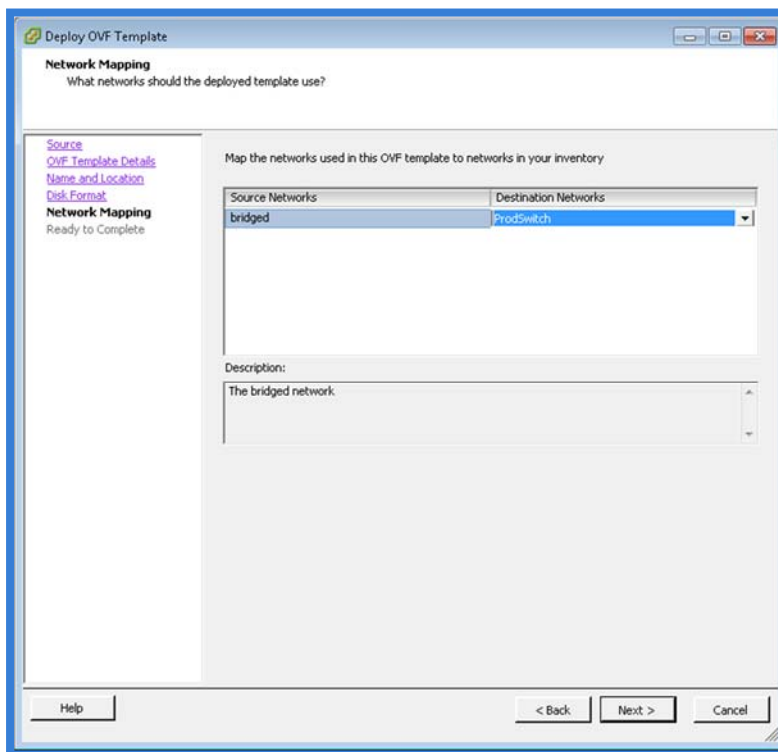
- If multiple datastores are available, choose the datastore to deploy the VM on. Press the “Next” button.



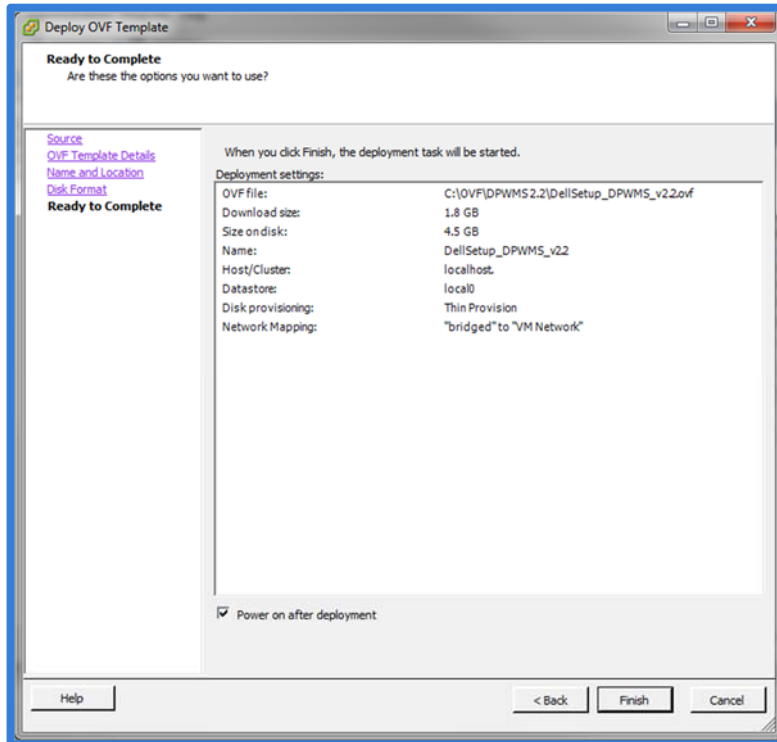
- Choose the desired disk format for the virtual disk. Press the “Next” button.



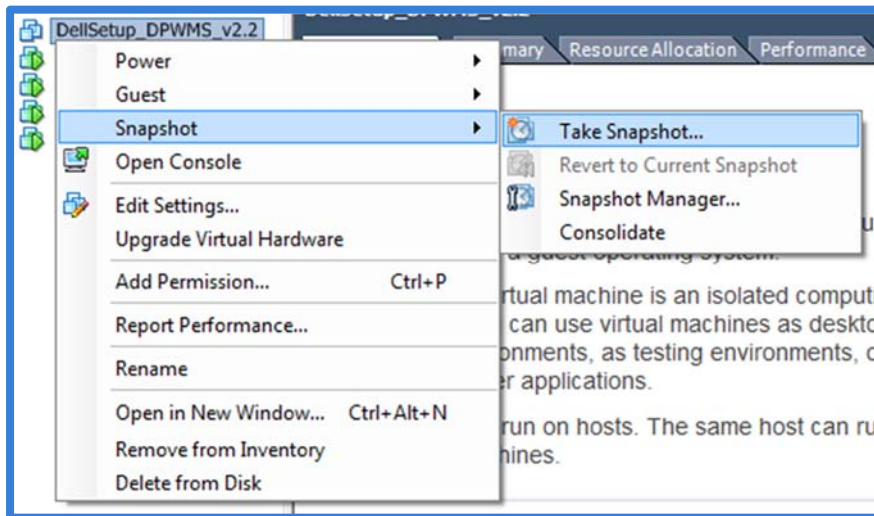
- Select the network that the VM will be connected to. Press the “Next” button.



10. Verify your configuration and press the “Finish” button.



11. Optional step: Once the OVF template has finished deploying, take a snapshot of the VM to retain the original settings before any configuration is done.



12. Power on the VM.

13. Installation of the DPWMS is now complete. Please continue to the [“Configuring the Dell Protected Workspace Management Server for Basic Operation”](#) section.

Installing VMware Tools for DPWMS running in a vSphere Environment

To install VMware Tools into the DPWMS appliance, follow these steps.

1. Connect to the console of the DPWMS from the vSphere client. Use the root account (default password is invincea)
2. From the VM menu, select Guest, then Install/Upgrade VMware Tools
3. Create a mount point for the cdrom by running the following command:

```
mkdir /mnt/cdrom
```

```
[root@ims ~]# mkdir /mnt/cdrom  
[root@ims ~]# _
```

4. Mount the VMware Tools image by running the following command:

```
mount /dev/cdrom /mnt/cdrom
```

```
[root@ims ~]# mkdir /mnt/cdrom  
[root@ims ~]# mount /dev/cdrom /mnt/cdrom  
mount: block device /dev/sr0 is write-protected, mounting read-only  
[root@ims ~]# _
```

5. Extract the tar file for VMware tools to the /var directory by running the following command:

```
tar xzf /mnt/cdrom/VMwareTools-X.X.X-YYYYYY.tar.gz -C /var/
```

```
[root@ims ~]# tar xzf /mnt/cdrom/VMwareTools-9.0.0-782409.tar.gz -C /var/_
```

NOTE: replace X.X.X-YYYYYY with the version number of the VMware Tools being installed

6. Change to the extracted directory by running the following command:

```
cd /var/vmware-tools-distrib/
```

```
[root@ims ~]# tar xzf /mnt/cdrom/VMwareTools-9.0.0-782409.tar.gz -C /var/  
[root@ims ~]# cd /var/vmware-tools-distrib/  
[root@ims vmware-tools-distrib]# _
```

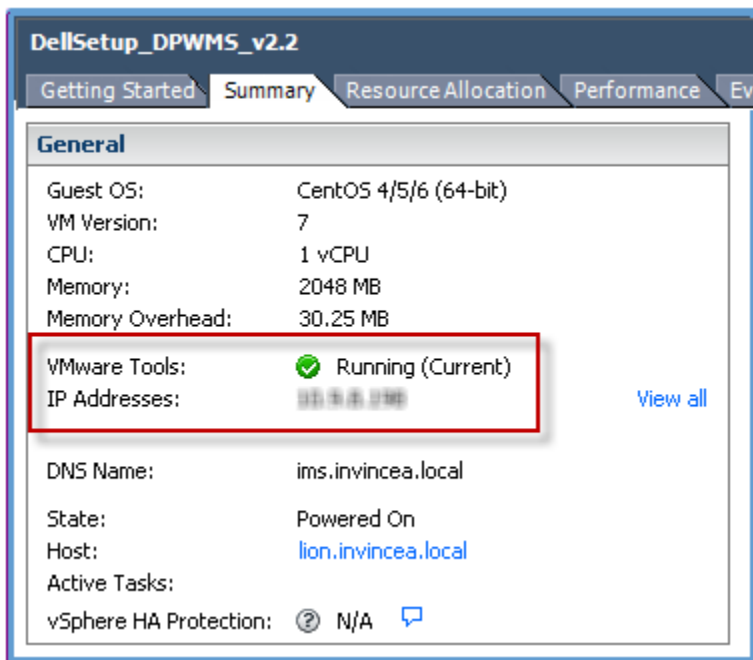
7. Run the VMware Tools installer script by running the following command:

```
./vmware-install.pl
```

```
[root@ims vmware-tools-distrib]# ./vmware-install.pl _
```

8. Follow the on-screen prompts and select the default setting for each option.

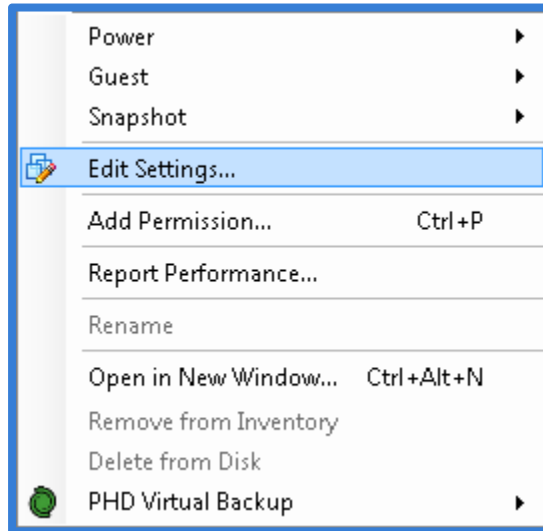
9. Confirm the installation was successful by viewing the details of the VM. A status of “VMware Tools: Running (Current)” should be displayed.



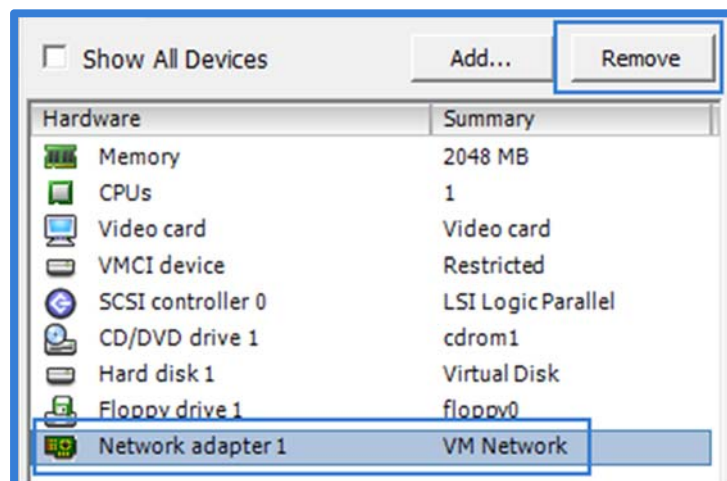
Upgrading the network adapter to VMXNET3 for DPWMS running in a vSphere Environment

In some VMware environments, changing the DPWMS appliance network adapter from the default E1000 adapter to a VMXNET3 adapter may be required. To change the appliance to the high-performance network adapter, follow these instructions.

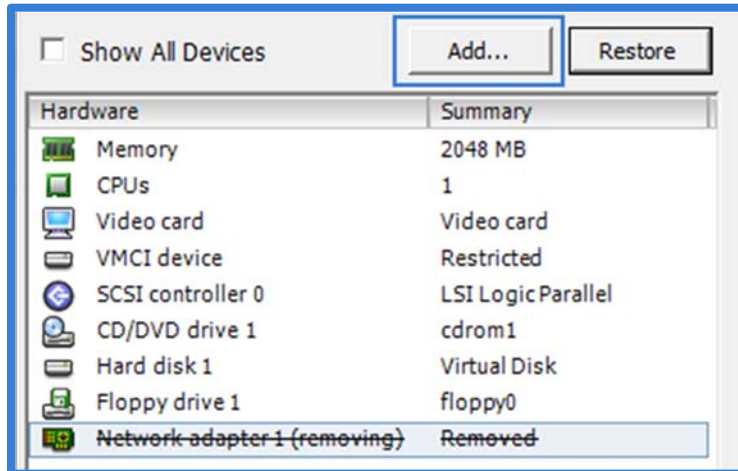
1. Connect to the DPWMS appliance VM via the vSphere console.
2. From the VM menu, choose Edit Settings



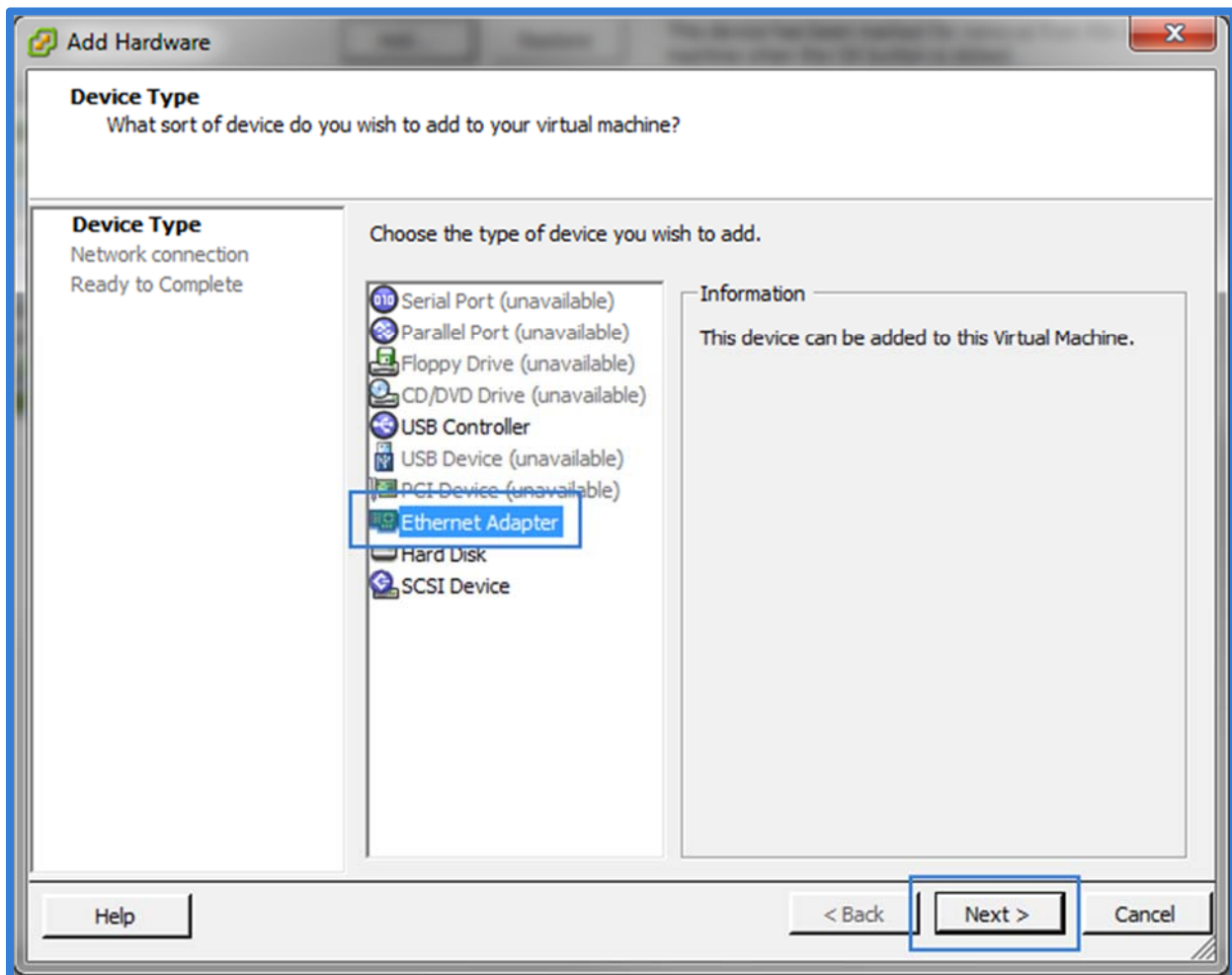
3. Select the “Network Adapter 1” device from the list and press the “Remove” button above the device list.



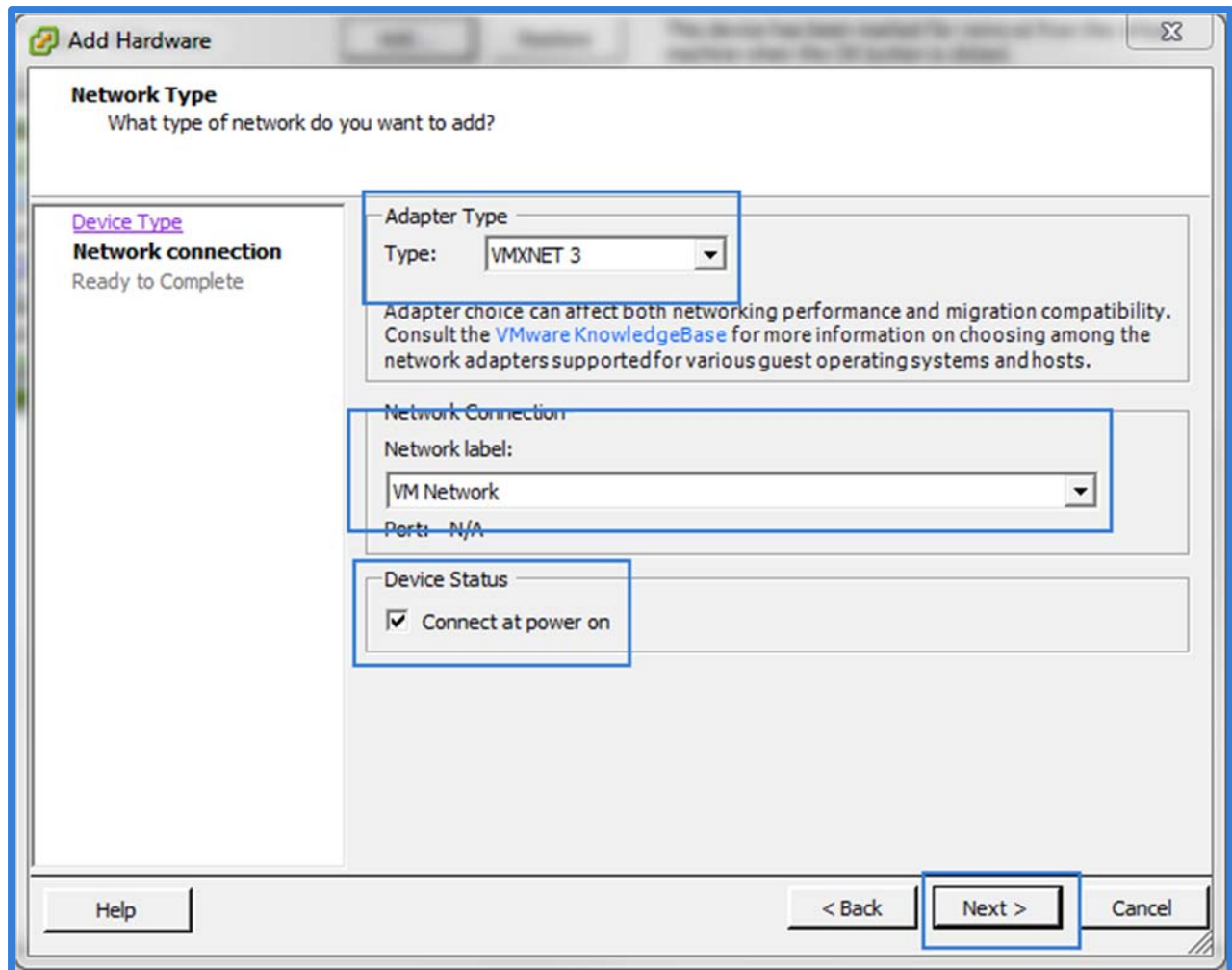
- Press the “Add” button above the device list.



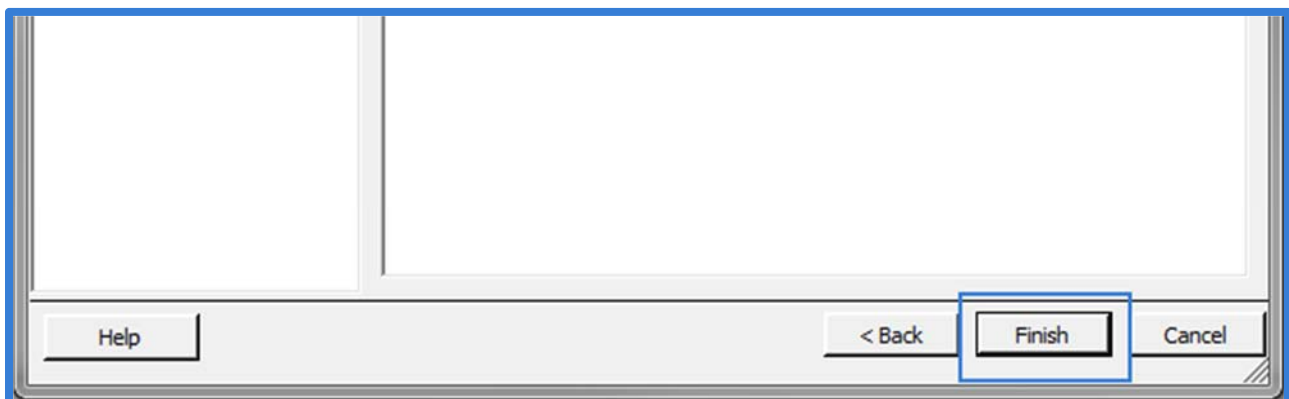
- Select “Ethernet Adapter” from the device list and then press the “Next” button.



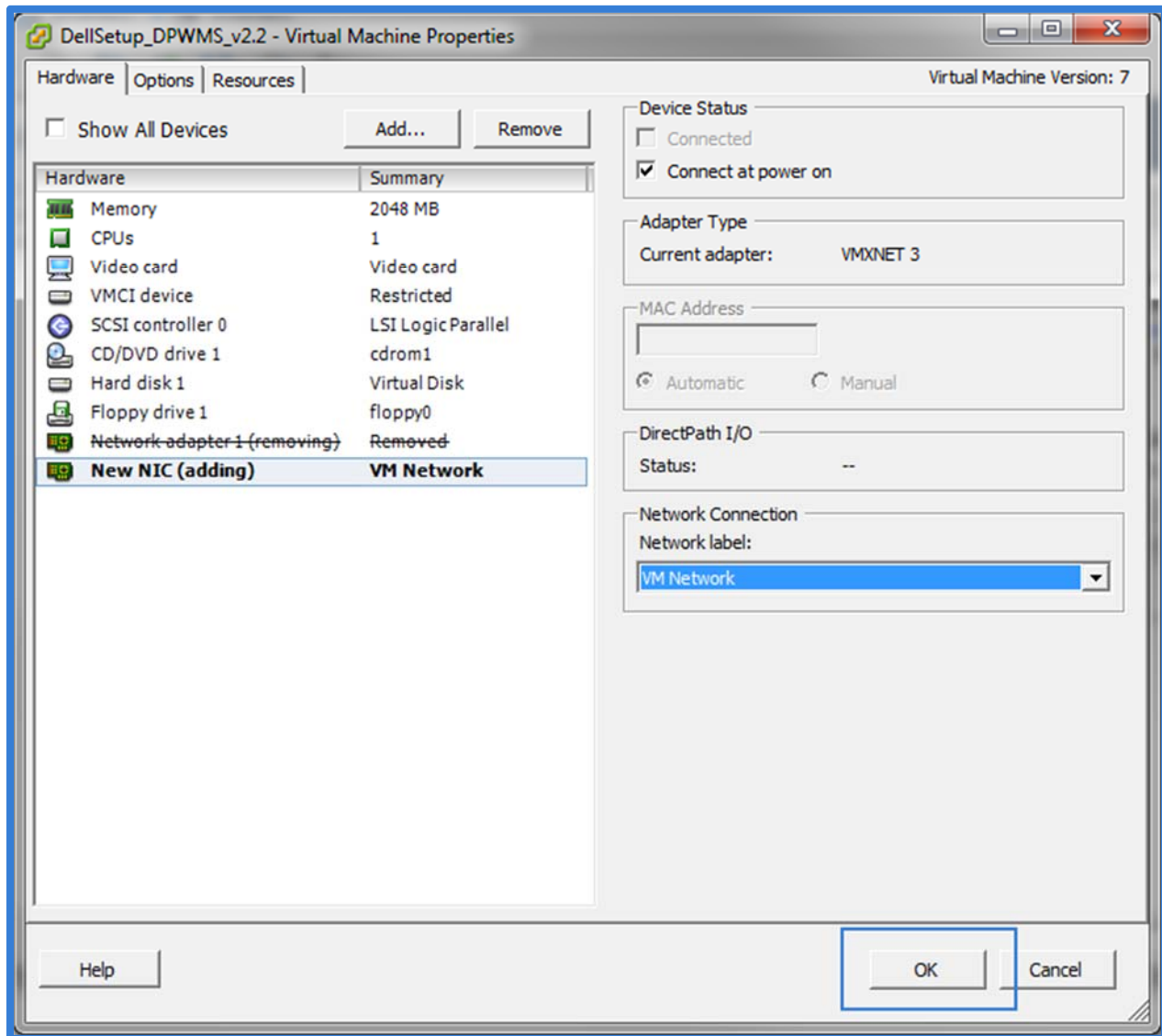
- From the Network Type window, select VMXNET 3 as the Adapter Type and select the correct network from the Network Connection drop-down. Also make sure the “Connect at power on” check box is selected. Press the “Next” button.



- Press the “Finish” button.



- Press the “OK” button.



9. From the console, log in as the root user and run the following command:

```
rm /etc/udev/rules.d/70-persistent-net.rules
```

```
[root@ims ~]# rm /etc/udev/rules.d/70-persistent-net.rules _
```

10. Confirm the delete process when prompted.

```
[root@ims ~]# rm /etc/udev/rules.d/70-persistent-net.rules  
rm: remove regular file '/etc/udev/rules.d/70-persistent-net.rules'? y_
```

11. Reboot the appliance by running the following command:

reboot

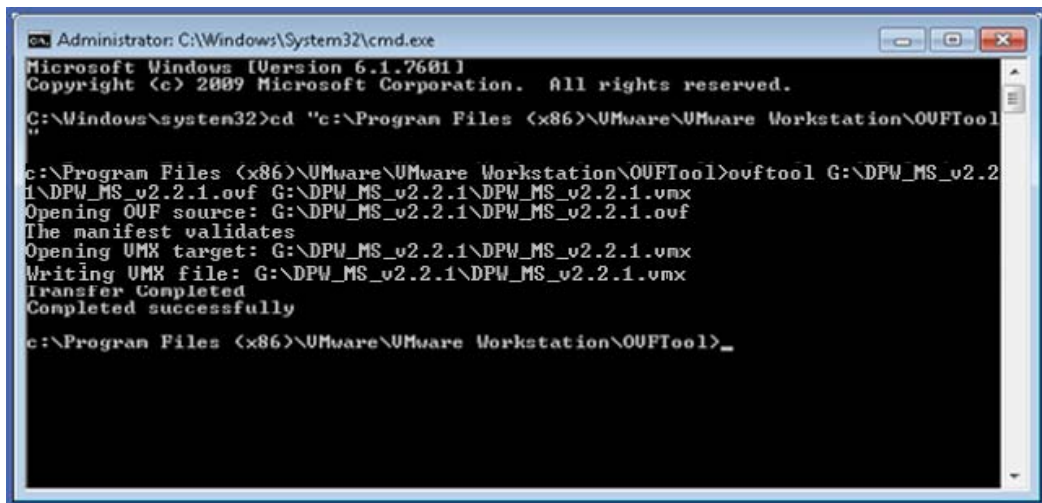
```
[root@ims ~]# rm /etc/udev/rules.d/70-persistent-net.rules
rm: remove regular file '/etc/udev/rules.d/70-persistent-net.rules'? y
[root@ims ~]# reboot_
```

12. Verify proper network connectivity after the system reboot.

Conversion of files for VMware Workstation 7 or 8

Before installation can begin on VMware Workstation version 7 or 8, the OVF file provided in the download must be converted to the correct format. The following steps will outline the proper steps for the conversion. The following steps also assume that VMware Workstation has already been installed.

1. Create a new folder where you want the virtual appliance to be stored on the host system. This will be used as the destination folder for the converted files.
2. Open a command prompt and navigate to the VMware Workstation installation folder (usually C:\Program Files (x86)\VMware\VMware Workstation\). Inside this folder, there is another folder called OVFTool. Navigate into this folder.
3. Use the ovftool.exe to convert the OVF file into the correct format using the following command (Note, the destination folder must exist before running the tool). File names are case sensitive.
 - a. `ovftool.exe <original ovf file location>.ovf <converted vmx file destination>.vmx`



```
Administrator: C:\Windows\System32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\system32>cd "c:\Program Files (x86)\VMware\VMware Workstation\OVFTool"

c:\Program Files (x86)\VMware\VMware Workstation\OVFTool>ovftool G:\DPW_MS_v2.2
1\DPW_MS_v2.2.1.ovf G:\DPW_MS_v2.2.1\DPW_MS_v2.2.1.vmx
Opening OVF source: G:\DPW_MS_v2.2.1\DPW_MS_v2.2.1.ovf
The manifest validates
Opening VMX target: G:\DPW_MS_v2.2.1\DPW_MS_v2.2.1.vmx
Writing VMX file: G:\DPW_MS_v2.2.1\DPW_MS_v2.2.1.vmx
Transfer Completed
Completed successfully

c:\Program Files (x86)\VMware\VMware Workstation\OVFTool>
```

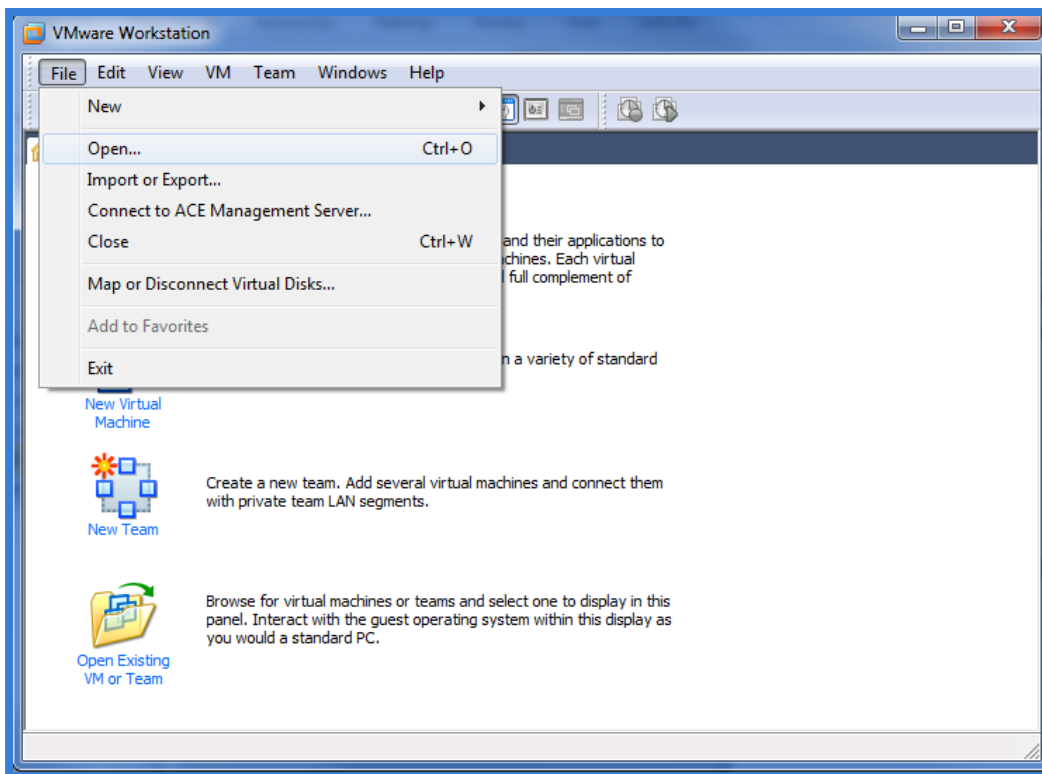
Example:

- b. `ovftool.exe C:\Users\Support\Documents\DPW_MS_v2.2.1\DPW_MS_v2.2.1.ovf
C:\Users\Support\Documents\DPW_MS_v2.2.1\DPW_MS_v2.2.1.vmx`
- c. This will create the converted VMX and VMDK files in the destination folder.

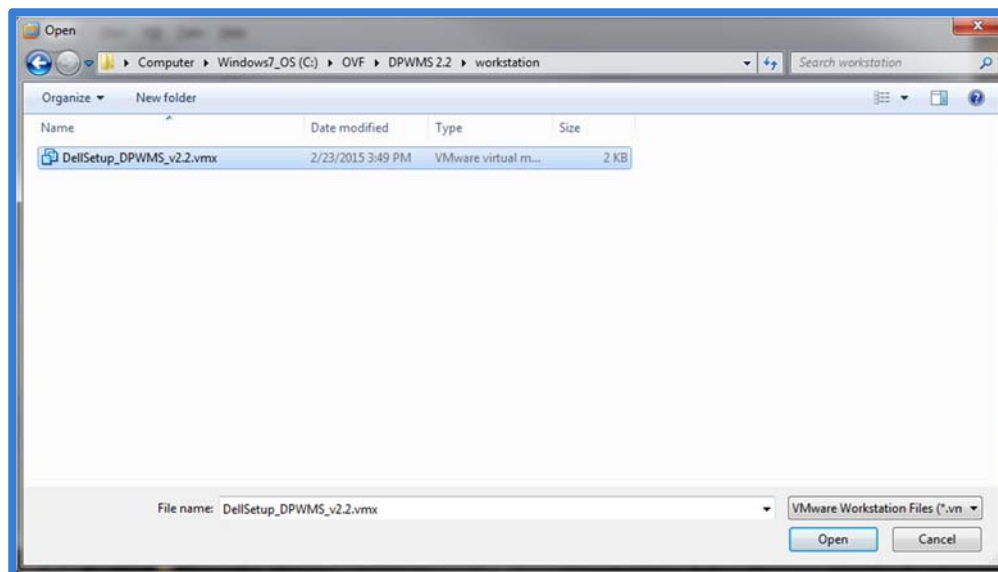
Note: VMware Workstation 9.x and later does not require this process. Simply use the Open command as outlined below and select the OVF file. VMware Workstation will do the conversion while opening the file.

Installing DPWMS on VMware Workstation 7.1.x or later

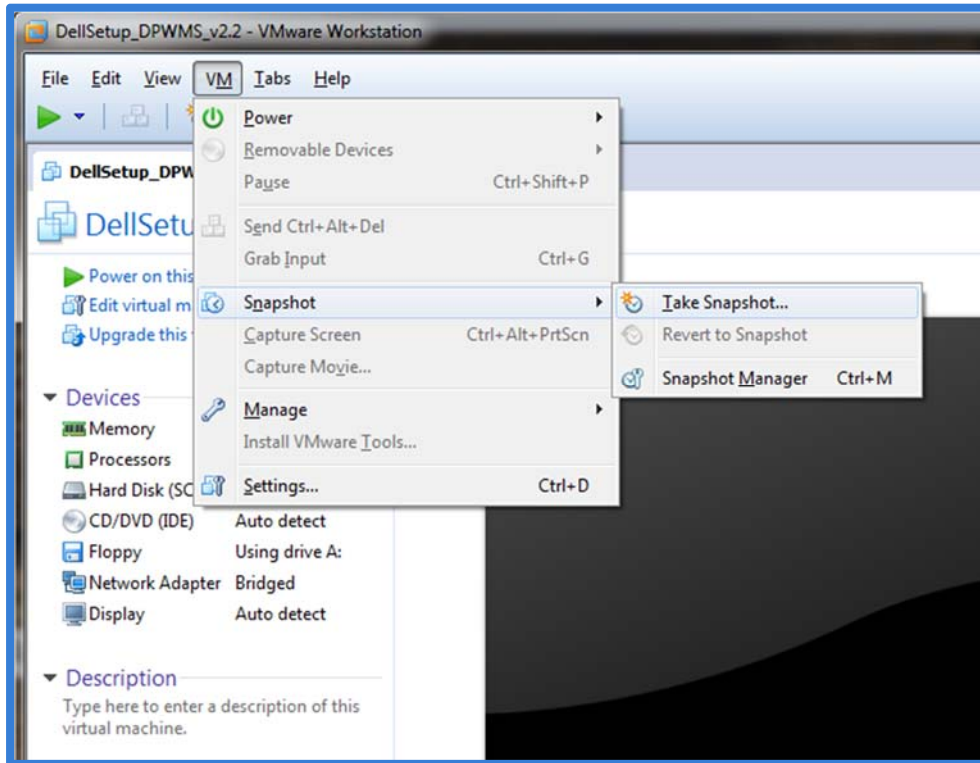
1. Open VMware Workstation. Select File → Open...



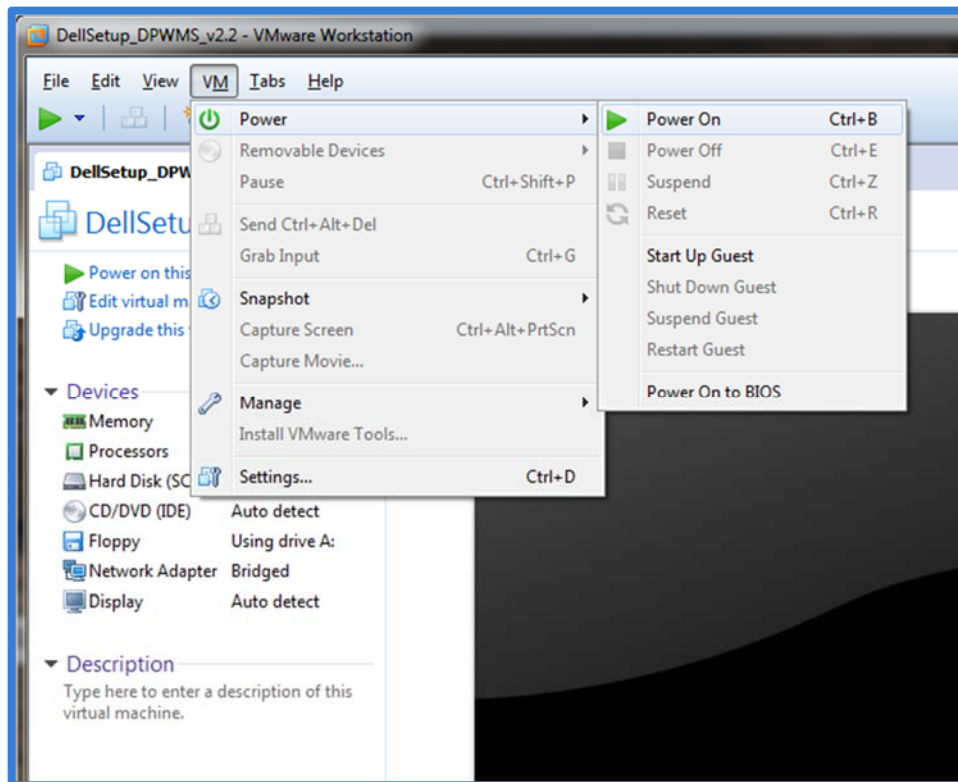
2. Browse to the location of extracted / converted files and select the <DPWMS file name>.vmx file (for Workstation 7 or 8). Choose Open.
 - a. For VMware Workstation 9 or later, select the OVF file.



- Optional step: Take a snapshot of the VM to retain the original settings before any configuration is done.



- Power on the DPWMS virtual machine and continue to the "[Configuring the Dell Protected Workspace Management Server for Basic Operation](#)" section.



Installing the DPWMS on Custom Hardware or a custom Virtual Machine

Installing the DPWMS and prerequisites

If administrators prefer to use their own version of Linux, a TGZ file is available for installation. Invincea uses CentOS 6.6 x86_64, but a similar Linux OS may be used (a 64-bit Linux OS is required). The DPWMS requires a MySQL database, either on the local system or on a remote system. The DPWMS also requires that the system has port 443 available through the local firewall for the DPWMS Console and API calls to work (assuming the recommended ports are used. This may vary based on custom configurations). The following packages are required for full system functionality (assuming RHEL or CentOS):

```
mysql-server
epel (only required if installing the next package via yum)
wine
```

The DPWMS can be installed via the tgz file supplied. A destination directory needs to be created first. It is recommended that the following directory be used: `/var/www/html/ims2`. Once the destination directory is created, the following command can be used to extract the components:

```
tar xzf dpwms-z.z.z-YYYYY.tgz -C /var/www/html/ims2
```

This assumes the recommended destination path is used and the DPWMS package is in the directory the command is being executed from.

Before the DPWMS can run, MySQL also needs to be installed on the host, as all DPWMS data is stored within a MySQL database. The database can be stored on a separate machine; however the default configuration file will need to be updated to point to the destination system. Also, a user name and password are necessary so the DPWMS process can connect to the mysql database. These will need to be entered into the `ims.conf` file.

Additionally, to support threat report uploads and package uploads, the `/etc/my.cnf` file needs to be modified to include the following under the `[mysqld]` section:

```
max_allowed_packet=150M
```

The default `my.cnf` included with the pre-built system contains the following:

```
[mysqld]
datadir=/var/lib/mysql
socket=/var/lib/mysql/mysql.sock
user=mysql
max_allowed_packet=150M

# Disabling symbolic-links is recommended to prevent assorted security risks
symbolic-links=0

[mysqld_safe]
log-error=/var/log/mysql.log
pid-file=/var/run/mysql/mysql.pid
```

Once the package and MySQL database are ready, following the steps in the [“Configuring the DPWMS SYSV startup script”](#) and [“Configuration the DPWMS configuration file”](#) sections.

Configuring the DPWMS SYSV startup script

In order to simplify and automate the startup of DPWMS, the following SYSV startup script can be added to the system.

Before creating the startup script, a change to the number of files a single process can access needs to be made. By increasing this limit, it allows the DPWMS process to handle a higher number of requests per API system. The file that needs to be modified is:

```
/etc/security/limits.conf
```

Using the vi command to edit this file, go to the end of the file and look for the following entries (the exact settings may vary):

```
root soft    nofile  4096
root hard    nofile  8192
```

Modify these entries by setting both limits to 65536. If the entries don't exist at all, add them as follows:

```
root soft    nofile  65536
root hard    nofile  65536
```

Save the file and exit the vi editor.

To create the startup script, start by creating the IMS2 startup file by running the following command as the root user:

```
vi /etc/init.d/ims2
```

While in the VI editor, go into "insert" mode by pressing the "i" (eye) key, then paste the following into the file:

```
#!/bin/sh
#
# ims2 - this script starts and stops the ims2.0 server
#
# chkconfig: 2345 95 20
# description: Invincea Management Server
# processname: main

# Source function library.
. /etc/init.d/functions

# Source networking configuration
. /etc/sysconfig/network

# Check that networking is up
[ "$NETWORKING" = "no" ] && exit 0

CONSOLE_OUTPUT=/var/log/ims2_console.log
IMS_PATH=/var/www/html/ims2
RUN="${IMS_PATH}"/run.sh

lockfile=/var/lock/subsys/ims2

start() {
    echo -n "Starting ims: "
    ulimit -n 65536
    cd $IMS_PATH && ($RUN >> $CONSOLE_OUTPUT 2>&1 &)
    retval=$?

    [ $retval -eq 0 ] && echo "started" && touch $lockfile
    return $retval
}

stop() {
    echo -n "Shutting down ims: "
```

```

killproc main
retval=$?
echo
[ $retval -eq 0 ] && rm -f $lockfile
return $retval
}

case "$1" in
start)
start
;;
stop)
stop
;;
status)
pgrep main > /dev/null 2>&1
status=$?
if [ $status -eq 0 ]; then
echo "running"
else
echo "not running"
fi
;;
restart)
stop
start
;;
reload)
stop
start
;;
*)
echo "Usage: <servicename> {start|stop|status|reload|restart}"
exit 1
;;
esac
exit $?

```

Save the file by typing “:wq!” This will close the file.

Now modify the permissions on the file by running the following command:

```
chmod a+x /etc/init.d/ims2
```

This now enables the DPWMS application to be started and stopped using the following options:

```

service ims2 start
service ims2 stop
service ims2 restart
service ims2 status

```

To set the DPWMS application to start with the OS starts (both for upgrades and new system installs), run the following command:

```
chkconfig ims2 on
```

Configuring the DPWMS configuration file

The DPWMS configuration file defines the necessary settings needed for the DPWMS to function, including port numbers, certificate locations, MySQL settings and logging settings. The configuration file is located at:

```
/var/www/html/ims2/ims.defaults (or ims.conf once the IMS has run at least once)
```

The following section reviews the configuration file and options. The virtual application defaults are listed, but can be modified to fit the needs of the environment:

[server]

This section defines the default server settings. It is important to properly define the port that the DPWMS UI will be available on and to define the SSL certificate location.

```
#port to use for http
#for https make sure ssl_cert and ssl_key are defined
port = 443 ← can be configured to any port, used to access the UI

#use 'localhost' to make server visible only to local machine
#use '0.0.0.0' to make server available publicly
host = 0.0.0.0 ← can be used to allow another process (such as Apache or Pound) to be the front-
end webserver, rather than running directly from the application.

#use this for SSL
#if all 3 items are not blank, SSL is used
ssl_cert = /etc/pki/tls/certs/dpwms.crt ← REQUIRED for SSL: provide path to crt file
ssl_key = /etc/pki/tls/private/dpwms.key ← REQUIRED for SSL: provide path to key file
# valid ssl_versions are ['SSLv3', 'SSLv23', 'TLSv1']
# if unspecified TLSv1 is used
ssl_version = TLSv1 ← REQUIRED for SSL: used to specify required client protocol

#use this to listen on another port but only expose the public request handlers
#(heartbeat, incident upload, etc.)
#will use SSL settings if specified above
api_port = ← this is the port that clients connect to, can be set to something else so that the UI
and API are on different ports. Leaving this blank means the UI and API will use the same port.

# enable FIPS mode for SSL
fips_enable = false ← used to enable FIPS for SSL connections

# set session timeout in seconds for UIclients
session_timeout = 86400 ← used to configure the timeout for DPWMS GUI before a user is logged
out

# the location of the admin tool (ie. Webmin)
# the string "localhost" will be replaced with the server hostname as the browser sees it
platform_admin = https://localhost:10000/ ← used to specify the URL for the "Platform
Administration Tool" on the Platform tab of the DPWMS GUI
```

[license]

```
#the license activation key to automatically attempt
activation_key = ← paste activation key here for automatic activation when the system starts
(prevents need to having to enter key into the UI)

#activation server url
server = http://delllicense.invincea.com/activate ← defines the URL that will be used to activate the
system with the supplied license key.
```

[mysql]

```
#mysql parameters
host = 127.0.0.1 ← defines the address for the MySQL server to use, default uses MySQL on local
system. If connecting to an external system, provide that systems IP address here.
port = 3306 ← defines the port to use to connect to MySQL. If going to an external system, this
port needs to be open on the local system firewall.
name = invincea2 ← name of database to use for the IMS
user = root ← username of user that has access to the above database on the selected MySQL server
pass = invincea ← password of the above user for access to the configured database
```

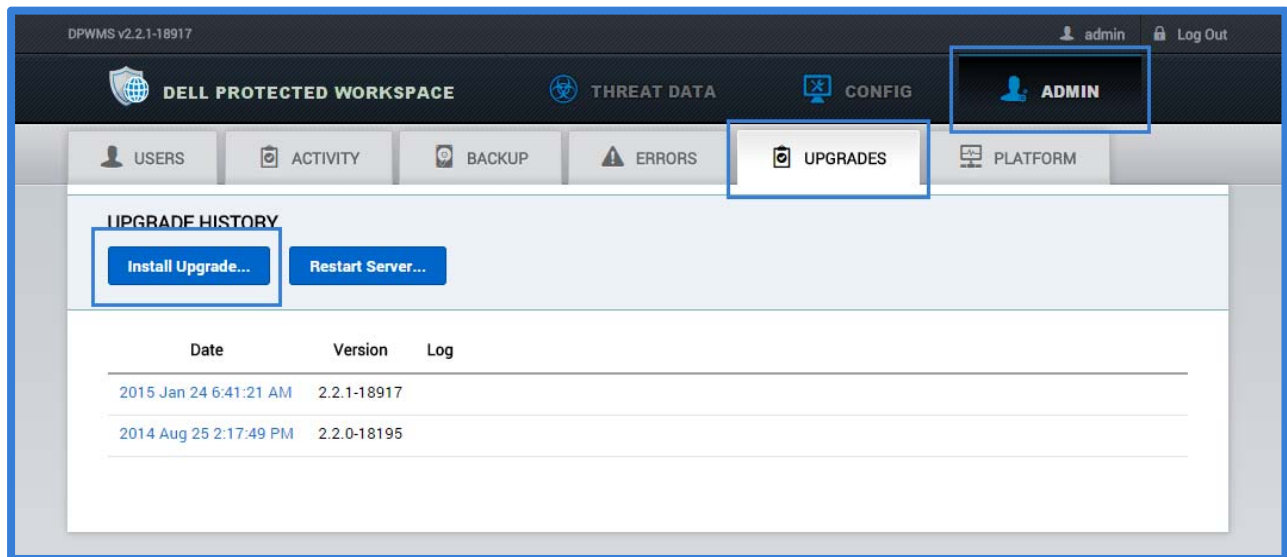
[logging]

```
file = ims.log ← name of file the DPWMS will log to within the install directory
level = DEBUG ← level of logging (available options: DEBUG, INFO, WARN, ERROR)
```

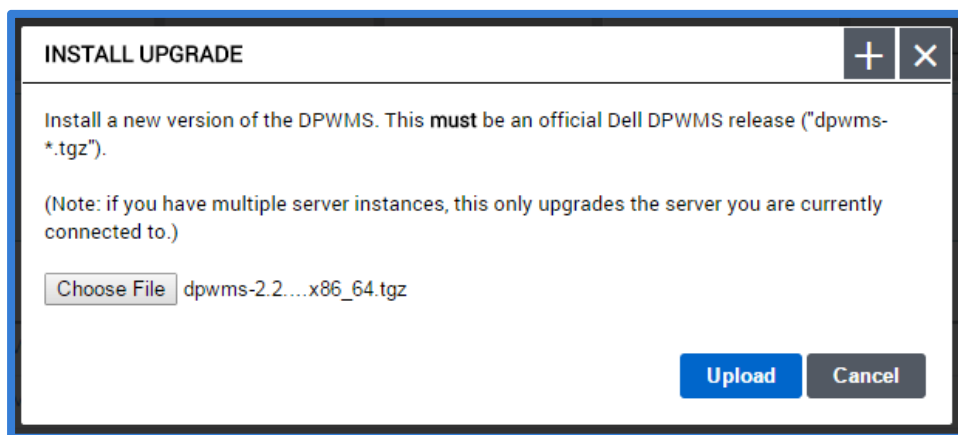
Applying New Updates via the UI

Server upgrades can now be done via the DPWMS management console for single API systems (multiple API systems must manually upgrade each API/UI system). The following steps outline the process to upgrade to a new DPWMS release.

1. Log into the DPWMS 2.x UI with an admin level account
2. From the Admin tab, click on the “Upgrades” tab
3. On the Upgrades tab, press the “Install Upgrade...” button

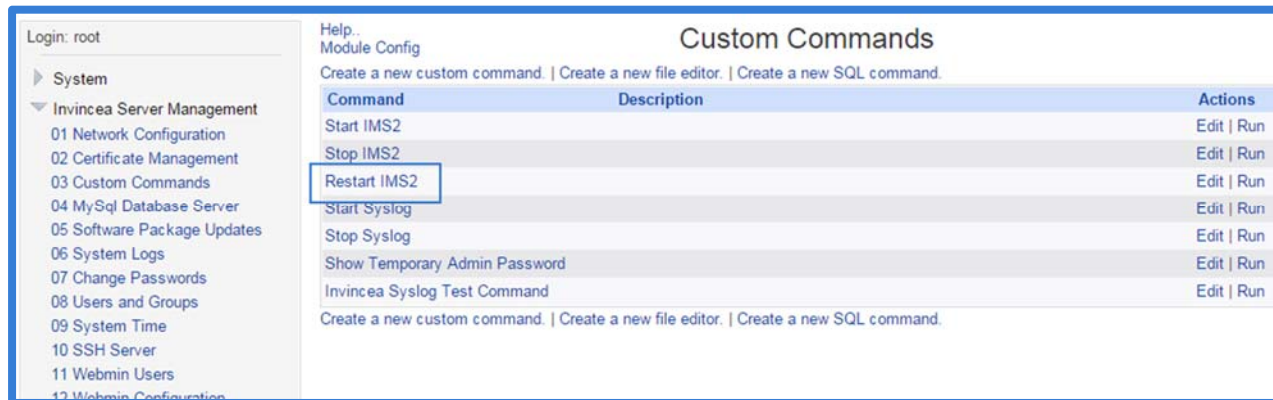


4. From the Install Upgrade dialog, browse to the downloaded tgz upgrade file (this file should be in the format: dpwms-y.y.y-xxxxx-x86_64.tgz)
5. After the file has been selected, press the “Upload” button



6. When the “Upload” button is pressed, the update will be uploaded to the server and applied, and once that has been finish, the DPWMS (ims2) service will restart. If the UI hangs or does not restart automatically, a manual restart of the DPWMS (ims2) service may be needed.
7. To restart the DPWMS (ims2) service manually, browse to the backend management page (port 10000) and go to the “03-Custom Commands” module.

- From the list of custom commands, click the “Restart IMS2” command



- Once the DPWMS (ims2) service restart has finished, return to the management console to access the upgraded system.

Manual Upgrade from via SSH/Console

In some environments, the upgrade process via the DPWMS UI may not work correctly if the upgrade package cannot copy to the DPWMS system before the allotted timeout or in cases where multiple API/UI systems exist. In these cases, the DPWMS upgrade will need to be applied manually by copying the update package to the server and unpacking it.

The following steps outline this procedure:

1. Using a tool such as WinSCP, connect to the server and transfer the DPWMS TGZ upgrade package to the /home/ims_admin directory
 - a. WinSCP uses the same credentials as SSH
 - b. The default port to connect to is 10022
 - c. The default credentials are ims_admin / invincea
2. Once the file has been successfully copied to the /home/ims_admin directory, run the following command to unpack the update:

```
tar xzf /home/ims_admin/dpwms-y.y.y-xxxxx-x86_64.tgz -C /var/www/html/ims2/
```

3. Once the unpack action is complete, the IMS service needs to be restarted to pick up the new settings. Run the following command to do that:

```
service ims2 restart
```

4. The upgrade process is now complete

NOTE: For systems that are running multiple API/UI servers, all DPWMS (ims2) services MUST be STOPPED before upgrading the first system. Once the first system is upgraded, all other systems MUST be upgraded before the system is brought back online.

Merging configuration file (ims.conf) changes after upgrade

After upgrading to a new version of the DPWMS, new configuration settings are enabled with “default” values that an admin may wish to change. In order to do this, new preferences from the “ims.default” file need to be copied into the active “ims.conf” file and configured with the correct settings.

Using a tool like Notepad ++, and admin can identify new settings that exist in the ims.defaults file (which displays all configurable options in the currently installed version).

```

ims.conf
6 port = 10443
7
8 #use 'localhost' to make server visible only to local machine
9 #use '0.0.0.0' to make server available publicly
10 host = 0.0.0.0
11
12 #use this for SSL
13 #if all 3 items are not blank, SSL is used
14 ssl_cert =
15 ssl_key =
16
17 #use this to listen on another port but only expose the public request
18 #(heartbeat, incident upload, etc.)
19 #will use SSL settings if specified above
20 api_port = 443
21
22 # enable FIPS mode for SSL
23 fips_enable = false
24
25 [license]
26
27 #the license activation key to automatically attempt
28 activation_key =
29
30 #activation server url
31 server = http://lic.invincea.com/activate
32
33 [mysql]
34 #mysql parameters
35 host =
36 port =
37 name =
38 user =
39 pass =
40
41 [logging]
42
43 file = ims.log
44 level = DEBUG
45

ims.defaults
6
7 #use 'localhost' to make server visible only to local machine
8 #use '0.0.0.0' to make server available publicly
9 host = 0.0.0.0
10
11 #use this for SSL
12 #if ssl_cert and ssl_key have values then SSL is used
13 ssl_cert =
14 ssl_key =
15 # valid ssl_versions are: ['SSLv3', 'SSLv23', 'TLSv1']
16 # if unspecified TLSv1 is used
17 ssl_version = TLSv1
18
19 #use this to listen on another port but only expose the public
20 #(heartbeat, incident upload, etc.)
21 #will use SSL settings if specified above
22 api_port =
23
24 # enable FIPS mode for SSL
25 fips_enable = true
26
27 # set session timeout in seconds for UI clients
28 session_timeout = 86400
29
30 # the location of the admin tool (ie. Webmin)
31 # the string "localhost" will be replaced with the server host
32 platform_admin = https://localhost:10000/
33
34 [license]
35
36 #the license activation key to automatically attempt
37 activation_key =
38
39 #activation server url
40 server = http://lic.invincea.com/activate
41
42 [mysql]
43 #mysql parameters

```

Configuring Secure Protocol for Client Connections

Starting with DPWMS 2.2, the required secure protocol for client connections can now be configured in the ims.conf file. Previous to DPWMS 2.2, TLS 1.0 was required to be enabled on client computers to enable communication to the DPWMS. This new feature now allows for TLS and SSL protocols.

By default, the DPWMS is still configured to require TLS 1.0, but this can be changed by modifying the following in the ims.conf file. This file is located in the root installation directory (default: /var/www/html/ims2/)

Under the [server] tag, the “ssl_version” tag can be set to the following:

- TLSv1 (default) = requires TLS 1.0 protocol to be enabled on clients
- SSLv3 = requires the SSL 3.0 protocol to be enabled on clients
- SSLv23 (supports the most protocols) = requires SSL 3.0 or TLS 1.0 to be enabled

NOTE: SSL v2 is not supported.

Configuring the Dell Protected Workspace Management Server for Basic Operation – Pre-Built Virtual Machine Only

Obtaining the DHCP Address of the System

By default, the DPWMS is configured to obtain a DHCP address. In order to continue with the configuration of the DPWMS, this address is needed so that the WebUI can be accessed.

To obtain the address of the system, open a console session to the server. At the login prompt, enter the following default credentials:

```
User: ims_admin
Password: invincea
```

```
ims login: ims_admin
Password:
Last login: Thu Jun  6 17:08:52 on tty1
[ims_admin@ims ~]$_
```

Once logged in, run the command:

```
[ims_admin@ims ~]# ifconfig
```

This will display the IP address for eth0. It is labeled as “inet addr:”

```
Kernel 2.6.32-358.6.2.el6.x86_64 on an x86_64
ims login: ims_admin
Password:
Last login: Thu Jun  6 16:48:56 on tty1
[ims_admin@ims ~]$_ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0C:29:AF:7F:8E
          inet addr:192.168.200.105  Bcast:192.168.200.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:feaf:7f8e/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:886 errors:0 dropped:0 overruns:0 frame:0
          TX packets:925 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:730430 (713.3 KiB)  TX bytes:61820 (60.3 KiB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:9 errors:0 dropped:0 overruns:0 frame:0
          TX packets:9 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:480 (480.0 b)  TX bytes:480 (480.0 b)

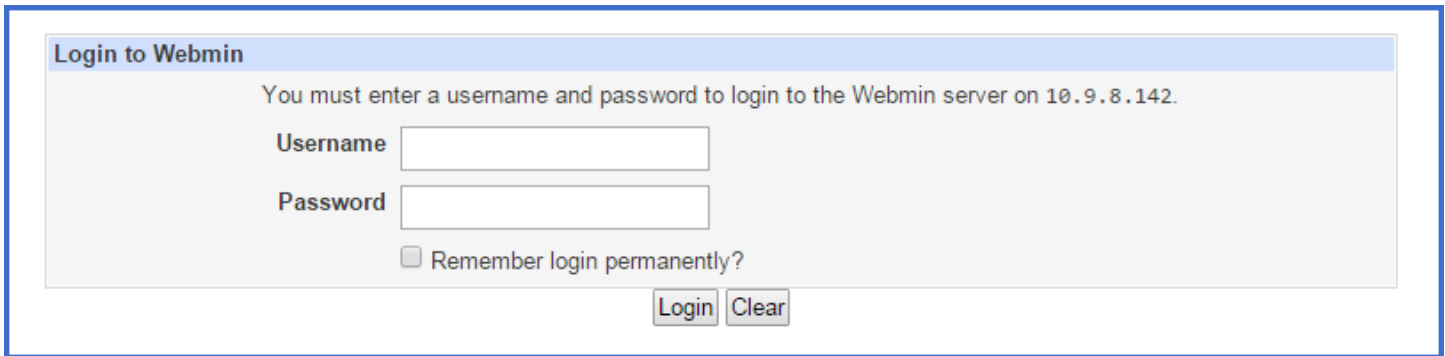
[ims_admin@ims ~]$_
```

Accessing the WebUI

The remaining initial configuration steps can be completed by accessing the Dell Protected Workspace Management Server WebUI. To access the WebUI, use a web browser to browse to the following address:

```
https://<system_IP_address>:10000
```

where <system_IP_address> is the one obtained in the last section. This address will be changed later in the setup. If prompted about an issue with the site certificate, choose “Continue to this website”.



Login to Webmin

You must enter a username and password to login to the Webmin server on 10.9.8.142.

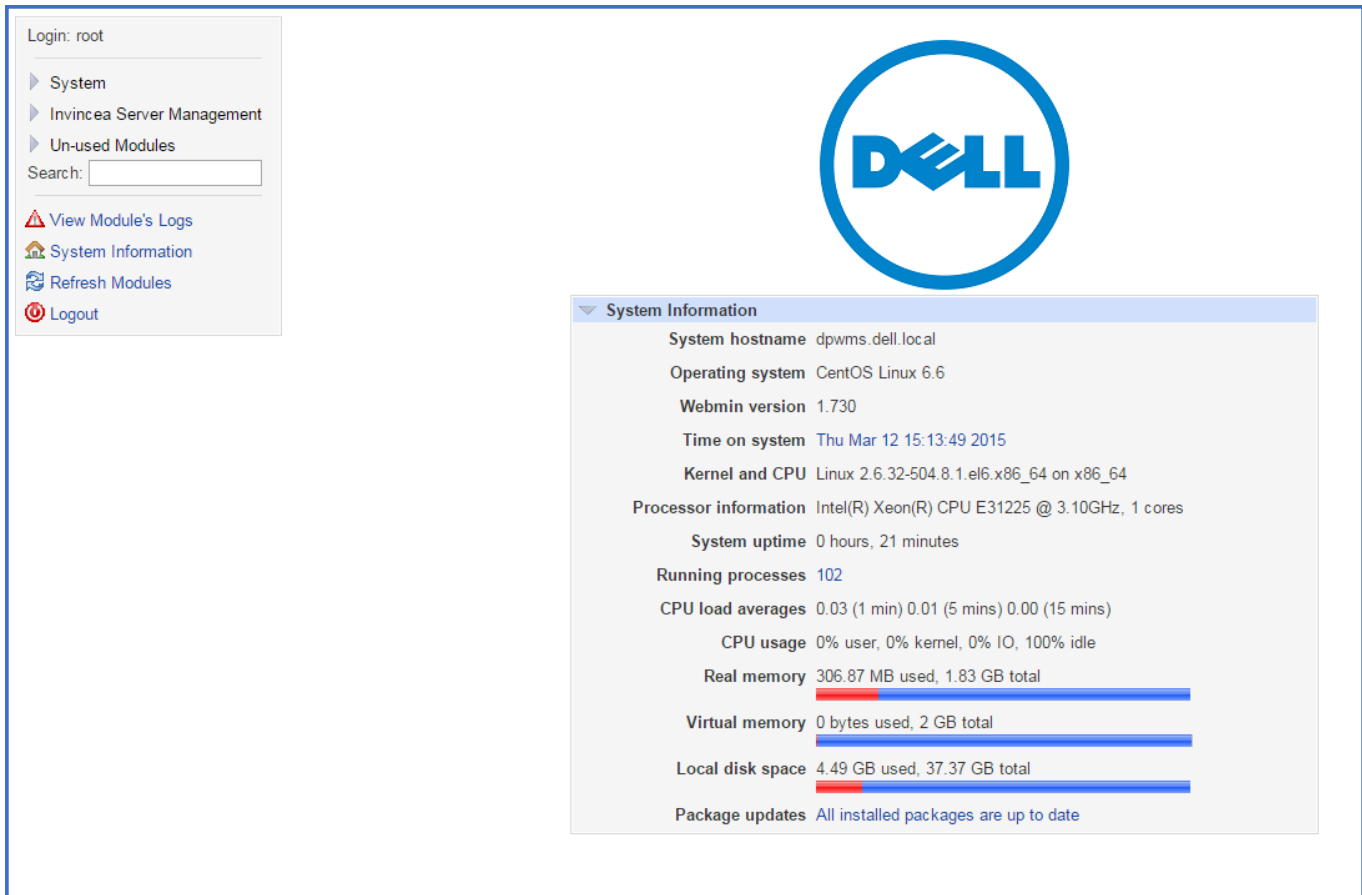
Username

Password

Remember login permanently?

At the login prompt, use the default credentials to log in to the WebUI. (ims_admin/invincea) Administrators should use ims_admin account for general DPWMS configuration. For advanced configuration, use the root account (root/invincea).

Once logged in, the DPWMS System Information Page will display:



System Information

System hostname dpwms.dell.local

Operating system CentOS Linux 6.6

Webmin version 1.730

Time on system Thu Mar 12 15:13:49 2015

Kernel and CPU Linux 2.6.32-504.8.1.el6.x86_64 on x86_64

Processor information Intel(R) Xeon(R) CPU E31225 @ 3.10GHz, 1 cores

System uptime 0 hours, 21 minutes

Running processes 102

CPU load averages 0.03 (1 min) 0.01 (5 mins) 0.00 (15 mins)

CPU usage 0% user, 0% kernel, 0% IO, 100% idle

Real memory 306.87 MB used, 1.83 GB total

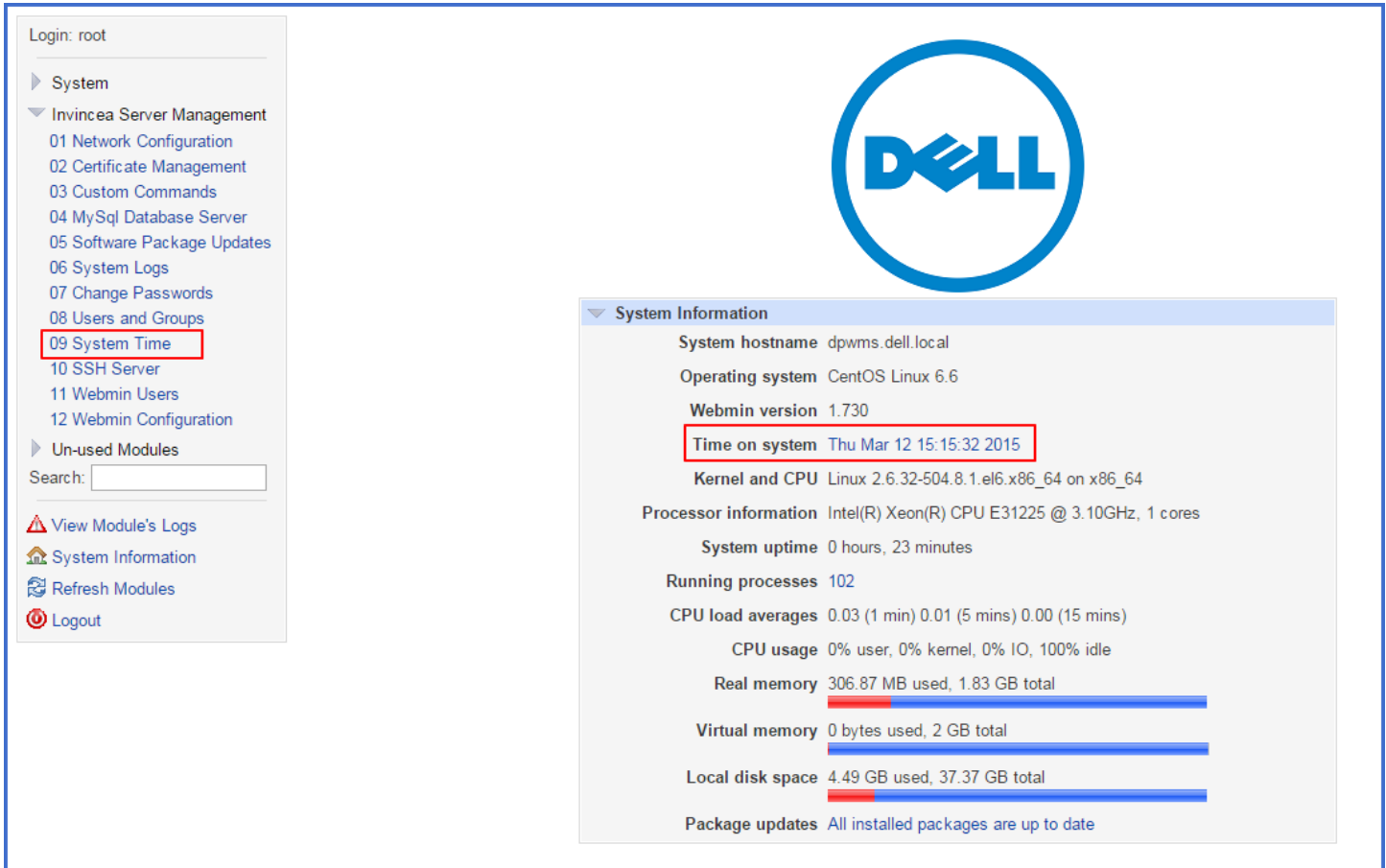
Virtual memory 0 bytes used, 2 GB total

Local disk space 4.49 GB used, 37.37 GB total

Package updates All installed packages are up to date

Changing the time or time zone

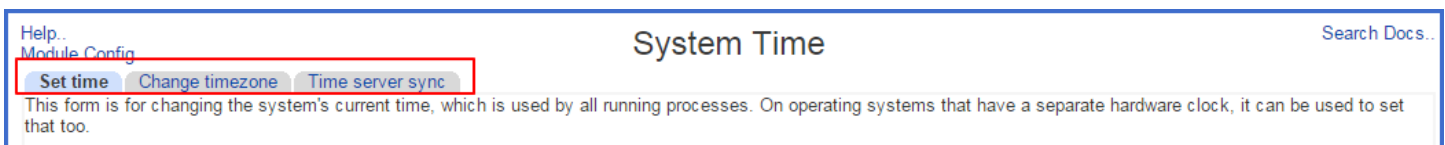
For the DPWMS to function properly, it is important that the system be configured with the correct date, time and time zone. The current date and time can be seen on the default landing page after logging into the WebUI. To modify these settings, select “09 System Time.”



The screenshot shows the Dell Protected Workspace Management Server WebUI. On the left sidebar, the menu item "09 System Time" is highlighted with a red box. The main content area displays the "System Information" page, which includes the following details:

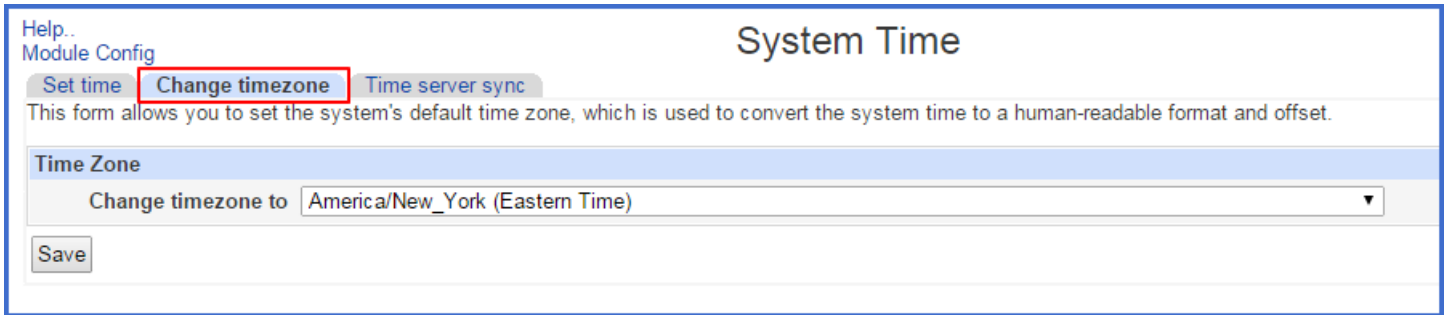
- System hostname: dpwms.dell.local
- Operating system: CentOS Linux 6.6
- Webmin version: 1.730
- Time on system: Thu Mar 12 15:15:32 2015 (highlighted with a red box)
- Kernel and CPU: Linux 2.6.32-504.8.1.el6.x86_64 on x86_64
- Processor information: Intel(R) Xeon(R) CPU E31225 @ 3.10GHz, 1 cores
- System uptime: 0 hours, 23 minutes
- Running processes: 102
- CPU load averages: 0.03 (1 min) 0.01 (5 mins) 0.00 (15 mins)
- CPU usage: 0% user, 0% kernel, 0% IO, 100% idle
- Real memory: 306.87 MB used, 1.83 GB total
- Virtual memory: 0 bytes used, 2 GB total
- Local disk space: 4.49 GB used, 37.37 GB total
- Package updates: All installed packages are up to date

The System Time page has three tabs at the top of the page: Set time, Change time zone and Time Server sync.



The screenshot shows the "System Time" page in the WebUI. The page title is "System Time" and there is a search bar for documentation. The "Set time" tab is highlighted with a red box. Below the tabs, there is a description: "This form is for changing the system's current time, which is used by all running processes. On operating systems that have a separate hardware clock, it can be used to set that too."

Start by setting the system to the correct time zone. The change time zone tab displays a drop-down box with the different time zones available to select from. Once the proper time zone has been selected, click Save.



Help..
Module Config

System Time

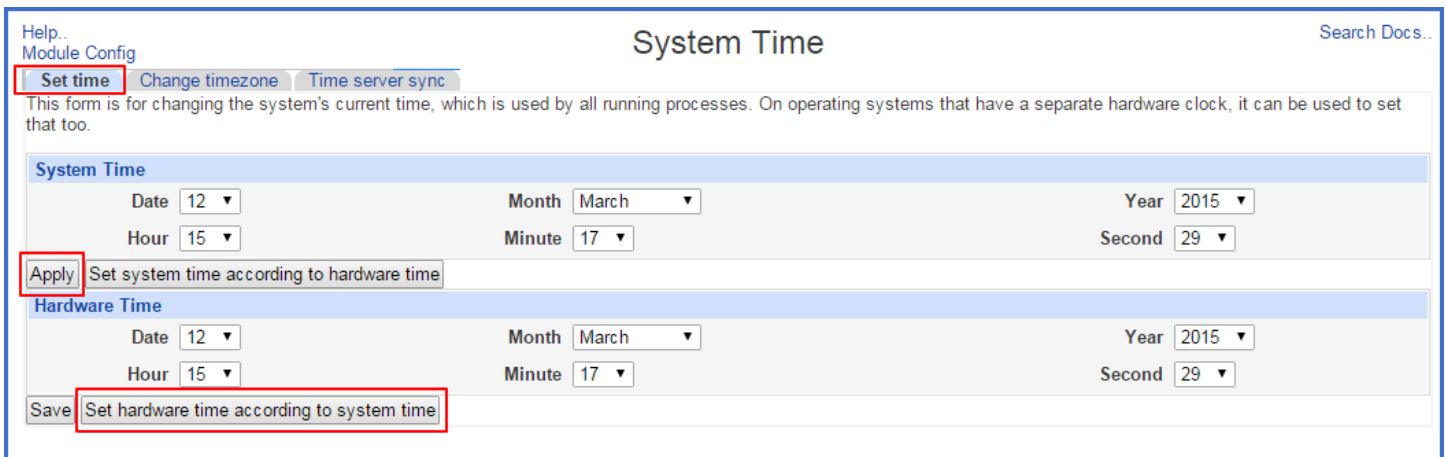
Set time **Change timezone** Time server sync

This form allows you to set the system's default time zone, which is used to convert the system time to a human-readable format and offset.

Time Zone

Change timezone to

From the Set time tab, the system and hardware time and date can be set. Set the System date and time first, pressing the apply button when finished. Next, press the Set hardware time to system time button to sync the hardware time.



Help.. Search Docs..
Module Config

System Time

Set time Change timezone Time server sync

This form is for changing the system's current time, which is used by all running processes. On operating systems that have a separate hardware clock, it can be used to set that too.

System Time

Date Month Year
Hour Minute Second

Set system time according to hardware time

Hardware Time

Date Month Year
Hour Minute Second

Set hardware time according to system time

The Time server sync tab lets administrators enter the name of a time server hostname or web address. Administrators also have the ability to set when the synchronization happens and the schedule by minutes, hours, days, months, and weekdays. Make sure to click Sync and Apply when finished making changes.

Help.. Search Docs..
 Module Config

System Time

This form is for configuring the system to automatically synchronize the time with a remote server. Synchronization will be done using the Unix `time` protocol or NTP, depending on which commands are installed and what the remote system supports.

Time Server

Set hardware time too

Synchronize when Webmin starts? Yes No

Synchronize on schedule? No Yes, at times below ..

Minutes	Hours	Days	Months	Weekdays
<input type="radio"/> All	<input type="radio"/> All	<input type="radio"/> All	<input checked="" type="radio"/> All	<input checked="" type="radio"/> All
<input checked="" type="radio"/> Selected ..	<input checked="" type="radio"/> Selected ..	<input type="radio"/> Selected ..	<input type="radio"/> Selected ..	<input type="radio"/> Selected ..
0 ▲ 12 ▲ 24 ▲ 36 ▲ 48 ▲ 1 13 25 37 49 ▲ 2 14 26 38 50 3 15 27 39 51 4 16 28 40 52 5 17 29 41 53 6 18 30 42 54 7 19 31 43 55 8 20 32 44 56 9 21 33 45 57 10 22 34 46 58 11 ▼ 23 ▼ 35 ▼ 47 ▼ 59 ▼	0 ▲ 12 ▲ 1 13 ▲ 2 14 3 15 4 16 5 17 6 18 7 19 8 20 9 21 10 22 11 ▼ 23 ▼	1 ▲ 13 ▲ 25 ▲ 2 14 26 ▲ 3 15 27 4 16 28 5 17 29 6 18 30 7 19 31 ▼ 8 20 9 21 10 22 11 ▼ 24 ▼	January ▲ February ▲ March April May June July August September October November December ▼	Sunday ▲ Monday Tuesday Wednesday Thursday Friday Saturday ▼

Network Configuration

The next task is to configure the network and DNS name of the system. To do this, select “01 Network Configuration” under the “Invincea Server Management” menu.

Module Config Search Docs..

Network Configuration

Network Interfaces Routing and Gateways Hostname and DNS Client Host Addresses

Apply Configuration Click this button to activate the current boot-time interface and routing settings, as they normally would be after a reboot. **Warning** - this may make your system inaccessible via the network, and cut off access to Webmin.

Click on the “Network Interfaces” icon to set the IP address of the system. Once in the configuration view click on “eth0” to set a static IP address for the network adapter. It is recommended that the system not be left with a DHCP address.

Module Index Network Interfaces

Active Now Activated at Boot

Interfaces listed in this table will be activated when the system boots up, and will generally be active now too.

Select all. | Invert selection. | Add a new interface. | Add a new bonding Interface. | Add Vlan Tagged Interface | Add a new bridge. | Add a new address range.

Name	Type	IPv4 address	Netmask	IPv6 address	Activate
<input checked="" type="checkbox"/> eth0	Ethernet	From DHCP	From DHCP		Yes
<input type="checkbox"/> lo	Loopback	127.0.0.1	255.0.0.0		Yes

Select all. | Invert selection. | Add a new interface. | Add a new bonding Interface. | Add Vlan Tagged Interface | Add a new bridge. | Add a new address range.

Delete Selected Interfaces Delete and Apply Selected Interfaces Apply Selected Interfaces

[Return to network configuration](#)

In the “Edit Bootup Interface” dialog for eth0, select the radio button for “Static Configuration” under IPv4 address and enter the assigned IP and netmask. Everything else can remain as default.

Boot Time Interface Parameters

Name eth0

Activate at boot? Yes No

IPv4 address No address configured
 From DHCP
 From BOOTP
 Static configuration

IPv4 address

Netmask

Broadcast Automatic

IPv6 addresses IPv6 disabled
 From IPv6 discovery
 Static configuration

IPv6 address	Netmask
<input type="text"/>	<input type="text" value="64"/>

MTU Default

Virtual interfaces 0 (Add virtual interface)

Hardware address Default

[Return to network interfaces](#)

Press the “Save” button when finished.

Now select the “Routing and Gateways” icon. On the “Boot time configuration tab”, select “eth0” as the interface under the Default route section. Then add the default gateway in the text box. Once that is entered, press Save. The WebUI will be directed back to the “Network Configuration” page when complete.

Boot time configuration Active configuration

This section allows you to configure the routes that are activated when the system boots up, or when network settings are fully re-applied.

Routing configuration activated at boot time

Default routes	Interface	Gateway	IPv6 gateway
	eth0	192.168.4.1	<input type="text"/>

Act as router? Yes No

Static routes	Interface	Network	Netmask	Gateway
	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>


Local routes	Interface	Network	Netmask
	<input type="text"/>	<input type="text"/>	<input type="text"/>

[Return to network configuration](#)


Once back on the Network Configuration page, press the “Apply Configuration” button.

Module Config Search Docs..


Network Configuration




Network Interfaces



Routing and Gateways



Hostname and DNS Client



Host Addresses

Apply Configuration

Click this button to activate the current boot-time interface and routing settings, as they normally would be after a reboot. **Warning** - this may make your system inaccessible via the network, and cut off access to Webmin.

After the settings have been applied, the browser needs to be pointed to the new address (either IP or DNS name). Once the login page loads on the new address, reenter the admin credentials, and navigate back to the “01 Network Configuration” dialog.

Next, select the “Hostname and DNS Client” icon. From the dialog, enter the new server name under host name (this needs to be the **Fully Qualified Domain Name**, host-only names will not work correctly), and enter the appropriate DNS servers and search domains.

Press the “Save” button when that is completed. The WebUI will be directed back to the “Network Configuration” page when complete.

Last, choose the “Host Addresses” icon from the Network Configuration page. Click on “Add a new host address.”

On the “Create Host Address” page, enter the IP address of the system in the “IP Address” box. Then, enter the Fully Qualified Domain Name of the system in the “Hostnames” box. Once they are entered, press the Create button.

On completion, the page will redirect back to the Host Addresses page. The new host address should now be listed.

Module Index Host Addresses

Select all. | Invert selection. | Add a new host address.

IP Address	Hostnames
<input type="checkbox"/> 127.0.0.1	localhost , localhost.localdomain , localhost4 , localhost4.localdomain4
<input type="checkbox"/> ::1	localhost , localhost.localdomain , localhost6 , localhost6.localdomain6
<input type="checkbox"/> 192.168.1.1	dpwms.dell.local

Select all. | Invert selection. | Add a new host address.

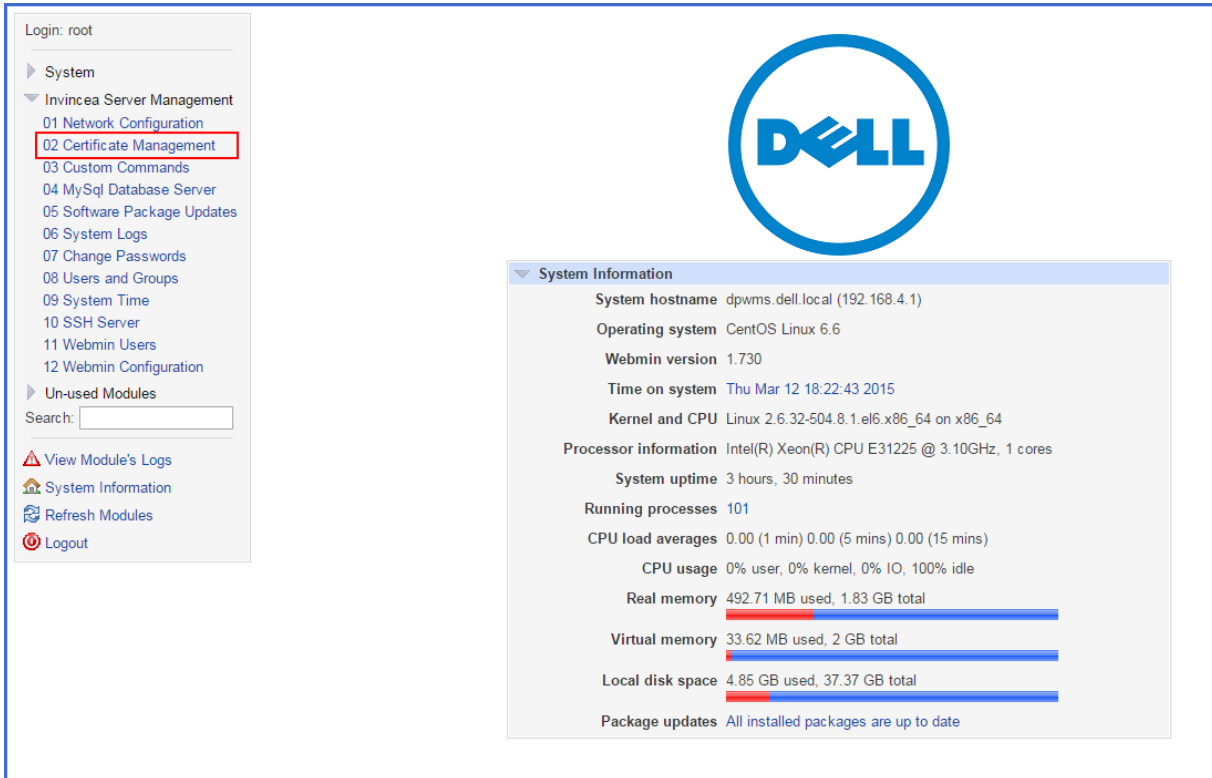
[← Return to network configuration](#)

The network configuration is now complete.

Self-Signed Certificate Creation

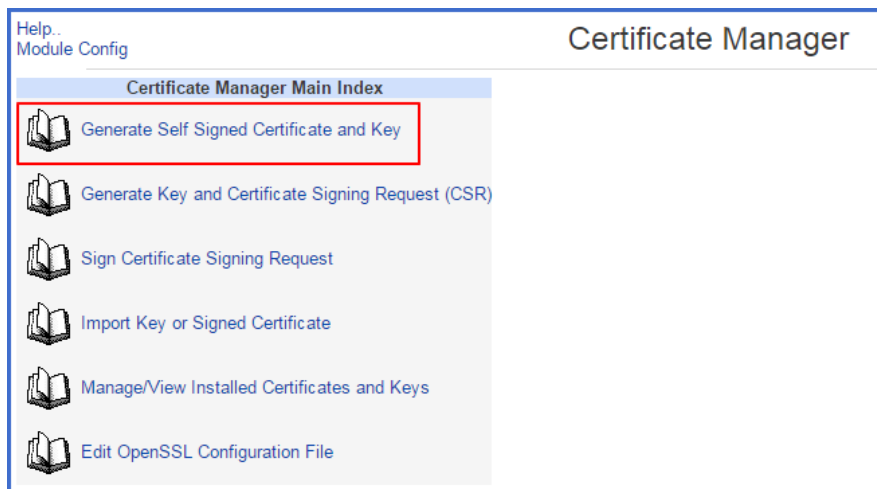
In order for the DPWMS to operate properly, a SSL certificate needs to be generated. The following steps outline the process for generating a self-signed certificate.

Start by selecting “02 Certificate Management” from the “Invincea Server Management” menu.



The screenshot shows the Invincea Server Management web interface. On the left, a navigation menu lists various system management tasks, with "02 Certificate Management" highlighted in red. The main content area displays system information for the host "dpwms.dell.local (192.168.4.1)". The system information includes details about the operating system (CentOS Linux 6.6), kernel and CPU (Linux 2.6.32-504.8.1.el6.x86_64 on x86_64), processor (Intel(R) Xeon(R) CPU E31225 @ 3.10GHz, 1 cores), system uptime (3 hours, 30 minutes), running processes (101), CPU load averages (0.00 (1 min) 0.00 (5 mins) 0.00 (15 mins)), CPU usage (0% user, 0% kernel, 0% IO, 100% idle), real memory (492.71 MB used, 1.83 GB total), virtual memory (33.62 MB used, 2 GB total), local disk space (4.85 GB used, 37.37 GB total), and package updates (All installed packages are up to date).

From the “Certificate Manager” page, click the “Generate Self Signed Certificate and Key” option.



The screenshot shows the Certificate Manager web interface. The main content area displays a list of options for certificate management, with "Generate Self Signed Certificate and Key" highlighted in red. The other options are "Generate Key and Certificate Signing Request (CSR)", "Sign Certificate Signing Request", "Import Key or Signed Certificate", "Manage/View Installed Certificates and Keys", and "Edit OpenSSL Configuration File".

Starting with the “Common Name (e.g. Host name)” field, fill out the information for the certificate. **Please note the fully qualified domain name MUST be entered for the product to work properly** (this should be automatically entered if the network configuration is correct, but should still be verified before continuing). The Key size should also be changed from 1024 to 2048.

Additionally, verify that the paths to the certificate files are correct before continuing. They should read as follows:

Certificate file name: /etc/pki/tls/certs/dpwms.crt
 Key file name: /etc/pki/tls/private/dpwms.key
 Key/Cert pair file name: /etc/pki/tls/private/dpwms.csr

Module Index Generate Certificate & Key

Note: If this key will be used as a server SSL key, any password entered here must be entered each time that an SSL service which uses this key is started. If you don't want to be required to provide the password each time, you may leave the password blank. However, anyone with root access to this machine can potentially take the key and decrypt any SSL traffic which uses this key.

Certificate Manager: Generate Self Signed Certificate and Key

Certificate file name	<input type="text" value="/etc/pki/tls/certs/dpwms.crt"/>
Key file name	<input type="text" value="/etc/pki/tls/private/dpwms.key"/>
Key/Certificate pair file name	<input type="text" value="/etc/pki/tls/private/hostkey+cert.pem"/>
Password	<input type="text"/>
Confirm Password	<input type="text"/>
Key size (in bits)	<input type="radio"/> 512 <input checked="" type="radio"/> 1024 <input type="radio"/> 2048
Certificate valid for (days)	<input type="text" value="730"/>
Common Name (eg. host name)	<input type="text" value="dpwms.dell.local"/>
Organization Name (eg. company)	<input type="text"/>
Organization Unit Name (eg. division)	<input type="text"/>
Locality (eg. city)	<input type="text"/>
State or Province (full name)	<input type="text"/>
Country (2 letter code)	<input type="text"/>
email Address (eg. webmaster@company.com)	<input type="text"/>

[Return to module index](#)

Once all of the information is filled out and verified, press the “Generate Key” button.

A confirmation page (displaying the old certificate that is about to be replaced) will display. Click the “Continue” button.

Module Index Generate Certificate & Key

/etc/pki/tls/certs/dpwms.crt	/etc/pki/tls/private/dpwms.key	Key size (in bits): 2048
Subject	Issuer	
dpwms.dell.local	dpwms.dell.local	
Issued on Mar 11 12:37:19 2015 GMT		
Expires on Mar 10 12:37:19 2017 GMT		

To download or view more information about a certificate or key, follow the link from its filename.

The above certificate(s) and/or key(s) will be replaced if you continue. Are you sure you wish to continue?

[Return to module index](#)

The new certificate has now been generated.

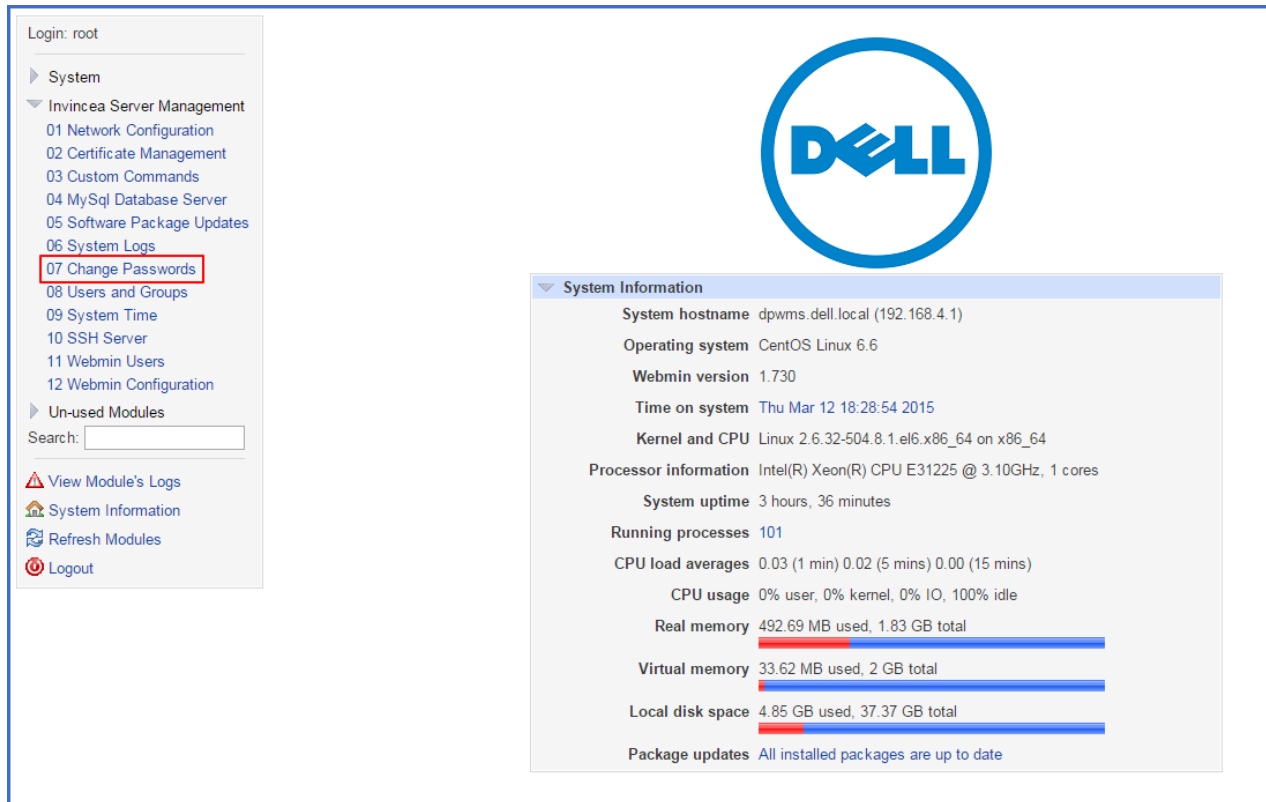
```
Module Index Generate Certificate & Key
Certificate and key generated
Generating a 1024 bit RSA private key
.....+++++
...+++++
writing new private key to '/etc/pki/tls/private/dpwms.key'
-----

The certificate was saved as /etc/pki/tls/certs/dpwms.crt
The key was saved as /etc/pki/tls/private/dpwms.key
The certificate+key file was saved as /etc/pki/tls/private/dpwms.key

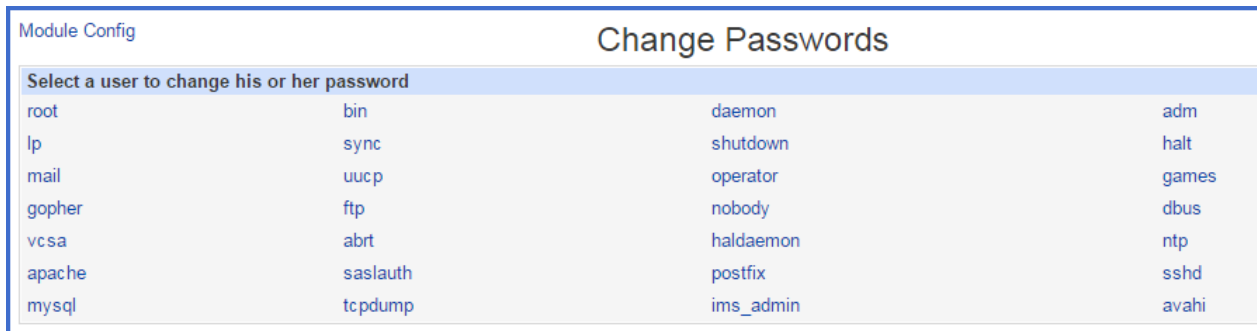
← Return to module index
```

Changing the root and ims_admin passwords

To change the passwords for the root and ims_admin user accounts, select the “07 Change Passwords” page from the “Invincea System Management” menu. Select “root” or “ims_admin” from the list of users.



The screenshot shows the Invincea System Management web interface. On the left, a navigation menu lists various system management tasks, with "07 Change Passwords" highlighted in red. The main content area features the Dell logo and a "System Information" section. This section provides details about the system, including the hostname (dpwms.dell.local), operating system (CentOS Linux 6.6), Webmin version (1.730), and system uptime (3 hours, 36 minutes). It also displays CPU load averages, CPU usage (0% user, 0% kernel, 0% IO, 100% idle), real memory usage (492.69 MB used, 1.83 GB total), virtual memory usage (33.62 MB used, 2 GB total), local disk space usage (4.85 GB used, 37.37 GB total), and package update status (All installed packages are up to date).



The screenshot shows the "Change Passwords" page in the Invincea System Management web interface. The page title is "Change Passwords" and it includes a "Module Config" section. Below this, there is a table titled "Select a user to change his or her password" with four columns of user names. The users listed are:

root	bin	daemon	adm
lp	sync	shutdown	halt
mail	uucp	operator	games
gopher	ftp	nobody	dbus
vcsa	abrt	haldaemon	ntp
apache	saslauth	postfix	sshd
mysql	tcpdump	ims_admin	avahi

Enter the new password in both fields and make sure the “Change passwords in other modules?” option is checked. Press the Change button to commit the new password.

The other user accounts are Linux system accounts and are not used to administer the DPWMS.

Additional Administrative Tasks

Modifying the default Firewall

In most cases the firewall will not need to be modified. However, if a custom firewall rule is needed or if a default rule needs to be removed, use the “Linux Firewall” page from the “Unused Modules” menu to make the modifications.

Incoming firewall rules should be added, changed or removed in the Chain RH-Firewall-1-INPUT section. Outgoing firewall rules should be added, changed or removed in the Chain RH-Firewall-1-OUTPUT section.

Chain RH-Firewall1-1-INPUT
Select all. | Invert selection.

Action	Condition	Move	Add
<input type="checkbox"/> Drop	If protocol is TCP and state of connection is NEW	↓	↓ ↑
<input type="checkbox"/> Accept	If input interface is lo	↓ ↑	↓ ↑
<input type="checkbox"/> Accept	If protocol is ICMP and ICMP type is echo-reply	↓ ↑	↓ ↑
<input type="checkbox"/> Accept	If protocol is ICMP and ICMP type is destination-unreachable	↓ ↑	↓ ↑
<input type="checkbox"/> Accept	If protocol is ICMP and ICMP type is source-quench	↓ ↑	↓ ↑
<input type="checkbox"/> Accept	If protocol is ICMP and ICMP type is redirect	↓ ↑	↓ ↑
<input type="checkbox"/> Accept	If protocol is ICMP and ICMP type is time-exceeded	↓ ↑	↓ ↑
<input type="checkbox"/> Accept	If protocol is ICMP and ICMP type is parameter-problem	↓ ↑	↓ ↑
<input type="checkbox"/> Accept	If protocol is ICMP and ICMP type is timestamp-reply	↓ ↑	↓ ↑
<input type="checkbox"/> Accept	If state of connection is ESTABLISHED,RELATED	↓ ↑	↓ ↑
<input type="checkbox"/> Accept	If protocol is UDP and destination port is 123 and state of connection is NEW	↓ ↑	↓ ↑
<input type="checkbox"/> Accept	If protocol is TCP and destination port is 443 and state of connection is NEW	↓ ↑	↓ ↑
<input type="checkbox"/> Accept	If protocol is TCP and destination port is 10443 and state of connection is NEW	↓ ↑	↓ ↑
<input type="checkbox"/> Accept	If protocol is TCP and destination port is 10022 and state of connection is NEW	↓ ↑	↓ ↑
<input type="checkbox"/> Accept	If protocol is TCP and destination port is 10000 and state of connection is NEW	↓ ↑	↓ ↑
<input type="checkbox"/> Drop	Always	↑	↓ ↑

Select all. | Invert selection.

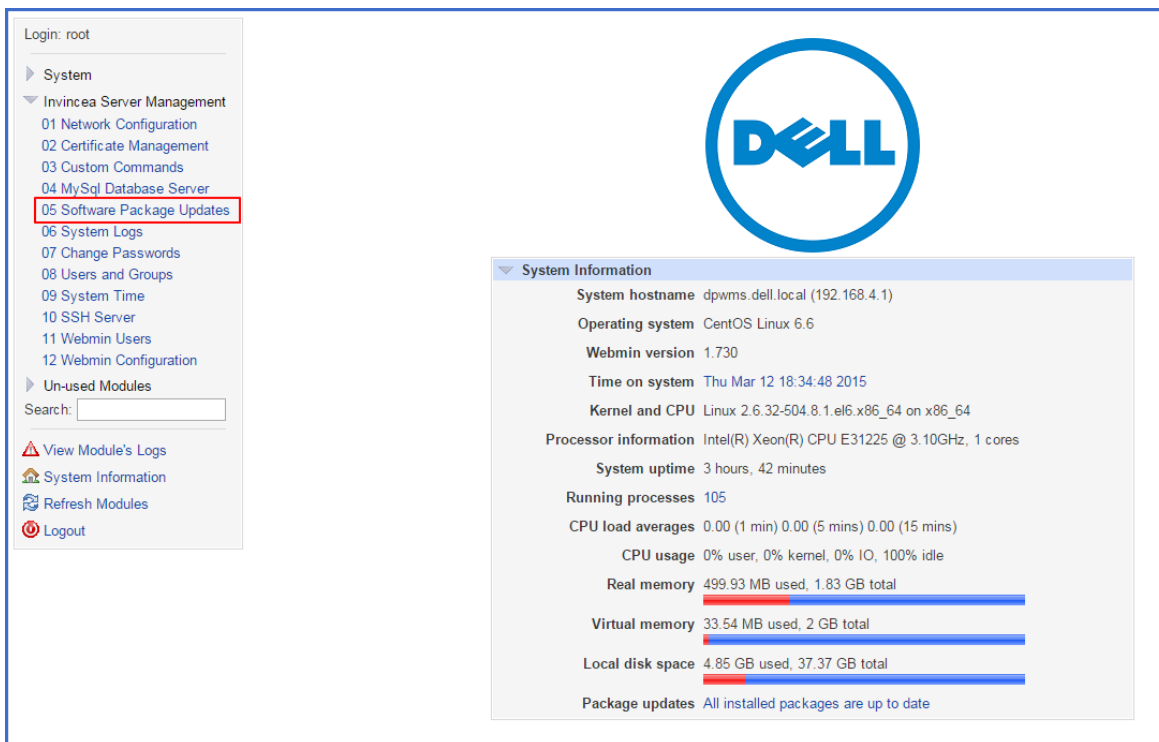
Chain RH-Firewall1-1-OUTPUT
Select all. | Invert selection.

Action	Condition	Move	Add
<input type="checkbox"/> Drop	If protocol is TCP and state of connection is NEW	↓	↓ ↑
<input type="checkbox"/> Accept	If output interface is lo	↓ ↑	↓ ↑
<input type="checkbox"/> Accept	If protocol is ICMP and ICMP type is echo-request	↓ ↑	↓ ↑
<input type="checkbox"/> Accept	If protocol is ICMP and ICMP type is destination-unreachable	↓ ↑	↓ ↑
<input type="checkbox"/> Accept	If protocol is ICMP and ICMP type is source-quench	↓ ↑	↓ ↑
<input type="checkbox"/> Accept	If protocol is ICMP and ICMP type is parameter-problem	↓ ↑	↓ ↑

Installing Linux Updates

In order to keep the Linux OS up to date, available system patches should be applied like any other server in the environment.

By navigating to the “05 Software Package Updates” page from the “Invincea Server Management” menu, a list of all available updates can be viewed.



The screenshot shows the Dell Protected Workspace Management Server interface. On the left, a navigation menu lists various system management options. The option "05 Software Package Updates" is highlighted with a red box. The main content area displays system information for the host "dpwms.dell.local".

System Information

System hostname	dpwms.dell.local (192.168.4.1)
Operating system	CentOS Linux 6.6
Webmin version	1.730
Time on system	Thu Mar 12 18:34:48 2015
Kernel and CPU	Linux 2.6.32-504.8.1.el6.x86_64 on x86_64
Processor information	Intel(R) Xeon(R) CPU E31225 @ 3.10GHz, 1 cores
System uptime	3 hours, 42 minutes
Running processes	105
CPU load averages	0.00 (1 min) 0.00 (5 mins) 0.00 (15 mins)
CPU usage	0% user, 0% kernel, 0% IO, 100% idle
Real memory	499.93 MB used, 1.83 GB total
Virtual memory	33.54 MB used, 2 GB total
Local disk space	4.85 GB used, 37.37 GB total
Package updates	All installed packages are up to date

States to display: [Installed](#) | [Only updates](#) | [Only new](#)

Find packages matching:

Found 181 matching packages ...

Select all | Invert selection

Package	Description	Status	Source
<input checked="" type="checkbox"/> abrt	Automatic bug detection and reporting tool	New version 2.0.8-6.el6.centos	Base
<input checked="" type="checkbox"/> abrt-addon-ccpp	abrt's C/C++ addon	New version 2.0.8-6.el6.centos	Base
<input checked="" type="checkbox"/> abrt-addon-kerneloops	abrt's kerneloops addon	New version 2.0.8-6.el6.centos	Base
<input checked="" type="checkbox"/> abrt-addon-python	abrt's addon for catching and analyzing Python exceptions	New version 2.0.8-6.el6.centos	Base
<input checked="" type="checkbox"/> abrt-cgi	abrt's command line interface	New version 2.0.8-6.el6.centos	Base
<input checked="" type="checkbox"/> abrt-libs	Libraries for abrt	New version 2.0.8-6.el6.centos	Base
<input checked="" type="checkbox"/> alsa-utils	Advanced Linux Sound Architecture (ALSA) utilities	New version 1.0.22-3.el6	Base
<input checked="" type="checkbox"/> apr	Apache Portable Runtime library	New version 1.3.9-5.el6_2	Updates
<input checked="" type="checkbox"/> at	Job spooling tools	New version 3.1.10-43.el6_2.1	Base
<input checked="" type="checkbox"/> audit	User space tools for 2.6 kernel auditing	New version 2.2.2.el6	Base
<input checked="" type="checkbox"/> audit-libs	Dynamic library for libaudit	New version 2.2.2.el6	Base
<input checked="" type="checkbox"/> authconfig	Command line tool for setting up authentication from network services	New version 6.1.12-10.el6	Base
<input checked="" type="checkbox"/> bash	The GNU Bourne Again shell	New version 4.1.2.9.el6_2	Base
<input checked="" type="checkbox"/> bind-libs	Libraries used by the BIND DNS packages	New version 9.8.2-0.10.rc1.el6	Base
<input checked="" type="checkbox"/> bind-utils	Utilities for querying DNS name servers	New version 9.8.2-0.10.rc1.el6	Base
<input checked="" type="checkbox"/> binutils	A GNU collection of binary utilities	New version 2.20.51.0.2-5.34.el6	Base
<input checked="" type="checkbox"/> btparser	Parser and analyzer for backtraces produced by GDB	New version 0.16-3.el6	Base
<input checked="" type="checkbox"/> busybox	Statically linked binary providing simplified versions of system commands	New version 1.15.1-15.el6	Base
<input checked="" type="checkbox"/> centos-release	CentOS release file	New version 6.3.el6.centos.9	Base
<input checked="" type="checkbox"/> chkconfig	A system tool for maintaining the /etc/rc* d hierarchy	New version 1.3.49-3.2.el6	Base
<input checked="" type="checkbox"/> coreutils	A set of basic GNU tools commonly used in shell scripts	New version 8.4-19.el6	Base
<input checked="" type="checkbox"/> coreutils-libs	Libraries for coreutils	New version 8.4-19.el6	Base
<input checked="" type="checkbox"/> cpio	A GNU archiving program	New version 2.10-10.el6	Base
<input checked="" type="checkbox"/> cryptsetup-luks	A utility for setting up encrypted filesystems	New version 1.2.0-7.el6	Base

To apply updates, select the desired updates and press the “Update Selected Packages” button at the bottom of the list.

samba-winbind Samba winbind New version 3.6.23-14.el6_6 Updates

samba-winbind-clients Samba winbind clients New version 3.6.23-14.el6_6 Updates

Select all | Invert selection

Scheduled checking options

Check for updates on schedule? No Yes, every

Email updates report to

Action when update needed Just notify Install security updates Install any updates

Generating a new self-signed certificate after initial configuration is complete

In case a new self-signed certificate needs to be generated, either because the system name has changed, the original certificate is incorrect or for any other reasons, follow the steps listed under “Certification Creation” and “Restarting the DPWMS.”

Installing a Trusted SSL certificate

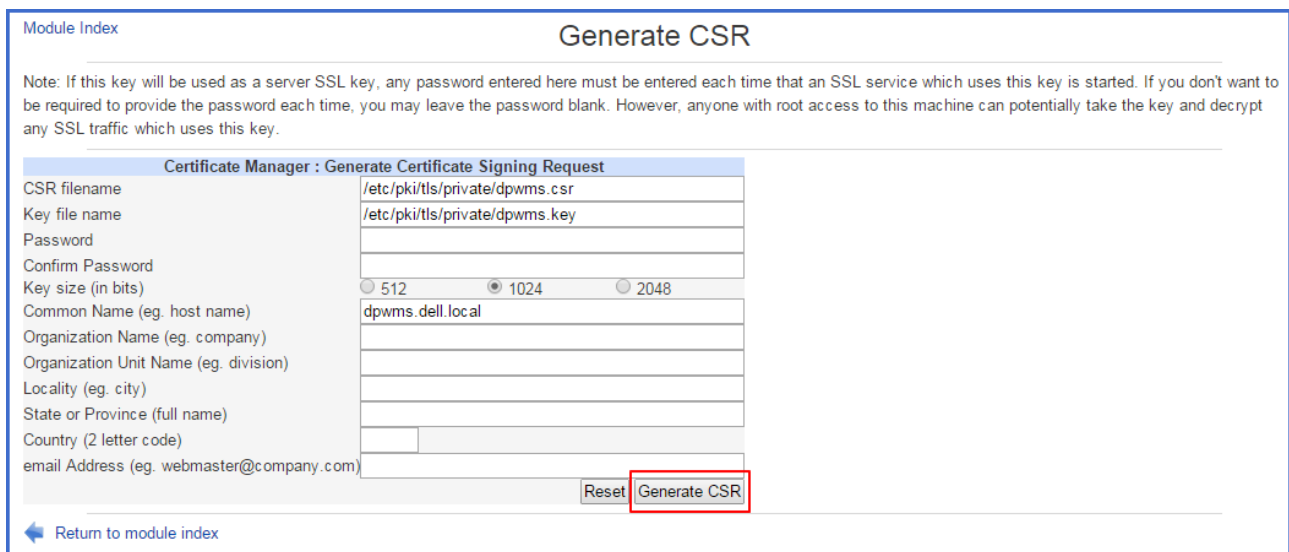
If a trusted SSL certificate is going to be used rather than a self-generated one, follow these steps to install it on the IMS.

Generating a CSR

If needed, a CSR can be created for the SSL Certificate. Start by selecting “02 Certificate Management” from the “Invincea Server Management” menu. From the “Certificate Manager” page, select the “Generate Key and Certificate Signing Request (CSR)” option.



Starting with the “FULLY QUALIFIED HOSTNAME” field, fill out the “Generate CSR” form. Once completed, press the “Generate CSR” button.



The screenshot shows the 'Generate CSR' form. At the top left is a 'Module Index' link. The title is 'Generate CSR'. A note reads: 'Note: If this key will be used as a server SSL key, any password entered here must be entered each time that an SSL service which uses this key is started. If you don't want to be required to provide the password each time, you may leave the password blank. However, anyone with root access to this machine can potentially take the key and decrypt any SSL traffic which uses this key.' Below the note is a section titled 'Certificate Manager : Generate Certificate Signing Request' with a table of input fields: 'CSR filename' (value: /etc/pki/tls/private/dpwms.csr), 'Key file name' (value: /etc/pki/tls/private/dpwms.key), 'Password' (empty), 'Confirm Password' (empty), 'Key size (in bits)' (radio buttons for 512, 1024 (selected), 2048), 'Common Name (eg. host name)' (value: dpwms.dell.local), 'Organization Name (eg. company)' (empty), 'Organization Unit Name (eg. division)' (empty), 'Locality (eg. city)' (empty), 'State or Province (full name)' (empty), 'Country (2 letter code)' (empty), and 'email Address (eg. webmaster@company.com)' (empty). At the bottom right of the form are 'Reset' and 'Generate CSR' buttons. The 'Generate CSR' button is highlighted with a red rectangular box. At the bottom left is a 'Return to module index' link with a left-pointing arrow.

On the next page, press the “Continue” button to generate the CSR.

Module Index
Generate CSR

[/etc/pki/tls/private/dpwms.key](#)
 Key size (in bits): 1024
 To download or view more information about a CSR or key, follow the link from its filename.

The above CSR and/or key will be replaced if you continue. Are you sure you wish to continue?

[Return to module index](#)

From the confirmation page, use the hyperlink locations to go to the download page for the CSR and KEY files. Press the “Download” button to display the file so it can be copied to the local machine.

Module Index
Generate CSR

CSR and key generated
 Generating a 1024 bit RSA private key
 ..++++++
++++++
 writing new private key to '/etc/pki/tls/private/dpwms.key'

The CSR was saved as [/etc/pki/tls/private/dpwms.csr](#)
 The key was saved as [/etc/pki/tls/private/dpwms.key](#)

[Return to module index](#)

Module Index
View Certificate/CSR/Key

[/etc/pki/tls/private/dpwms.csr](#)
Subject
 dpwms.dell.local
 Key size (in bits)
 Key Type
 Public Exponent 65537 (0x10001)
 Modulus (from public key):

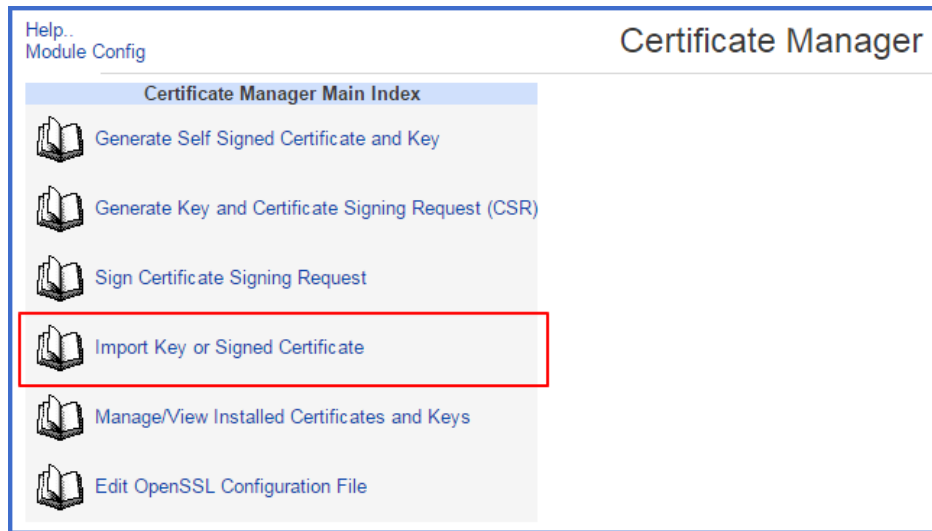
[Return to module index](#)

```

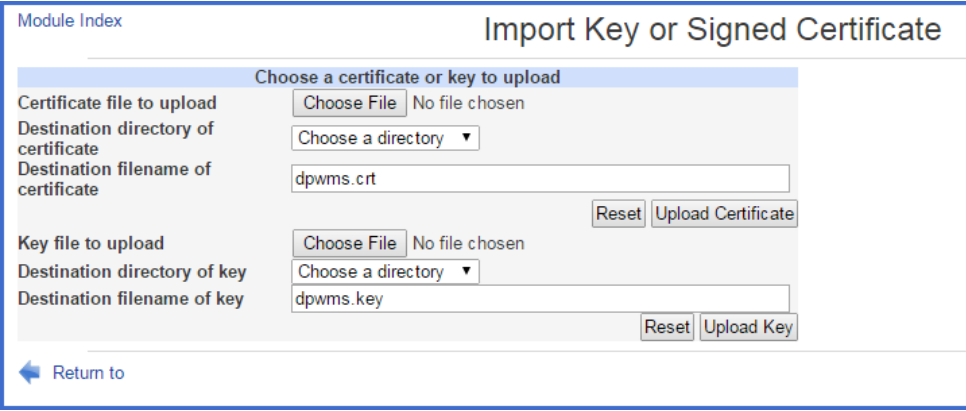
-----BEGIN CERTIFICATE REQUEST-----
MIIBWjCBxAIBADAbMRkwFwYDVQQDExBkcHdscy5kZWxsLmxvY2FsmIGfMA0GCSqG
SIb3DQEBAQUAA4GNADCBiQKBgQC5Mtr6a2HoHuSk0YivjOPDB1PuG9yJ630tWRT5
OyDAfT5XqOd5YFrQ11DdT7V/BKNymqaqK54wHeL5q5kxLbeX69ntG7Zb1FdNF5Pg
f53z28v33S01Mrfh+oHbM+PkKo1X5V6oYsrgkzNbEq3dzK1DV/Wx54Vff4tqWahF
RcV7vwIDAQABoAAwDQYJKoZIhvcNAQEFBQADgYEAAM47+AJsNbXhJn/0hd4LgfbHm
ks03DpXNbeTTOasTxkKs7eoTMAB63YJnH2EXry5qoHPgTkhW1C5D79ns7fMRCwqj
C1ebNTfyurjw5vpDIC1N5056vr1DR48ujydd7x+axGdtexU2V96dgf4nhctHcEcI
T/4oB25fJwdp9bbJ+H8=
-----END CERTIFICATE REQUEST-----
    
```

Importing Signed Certificate and Key

To import a certificate and key from a trusted CA, start by choosing the “02 Certificate Management” option from the “Invincea Server Management” menu. From the “Certificate Manager” page, select “Import Key or Signed Certificate.”



From the “Import Key or Signed Certificate” page, press the “Browse” button to choose the certificate or key that needs to be uploaded. Once selected, press the “Upload Certificate” and/or “Upload Key” button(s) to complete the upload.



The screenshot shows the 'Import Key or Signed Certificate' form. The form is titled 'Choose a certificate or key to upload'. It has two main sections: 'Certificate file to upload' and 'Key file to upload'. Each section has a 'Choose File' button, a 'No file chosen' status, a 'Destination directory' dropdown menu, and a 'Destination filename' text input field. The 'Certificate' section has a filename of 'dpwms.crt' and buttons for 'Reset' and 'Upload Certificate'. The 'Key' section has a filename of 'dpwms.key' and buttons for 'Reset' and 'Upload Key'. At the bottom left, there is a 'Return to' link with a left-pointing arrow.

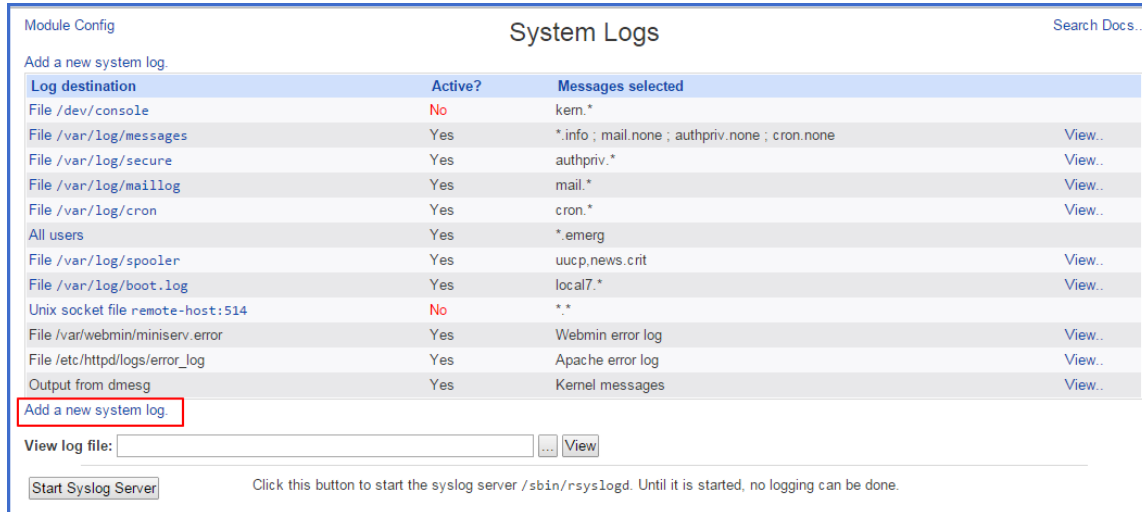
The certificate files (named dpwms.crt) must be uploaded to the following directory: /etc/pki/tls/certs

The private key file (named dpwms.key), if it needs to be replaced, must be uploaded to the following directory: /etc/pki/tls/private

Configuring the Dell Protected Workspace Management Server for SYSLOG

For SIEM integration it is necessary to add a SYSLOG destination server to the DPWMS. To configure this, select the “06 System Logs” option from the “Invincea Server Management” menu.

From the System Logs page, select the “Add a new system log” hyperlink located at the bottom of the table.



Module Config Search Docs..

System Logs

Add a new system log.

Log destination	Active?	Messages selected	
File /dev/console	No	kern.*	
File /var/log/messages	Yes	*.info ; mail.none ; authpriv.none ; cron.none	View..
File /var/log/secure	Yes	authpriv.*	View..
File /var/log/maillog	Yes	mail.*	View..
File /var/log/cron	Yes	cron.*	View..
All users	Yes	*.emerg	
File /var/log/spooler	Yes	uucp,news.crit	View..
File /var/log/boot.log	Yes	local7.*	View..
Unix socket file remote-host:514	No	*.*	
File /var/webmin/miniserv.error	Yes	Webmin error log	View..
File /etc/httpd/logs/error_log	Yes	Apache error log	View..
Output from dmesg	Yes	Kernel messages	View..

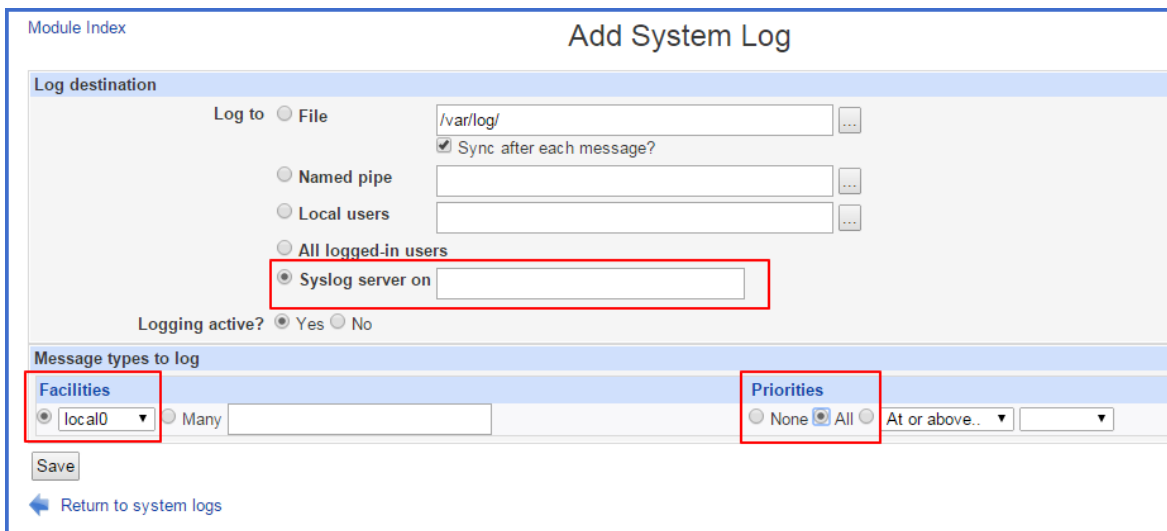
[Add a new system log.](#)

View log file:

Click this button to start the syslog server /sbin/rsyslogd. Until it is started, no logging can be done.

In the “Log to” section of the “Add System Log” page, change the radio button to select “Syslog server on” and enter the destination IP address of your syslog listener.

Under the “Facilities” section, choose “local0” from the drop-down and select the “All” radio button under “Priorities.” Press the Save button when finished.



Module Index Add System Log

Log destination

Log to File

Sync after each message?

Named pipe

Local users

All logged-in users

Syslog server on

Logging active? Yes No

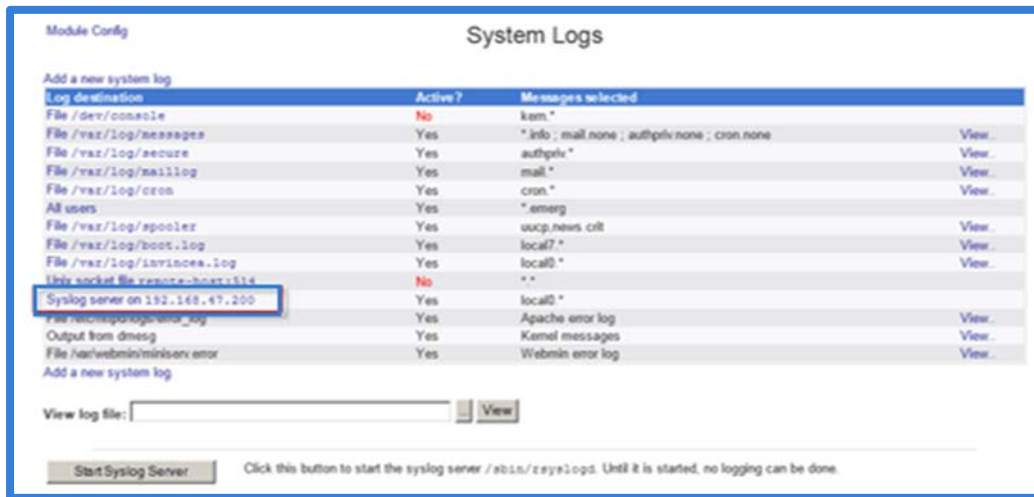
Message types to log

Facilities local0 Many

Priorities None All At or above..

[Return to system logs](#)

Verify that the syslog server is now configured in the “System Logs” page. It should be listed as “Syslog server on <IP_ADDRESS>”, be Active and selected for local0.*



To complete the syslog configuration, the syslog service needs to be restarted (or started if it was not running). To do this, navigate to the 03 Custom Commands menu and use the Syslog commands.

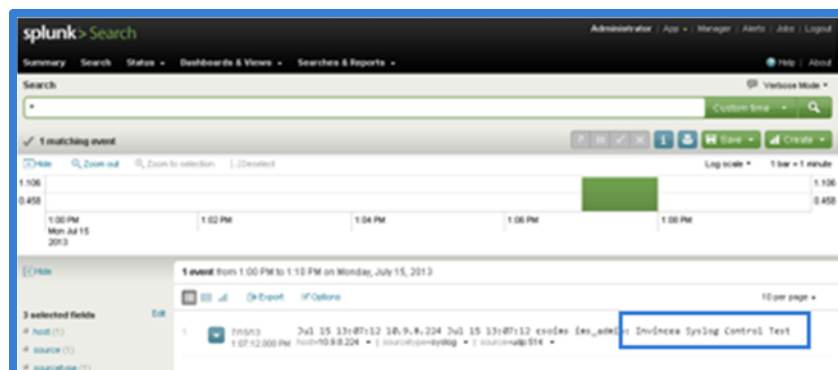
Testing SYSLOG connection from DPWMS

To validate that the DPWMS is sending data to the configured SYSLOG destination server, go to the “03 Custom Commands” menu from the “Invocea Server Management” Menu.

Listed under the Custom Commands Menu is a command labeled “DPWMS Syslog Test Command.” Click on this command link to send a destination to the specified destination server.



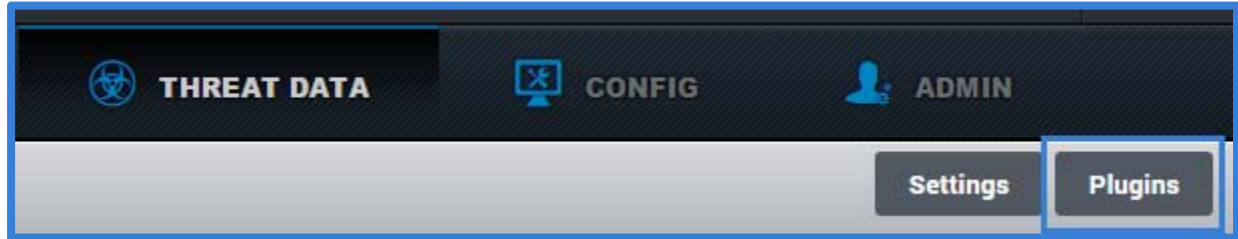
Once the command is run, verify that the SYSLOG destination server received a SYSLOG message with the text “DPWMS Syslog Control Test.” If this message was received by the destination server, SYSLOG reporting is working correctly.



Configuring the Threats Module with the Correct SYSLOG format

The DPWMS Threats Module is able to send Threat Report information to SIEM systems in a few different formats to better suit the receiving SIEM system. Available formats are Splunk, Q1 Labs, Arcsight and RSA Envision.

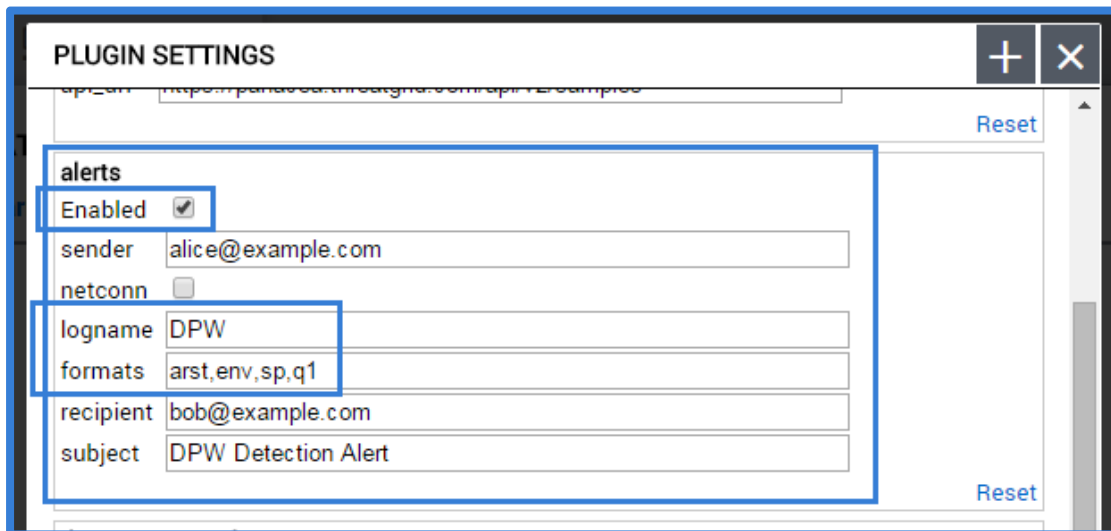
To set the proper logging format, select the Plugins menu from the Threat Data tab.



From the Plugin Settings dialog, locate the entry for formats under the alerts header and make sure that the “Enabled” box is checked. If not, check the box and restart the DPWMS (ims2) service. Now, modify this line to the correct format (only one should be selected. All four are displayed by default, and should be modified to the correct selection):

- sp = Splunk
- q1 = Q1 Labs
- arst = Archsight
- env = RSA Envision

Optionally, modify the logname entry to create a custom search word in the SYSLOG entry. This logname is including at the beginning of the SYSLOG messages generated by the Threats Module.



Press the “Save” button and close the dialog once the changes have been made.

Operational Notes for the Dell Protected Workspace Management Server

Security Restrictions/Features

The Dell Protected Workspace server has the following security restrictions that may need to be taken into consideration within your environment.

- ICMP echo (ping) is disabled
- SELinux is enabled and configured with the strictest default policy.
- You can only connect to the appliance using HTTPS on port 443 and SSH on port 10022.
- You can only make outbound connections from the appliance to port 80 and 443.

Logging into the Appliance Remotely via SSH

You can log into the host remotely using a SSHv2 client, such as OpenSSH, SecureCRT or PuTTY. The username is `ims_admin` and the password will be the default password or what the administrator has changed it to. The `ims_admin` account is the ONLY account that has SSH access to the system. The SSH server runs on port 10022, so the client will need to use that port rather than the default. The command using OpenSSH is:

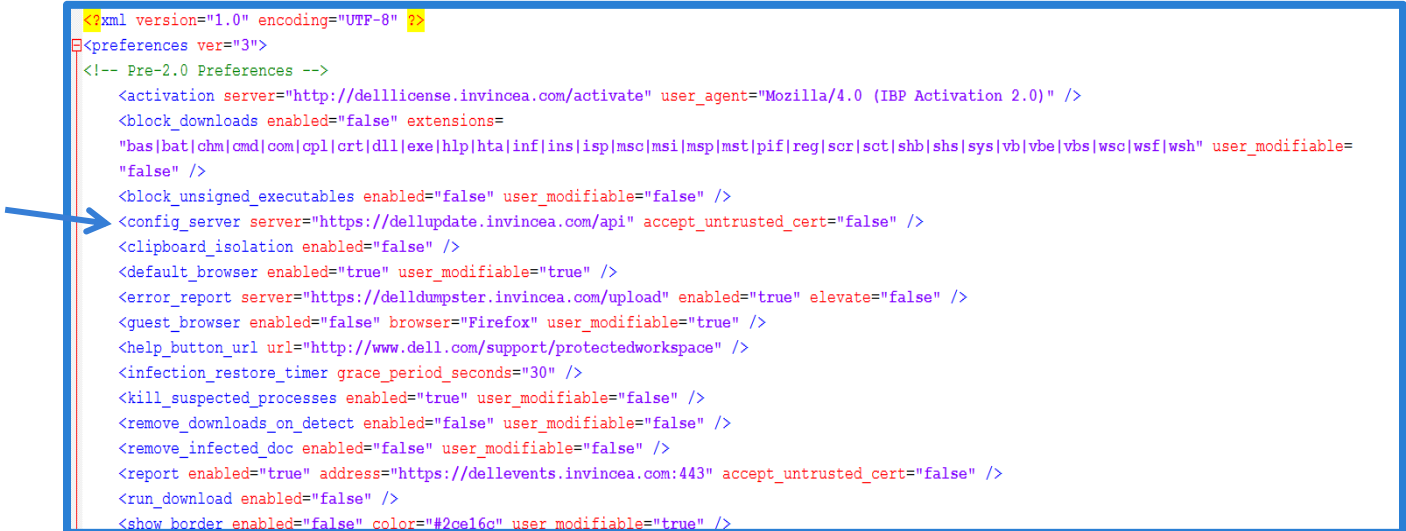
```
ssh -P10022 ims_admin@your.host.name.here
```

Once logged into the `ims_admin` account, the “`su`” command can be used to elevate privileges and become root. This will be required if administrative tasks need to be performed.

Configuring Dell Protected Workspace to work with the Dell Protected Workspace Management Server – Configuration Management Module

In order for installations of Dell Protected Workspace to report to the Dell Protected Workspace Management Server – Configuration Management Module, the client software needs to be configured to point to the DPWMS. The following steps outline how to properly configure the clients.

1. From the Dell Protected Workspace configuration files, open the preferences.xml file with a standard text editor.



```
<?xml version="1.0" encoding="UTF-8" ?>
<preferences ver="3">
  <!-- Pre-2.0 Preferences -->
  <activation server="http://delllicense.invincea.com/activate" user_agent="Mozilla/4.0 (IBP Activation 2.0)" />
  <block_downloads enabled="false" extensions=
    "bas|bat|chm|cmd|com|cpl|crt|dll|exe|hlp|hta|inf|ins|isp|mso|msi|msp|mst|pif|reg|scr|sct|shb|shs|sys|vb|vbe|vbs|wsc|wsf|wsh" user_modifiable=
    "false" />
  <block_unsigned_executables enabled="false" user_modifiable="false" />
  <config_server server="https://dellupdate.invincea.com/api" accept_untrusted_cert="false" />
  <clipboard_isolation enabled="false" />
  <default_browser enabled="true" user_modifiable="true" />
  <error_report server="https://dell dumpster.invincea.com/upload" enabled="true" elevate="false" />
  <guest_browser enabled="false" browser="Firefox" user_modifiable="true" />
  <help_button_url url="http://www.dell.com/support/protectedworkspace" />
  <infection_restore_timer grace_period_seconds="30" />
  <kill_suspected_processes enabled="true" user_modifiable="false" />
  <remove_downloads_on_detect enabled="false" user_modifiable="false" />
  <remove_infected_doc enabled="false" user_modifiable="false" />
  <report enabled="true" address="https://dellevents.invincea.com:443" accept_untrusted_cert="false" />
  <run_download enabled="false" />
  <show_border enabled="false" color="#2ce16c" user_modifiable="true" />
```

2. Locate the line beginning with “<config_server”.
3. Modify this line to point to the DNS name of the newly configured DPWMS
 - a. <config_server server="https://<FQDN SERVER NAME>/api" accept_untrusted_cert="false" />
4. If using a self-generated certificate, also change the value of “accept_untrusted_cert” on the same line to “true”.
 - a. <config_server server="https:// ://<FQDN SERVER NAME>/api" accept_untrusted_cert="true" />
5. Save the file and deploy it with new client installs.

Configuring Dell Protected Workspace to work with the Dell Protected Workspace Management Server – Threat Data Module

In order for installations of Dell Protected Workspace to report to the Dell Protected Workspace Management Server – Threat Data Module, the client software needs to be configured to point to the DPWMS. The following steps outline how to properly configure the clients.

1. From the Dell Protected Workspace configuration files, open the preferences.xml file with a standard text editor.

```
<?xml version="1.0" encoding="UTF-8" ?>
<preferences ver="3">
<!-- Pre-2.0 Preferences -->
  <activation server="http://delllicense.invincea.com/activate" user_agent="Mozilla/4.0 (IBP Activation 2.0)" />
  <block_downloads enabled="false" extensions=
"bas|bat|chm|cmd|com|cpl|ort|dll|exe|hlp|hta|inf|ins|isp|mso|msi|msp|mst|pif|reg|scr|sct|shb|shs|sys|vb|vbe|vbs|wsc|wsf|wsh" user_modifiable=
"false" />
  <block_unsigned_executables enabled="false" user_modifiable="false" />
  <config_server server="https://dellupdate.invincea.com/api" accept_untrusted_cert="false" />
  <clipboard_isolation enabled="false" />
  <default_browser enabled="true" user_modifiable="true" />
  <error_report server="https://delldumpster.invincea.com/upload" enabled="true" elevate="false" />
  <guest_browser enabled="false" browser="Firefox" user_modifiable="true" />
  <help_button_url url="http://www.dell.com/support/protectedworkspace" />
  <infection_restore_timer grace_period_seconds="30" />
  <kill_suspected_processes enabled="true" user_modifiable="false" />
  <remove_downloads_on_detect enabled="false" user_modifiable="false" />
  <remove_infected_doc enabled="false" user_modifiable="false" />
  <report enabled="true" address="https://dellevents.invincea.com:443" accept_untrusted_cert="false" />
  <run_download enabled="false" />
  <show_border enabled="false" color="#2ce16c" user_modifiable="true" />
```

2. Locate the line beginning with “<report”.
3. Modify this line to point to the DNS name of the newly configured DPWMS
 - a. <report enabled="true" address="https://<FQDN SERVER NAME>:443" accept_untrusted_cert="false" />
4. If using a self-generated certificate, also change the value of “accept_untrusted_cert” on the same line to “true”.
 - a. <report enabled="true" address="https://<FQDN SERVER NAME>:443" accept_untrusted_cert="true" />
5. Save the file and deploy it with new client installs.

Dell Protected Workspace Management Server Administrative Tasks

Acquiring the temporary administrator password for DPWMS UI

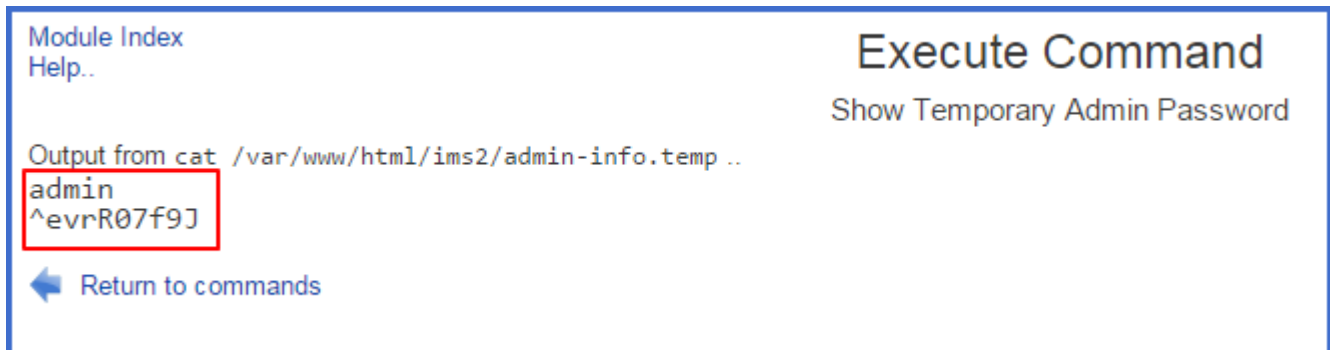
Upon startup of the DPWMS 2.x server, a temporary password is generated and stored in the database for the DPWMS system. The follow steps outline how to access the temporary password so that access can be granted to the DPWMS UI.

From the WebUI (port 1000) interface, log in and browse to Invincea Server Management -> 03 Custom Commands. Click on the “Show Temporary Admin Password” link.



Command	Description	Actions
Start DPWMS (ims2) Service		Edit Run
Stop DPWMS (ims2) Service		Edit Run
Restart DPWMS (ims2) Service		Edit Run
Start Syslog		Edit Run
Stop Syslog		Edit Run
Show Temporary Admin Password		Edit Run
DPWMS Syslog Test Command - Send message to Destination		Edit Run

This link will display the temporary password assigned to the admin user. This password is needed to log into the DPWMS 2.x system for the first time. The first line of the output will display the user name “admin”. The second line will display the temporary password.



Module Index
Help..

Execute Command

Show Temporary Admin Password

Output from `cat /var/www/html/ims2/admin-info.temp ..`

```
admin
^evrR07f9J
```

← Return to commands

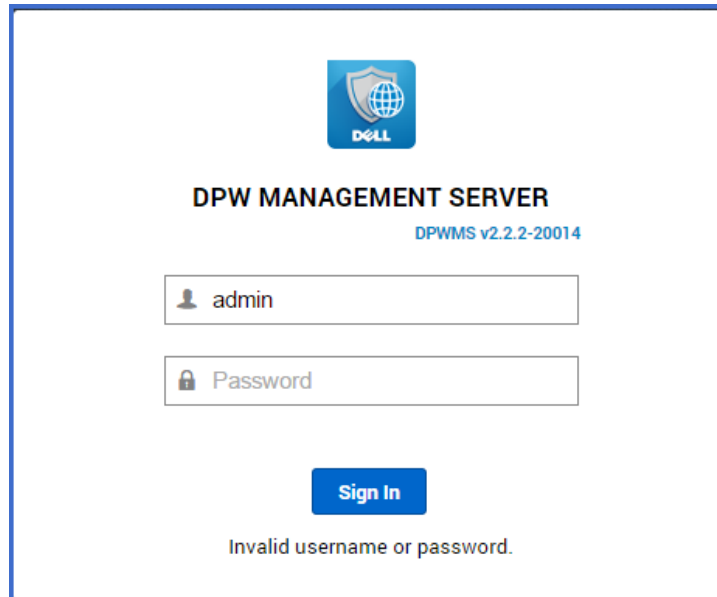
If the Webmin (port 10000) interface is not available, the temporary password can be view by looking at the contents of the `/var/www/html/ims2/admin-info.temp` file.

Logging into the Dell Protected Workspace Management Server Console

To access the Dell Protected Workspace Management Server Console (DPWMS Console), use a web browser to browse to the following address:

`https://<dpw_management_hostname>`

where `<dpw_management_hostname>` is the FQDN defined during setup (alternatively, the IP address of the system can be used). If prompted about an issue with the site certificate, choose “Continue to this website”



The screenshot shows the login interface for the DPW Management Server. At the top center is the Dell logo. Below it, the text reads "DPW MANAGEMENT SERVER" in bold, with "DPWMS v2.2.2-20014" in smaller blue text underneath. There are two input fields: the first is labeled "admin" with a user icon, and the second is labeled "Password" with a lock icon. A blue "Sign In" button is centered below the password field. At the bottom of the page, the text "Invalid username or password." is displayed.

At the login prompt, use the default credentials to log in to the DPWMS Console.

User: admin

Password: <acquired via WebUI custom_command>

When accessing the Dell Protected Workspace Management Server, the home page is displayed first. This home page will display differently depending on what modules the system is licensed for. The following information describes the available modules and their functions.

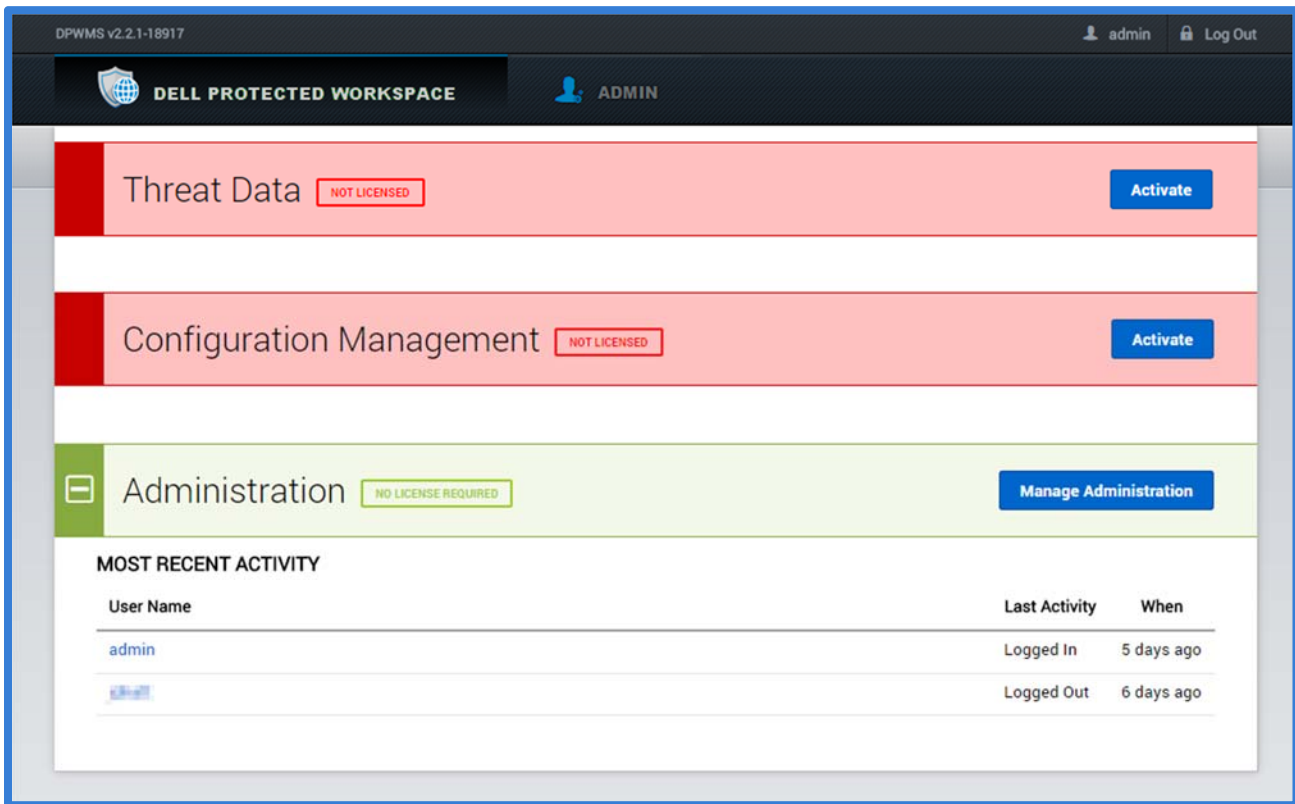
Entering the DPWMS License Key

The DPWMS license key can be entered via two different methods: via the DPWMS UI or via the DPWMS configuration file.

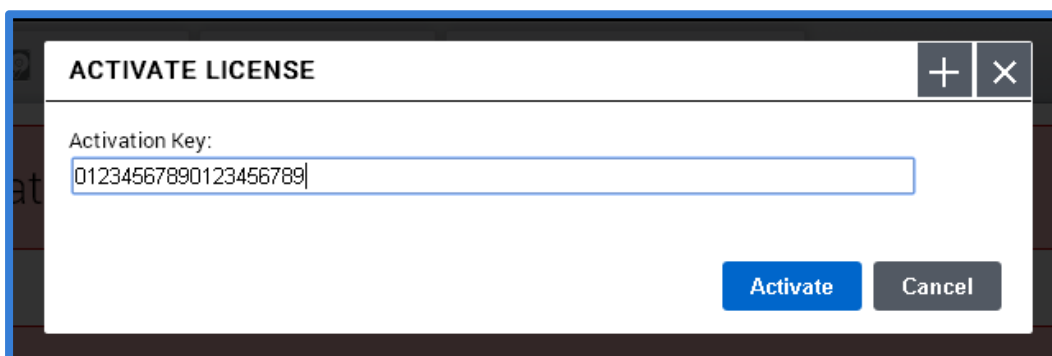
IMPORTANT NOTE: The Dell Protected Workspace Management Server requires an internet connection to allow product activation of the server. If an internet connection is not available, please contact Dell Support for assistance.

DPWMS UI Method

When the Admin account is logged into the DPWMS for the first time, the unlicensed modules will be displayed on the landing page.

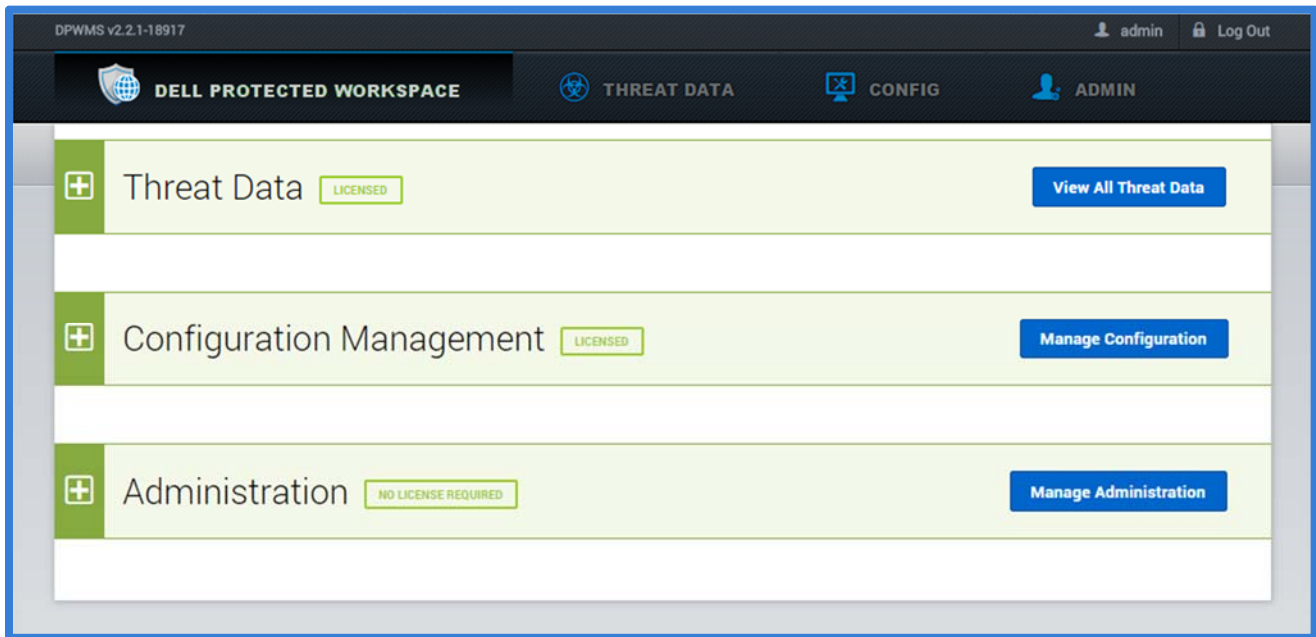


To activate the modules, click on the “Activate” button on either the Threat Data or Configuration Management module headers.



When the Activate License dialog box is displayed, enter the license key from the License Entitlement Certificate. Press the “Activate” button to finish the activation.

If the activation is successful, the Activate License dialog will close and the modules will now be available for use.



If the activation does not work, an error message will display on the dialog box.

If activation fails, validate that the DPWMS system has access to <http://delllicense.invincea.com/activate>

If an internet connection is not available, please contact Dell Support.

Note: If any of the system properties of the DPWMS change (system name, mac address, etc.) the license key will need to be re-entered when using this method. In some cases it will need to be reissued.

DPWMS Configuration File Method

By placing the DPWMS activation key into the configuration file, the DPWMS will automatically attempt to activate, if it has not done so already, when the DPWMS (ims2) service is started. This ensures that any hardware / configuration changes (MAC, FQDN, etc.) will not cause a user to be prompted to enter the activation key when they log in.

To enter the activation key into the configuration file, start by connecting to the virtual machine console or using SSH to access the system. An elevated account, such as the root account, will need to be used in order to make changes to the configuration file.

Once connected, stop the DPWMS (ims2) service by running the following command:

```
service ims2 stop
```

Change to the installation directory (which is `/var/www/html/ims2` by default; if a custom install was done, it may be different).

Use a text editor, such as `vi` to modify the `ims.conf` file.

Find the following line and enter the activation key after the equals sign on the `activation_key` line:

```
[license]
#the license activation key to automatically attempt
activation_key = 12345678901234567890
```

Save the file, then restart the IMS 2 service by running the following command:

```
service ims2 start
```

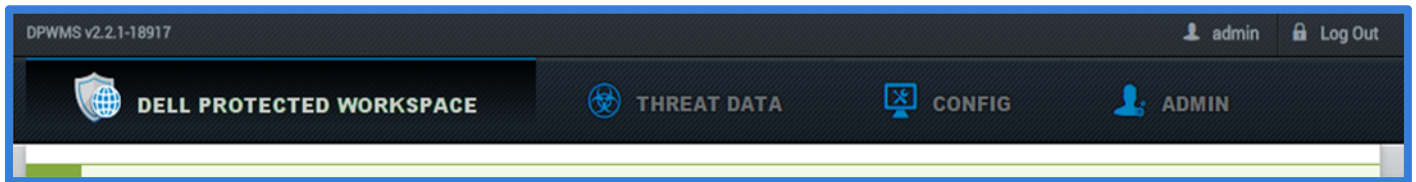
Validate the activation was successful by logging into the DPWMS UI. The modules should now be active. If not, view the `ims.log` file (located in the same installation directory as the `ims.conf` file) for details on what the error was.

If activation fails, validate that the DPWMS system has access to <http://delllicense.invincea.com/activate>

If an internet connection is not available, please contact Dell Support.

Modules

The Dell Protected Workspace Management Server is broken into different modules. Each module can be accessed by clicking on the appropriate module icon on the navigation bar.

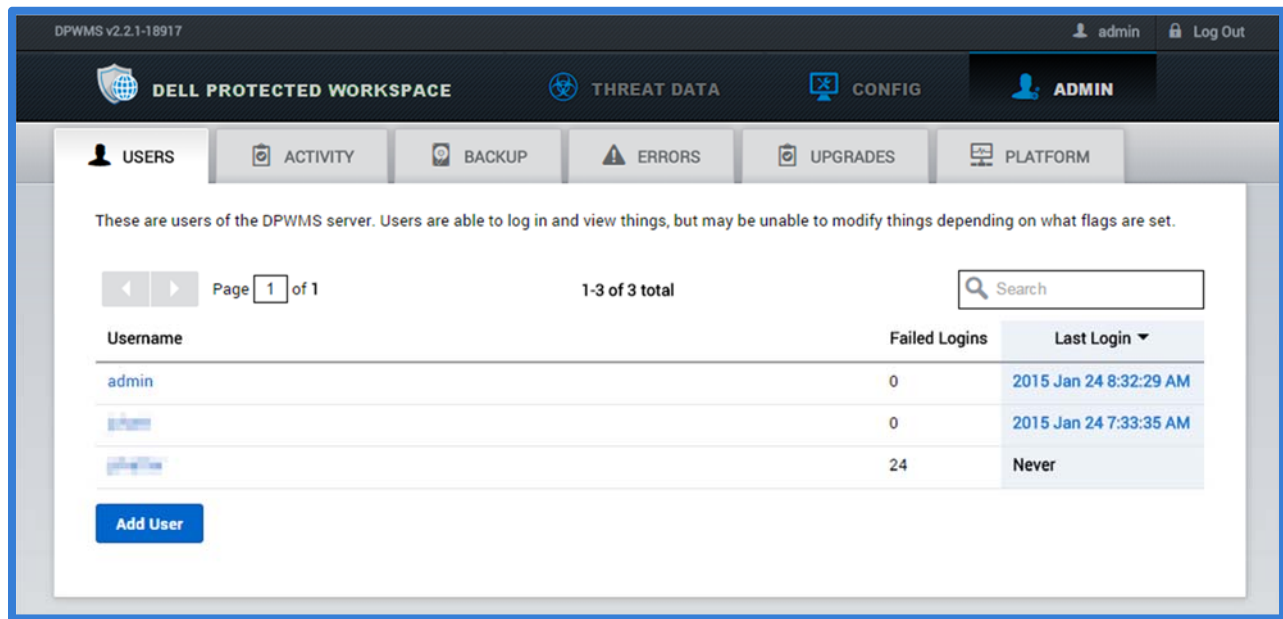


This version of the Dell Protected Workspace Management Server contains the following modules:

- Dell Protected Workspace Home – The Home module is a consolidated view of the Configuration and Threats Modules. This view contains a system overview. Information will only be displayed for those modules that are licensed.
- Threat Data – The Threat Data Module provides an analyst view of Threat Reports submitted from the client software.
- Config – The Config Module is used to manage client software configuration files and versions.
- Admin – The Admin Module is always available and is used to create user accounts and view user activity.

Admin Module

The Admin module is used for user management and activity tracking, database backups, error log viewing and DPWMS upgrades. It can be accessed by clicking on the Admin tab in the navigation bar.



Users Tab

The Admin module defaults to the Users tab when it is loaded. From this tab, new users can be added and existing users can be modified or removed.

With the release of DPWMS 2.0, role-based access is now available for DPWMS users. All users will have read-only access to the full DPWMS system by default, but can be granted modify access to any of the modules.

Admin access can also be set by enabling the appropriate flag for a user account:

FLAGS

Flags determine what permissions the user has. Only an administrator can modify these.

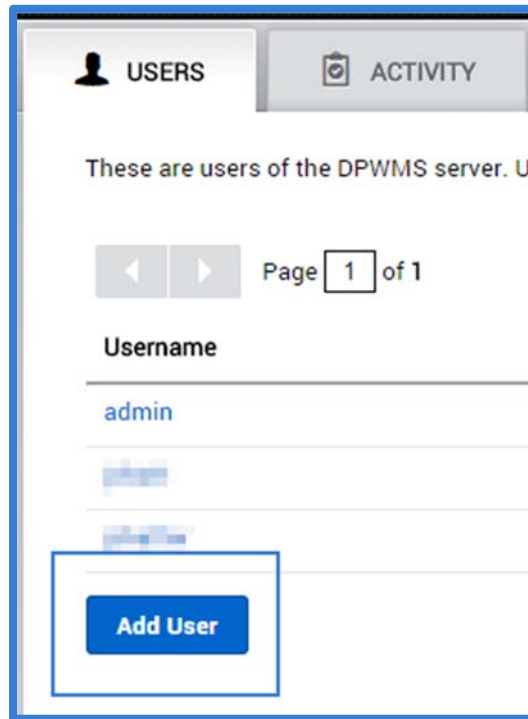
- admin** - Has full access, and also the ability to create and manage users
- cms_modify** - Has the ability to modify the CMS
- tds_modify** - Has the ability to modify the TDS

Flags:

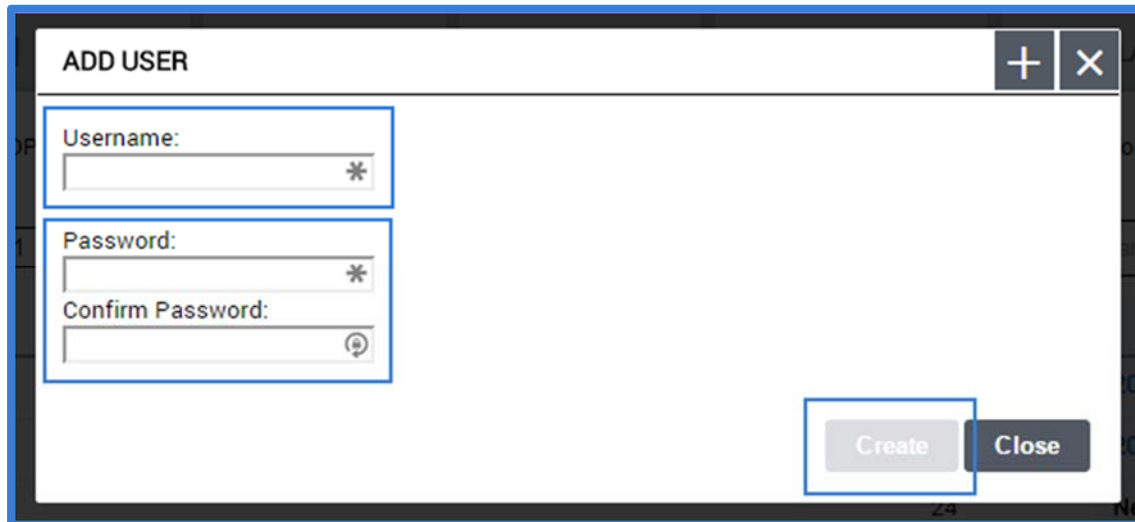
- Admin – has full access to the DPWMS system and all modules
- cms_modify – has full access to the CMS module only
- tds_modify – has full access to the TDS module only

Adding a new DPWMS User

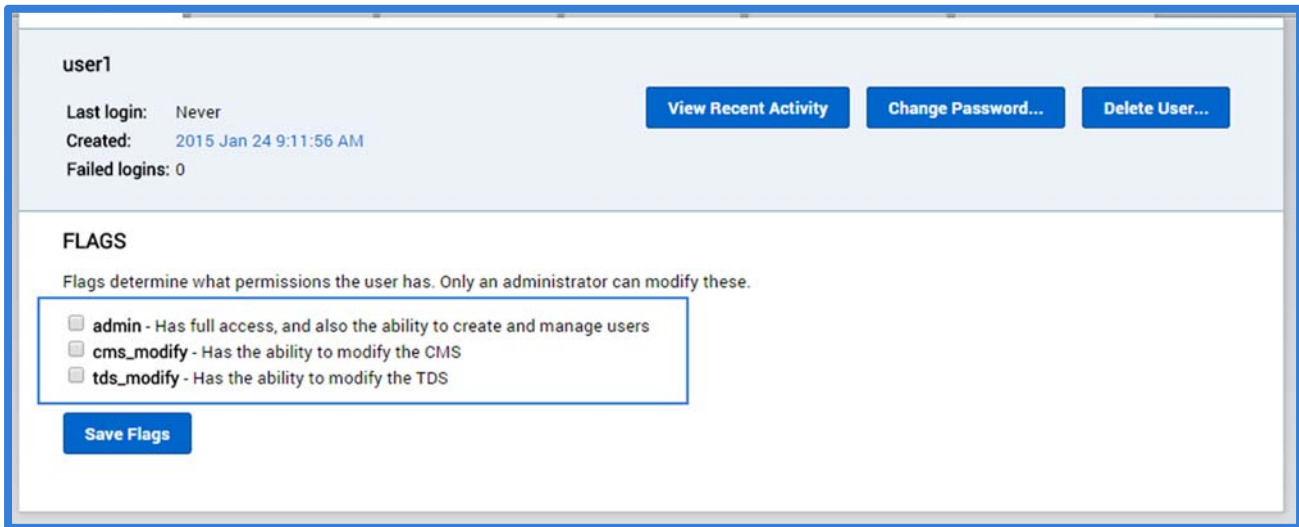
To add a new user to the DPWMS, click on the “Add User” button:



When the Add User dialog box is displayed, enter a user name. Then enter a password for the user and confirm it. When finished, click the “Create” button. To cancel the add user action, press the “Cancel” button.



After the user has been created, the user details will display. If required, select the additional flags necessary to give the user the correct permission level. Press the Save Flags button when finished.



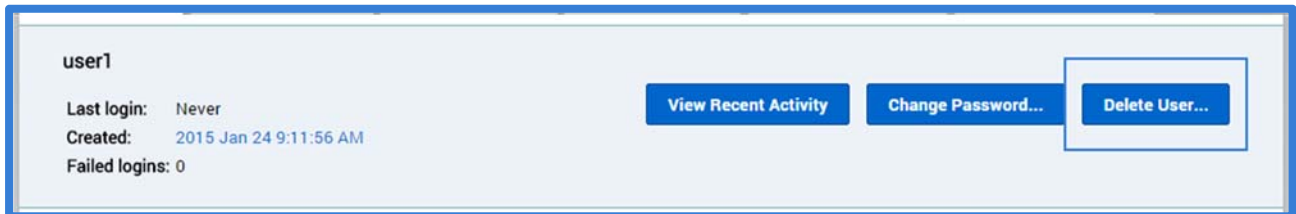
The screenshot shows the user details for 'user1'. The top section includes the user name, last login status (Never), creation date (2015 Jan 24 9:11:56 AM), and failed logins (0). There are three buttons: 'View Recent Activity', 'Change Password...', and 'Delete User...'. Below this is the 'FLAGS' section, which explains that flags determine permissions and only an administrator can modify them. Three flags are listed with checkboxes: 'admin' (full access), 'cms_modify' (modify CMS), and 'tds_modify' (modify TDS). A 'Save Flags' button is at the bottom.

user1	View Recent Activity	Change Password...	Delete User...
Last login: Never			
Created: 2015 Jan 24 9:11:56 AM			
Failed logins: 0			
FLAGS			
Flags determine what permissions the user has. Only an administrator can modify these.			
<input type="checkbox"/> admin - Has full access, and also the ability to create and manage users			
<input type="checkbox"/> cms_modify - Has the ability to modify the CMS			
<input type="checkbox"/> tds_modify - Has the ability to modify the TDS			
Save Flags			

Note: once a user is given admin level privileges, only that user can remove the admin level flag from the account.

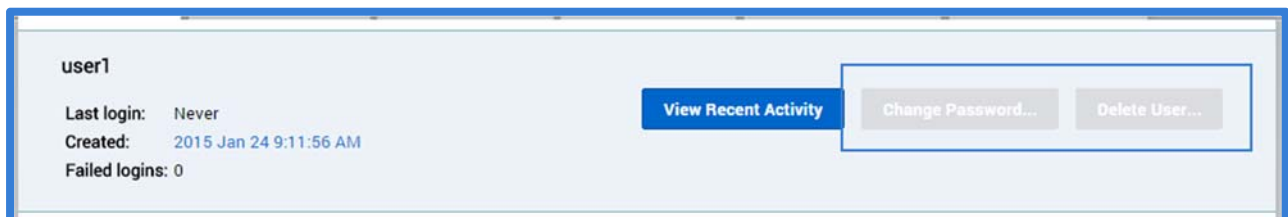
Deleting a user from the DPWMS

To delete a user from the DPWMS, go to the user's details page and press the Delete User button.



This screenshot is identical to the previous one, but the 'Delete User...' button is highlighted with a blue border, indicating it is the focus of the current step.

If the Delete User button is disabled, the user account will need to be modified to a standard (not admin) account before it can be deleted. This can only be done while the account is logged in.



This screenshot shows the user details for 'user1' where the 'Delete User...' button is disabled (greyed out). The 'Change Password...' button is also highlighted with a blue border.

Activity Tab

The Activity Tab is used to display the user audit log. This log will display when users log in and out of the system, and what actions they take while modifying the system. For example, activities such as creating or deleting a new group are tracked.

Date	Username	Type	Value
2015 Jan 24 9:15:17 AM	admin	Changed Flags For User	user1
2015 Jan 24 9:11:56 AM	admin	Created User	user1
2015 Jan 24 8:32:29 AM	admin	Logged In	
2015 Jan 24 8:30:02 AM	admin	Logged Out	

Backup Tab

The Backup Tab is used to backup and restore the DPWMS database. The backup table displays a list of all backups that have been run or uploaded to the DPWMS.

Date	Size	Name	Actions
2014 Jun 18 9:12:56 PM	1 KB	2014-06-19-01125616.mysql.gz	Download / Restore / Delete

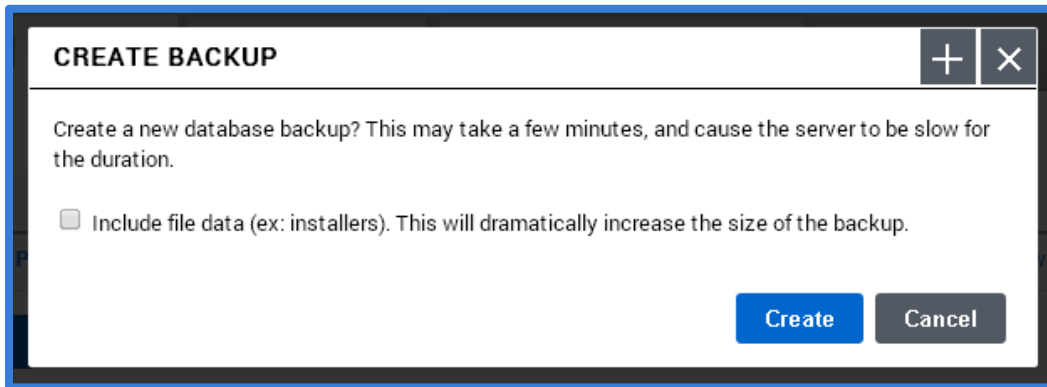
Create Upload

The table displays the time of the backup (when it was created or uploaded), the size of the backup, and the backup file name. Additionally, it allows for three actions to be taken with that backup:

- Download – downloads a copy of the backup file through the browser accessing the UI
- Restore – used to restore the DPWMS to the data that exists in the backup file. This will overwrite all existing data within the database. **NOTE: This functionality cannot be used with a multiple API setup.**
- Delete – removes the backup from the system

Create a Database Backup

To create a new database backup, press the “Create” button at the bottom of the table.

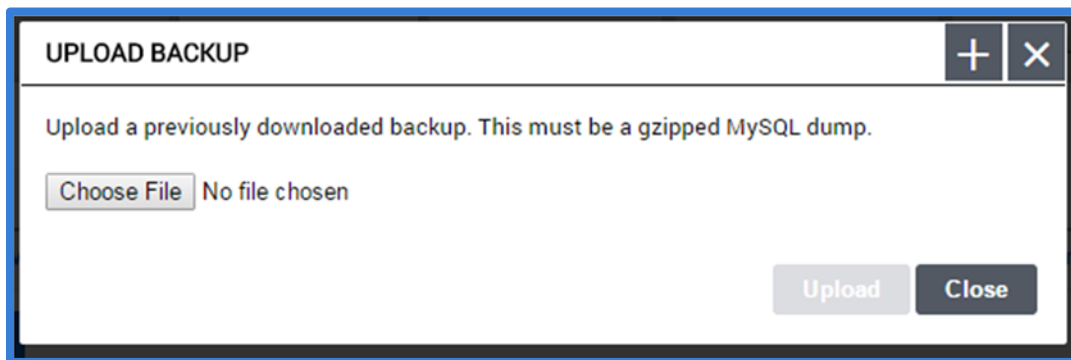


When the Create Backup dialog is displayed, select whether to include the client install kits currently uploaded to the DPWMS Config module as part of the backup, and then press the “Create” button to finish the creation. To cancel the action, press the “Cancel” button.

Once the backup is successfully created, it will be displayed in the list of available backups. Press the “Download” link on a selected backup file to download a local copy of the backup. Press the “Restore” link to restore the database from this backup. Press the “Delete” button to remove the selected backup.

Recovering from a Database Backup File

In the case of recovering a DPWMS from a backup file, stand up a new DPWMS system based on the instructions in this guide. Then from the backup tab, press the “Upload” button to upload a copy of the database to be restored.

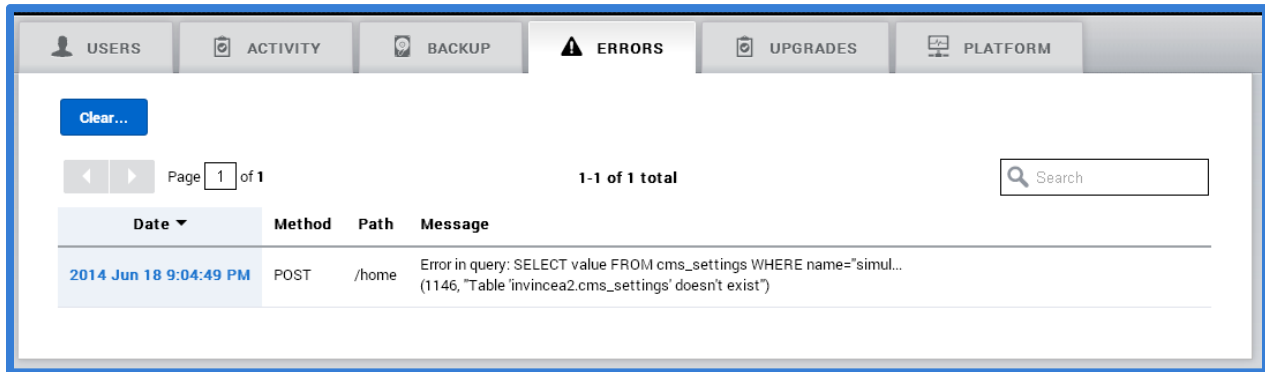


Press the “Choose File” button to select the backup file, and then press the “Upload button”. Once the database backup is uploaded, use the “restore” option to restore the database.

Note: if the database backup did not include the installation packages, they will need to be re-uploaded to the system.

Errors Tab

The Errors Tab provides a UI display of the latest errors logged by the system. These error messages may be useful in troubleshooting an issue with the DPWMS.



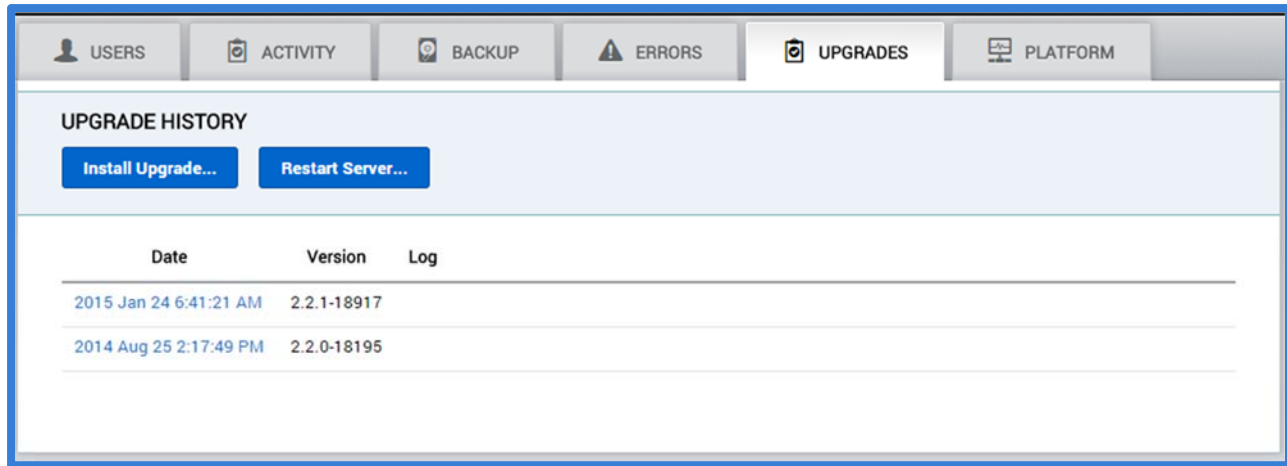
Date ▼	Method	Path	Message
2014 Jun 18 9:04:49 PM	POST	/home	Error in query: SELECT value FROM cms_settings WHERE name="simul... (1146, "Table 'invincea2.cms_settings' doesn't exist")

The table displays the error messages, with the most recent issue listed first. The table can be sorted by clicking on the column headers. If more than ten errors exist in the log, the table will display multiple pages that can be navigated and searched using the navigation bar.

The “Clear...” button can be used to clear the message from the Errors table.

Upgrades Tab

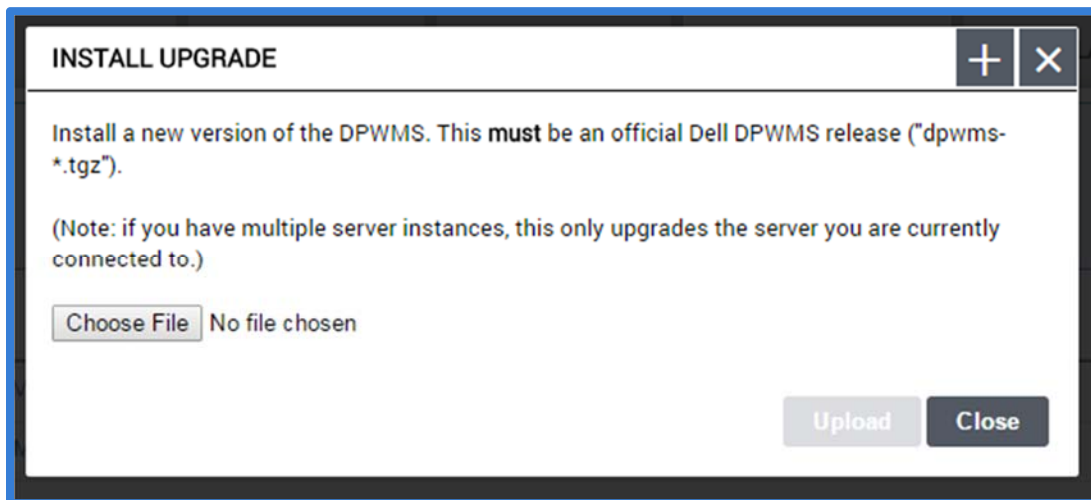
The Upgrades Tab is used to display the upgrade history of the DPWMS system and can also be used to apply new versions of the DPWMS software, as well as to restart the DPWMS process.



The Upgrade History table displays the date and version of the DPWMS software that was installed. The log entry may also display any important details about the version applied.

Upgrading the DPWMS

To apply an upgrade to DPWMS 2.0, click on the “Install Upgrade...” button.



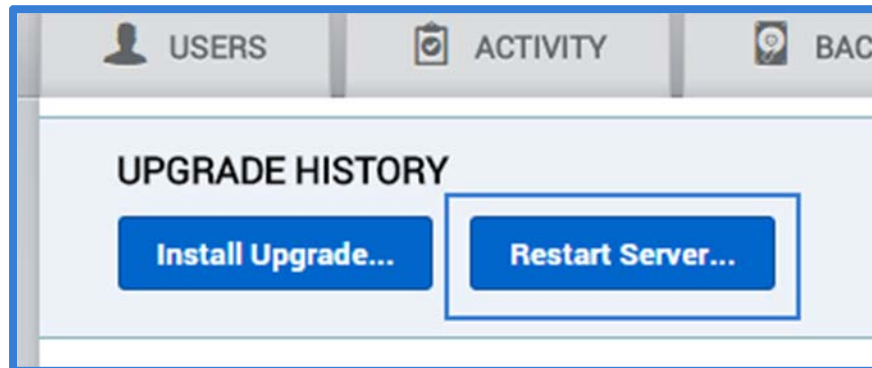
When the “Install Upgrade” dialog is displayed, press the “Choose File” button and select the upgrade file, then press the “Upload” button. To cancel the upgrade process, press the “Cancel/Close” button.

Once the upgrade has begun, it cannot be stopped. When the upgrade has finished, the UI should refresh, and the new version should be listed at the top of the list. If the browser does not refresh or times out, manually refresh the browser to display the upgraded system.

If for some reason the UI does not return, use the Custom Command section of the WebUI (port 10000) interface to restart the DPWMS 2 service.

Restarting the DPWMS Process

If the DPWMS process needs to be restarted, such as when enabling new plugins for the Threat Data module, a “Restart Server...” button is also available on the Upgrade History tab. To restart the DPWMS process on the system, press the “Restart Server...” button.



NOTE: This functionality is not supported for multiple API set ups.

Platform Tab

The Platform Tab provides some basic information about the DPWMS server, including the currently configured host name, CPU usage information, Memory usage information, and disk usage information.

IDENTITY

██████████.██████████.██████████

CPU USAGE

```
top - 09:35:16 up 4 days, 21:29, 1 user, load average: 0.00, 0.00, 0.00
Tasks: 97 total, 1 running, 96 sleeping, 0 stopped, 0 zombie
Cpu(s): 0.4%us, 0.2%sy, 0.0%ni, 98.9%id, 0.4%wa, 0.0%hi, 0.0%si, 0.0%st
```

MEMORY USAGE

	total	used	free	shared	buffers	cached
Mem:	1921452	1303988	617464	0	58200	1020944
-/+ buffers/cache:		224844	1696608			
Swap:	2097144	10052	2087092			

DISK USAGE

Filesystem	1K-blocks	Used	Available	Use%	Mounted on
/dev/mapper/VolGroup00-lv_root					

Additionally, two buttons exist at the bottom of the screen to allow access to the server's `ims.log` file and also to provide one-click button access to the backend management page (webmin).

/dev/mapper/VolGroup00-lv_home	4128448	139420	377931		
/dev/mapper/VolGroup00-lv_temp	4128448	139408	377932		
/dev/mapper/VolGroup00-lv_var	4128448	358340	356039		
/dev/mapper/VolGroup00-lv_mysql	31963056	202284	3013712		

Platform Administration Tool

Server Log

If the “Platform Administration Tool” is not visible after upgrading from DPWMS 2.0 to DPWMS 2.X, a change to the `ims.conf` file needs to be made. From the server console or via ssh, connect as the root user and use vi or a similar tool to edit the configuration file: `/var/www/html/ims2/ims.conf`

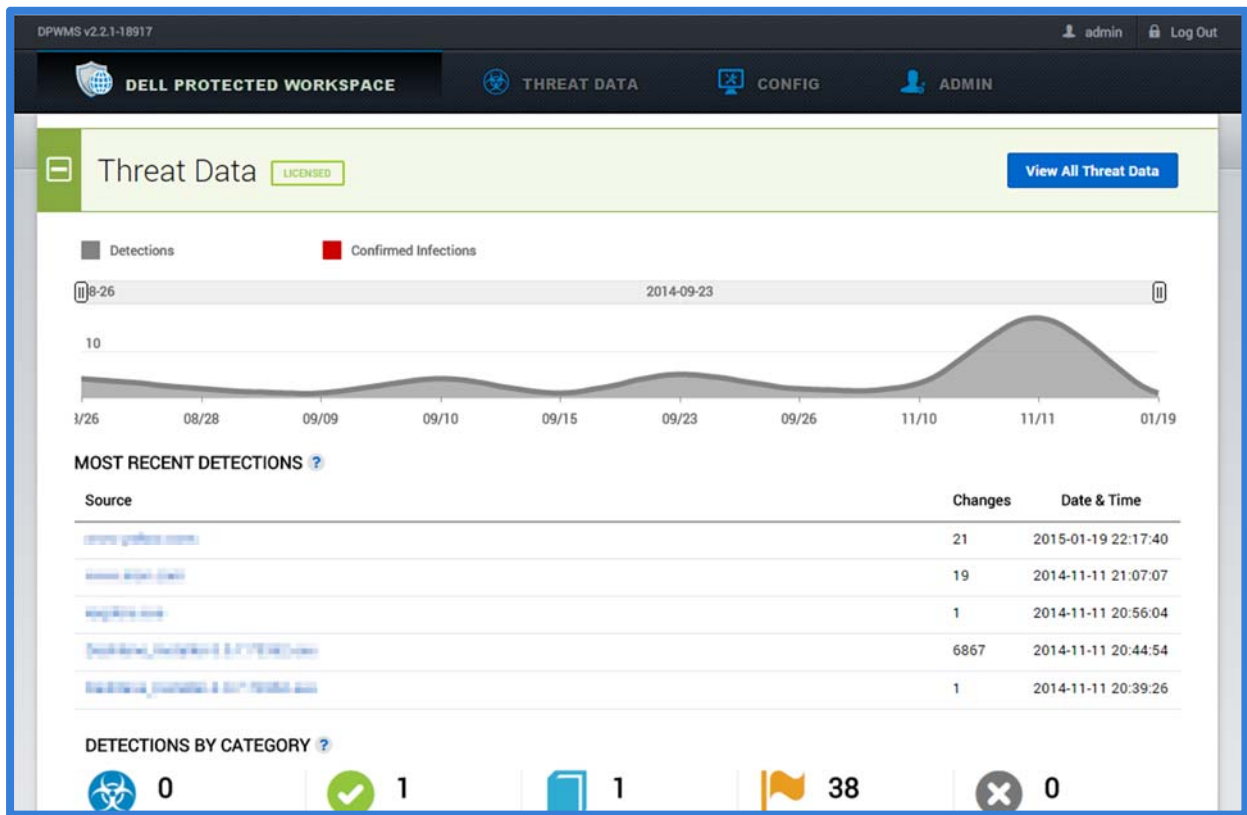
Under the existing option “`fips_enable = true`” add the following:

```
platform_admin = https://localhost:10000/
```

Once the above line has been added, save the file, and restart the `ims2` service. After the service restart, the “Platform Administrator Tool” button will now be available.

Dell Protected Workspace Home Module

The Dell Protected Workspace Home Module is a consolidated view of the Modules. This view will change based on which modules are available in the system.

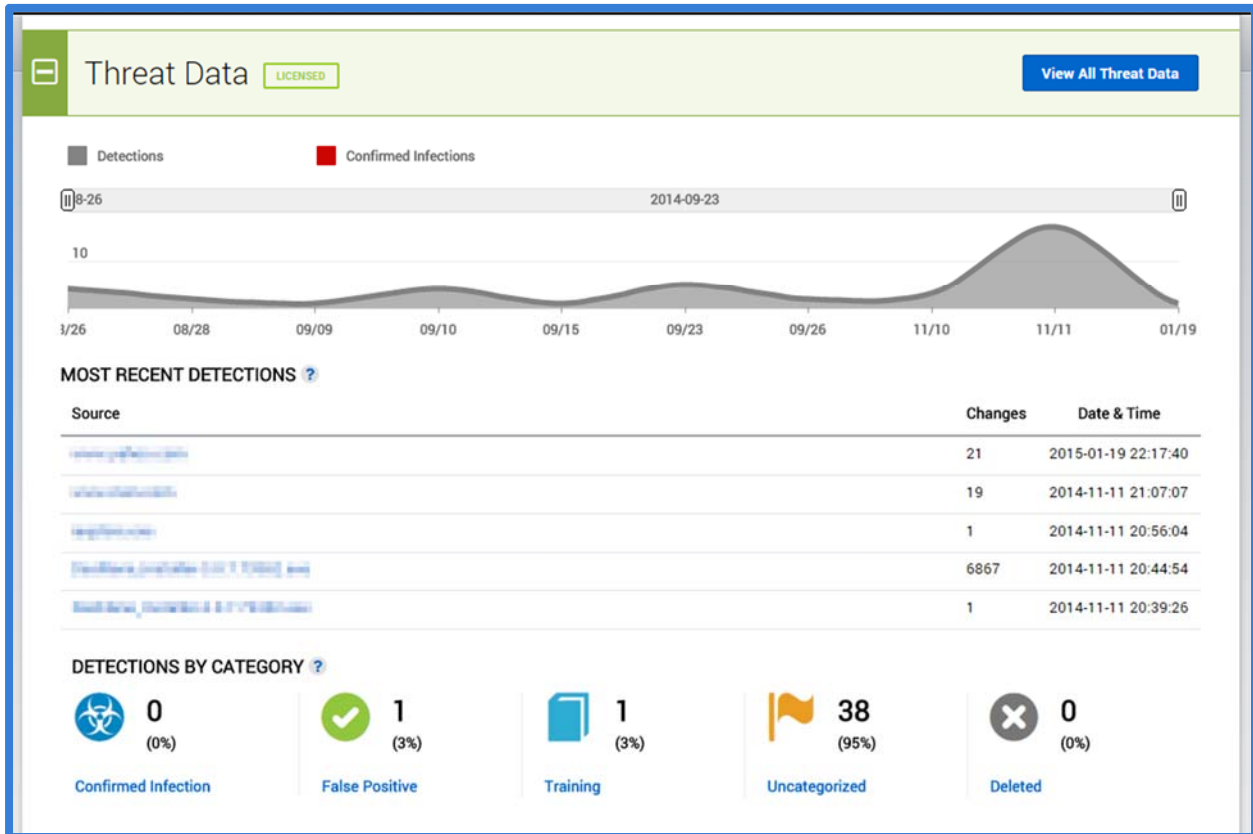


Home Tab

Threat Data Section

The Threat Data Section provides a brief overview of threats that have been reported to the system. The section header contains a “View All Threat Data” button that will direct the user to the Threat Data module.

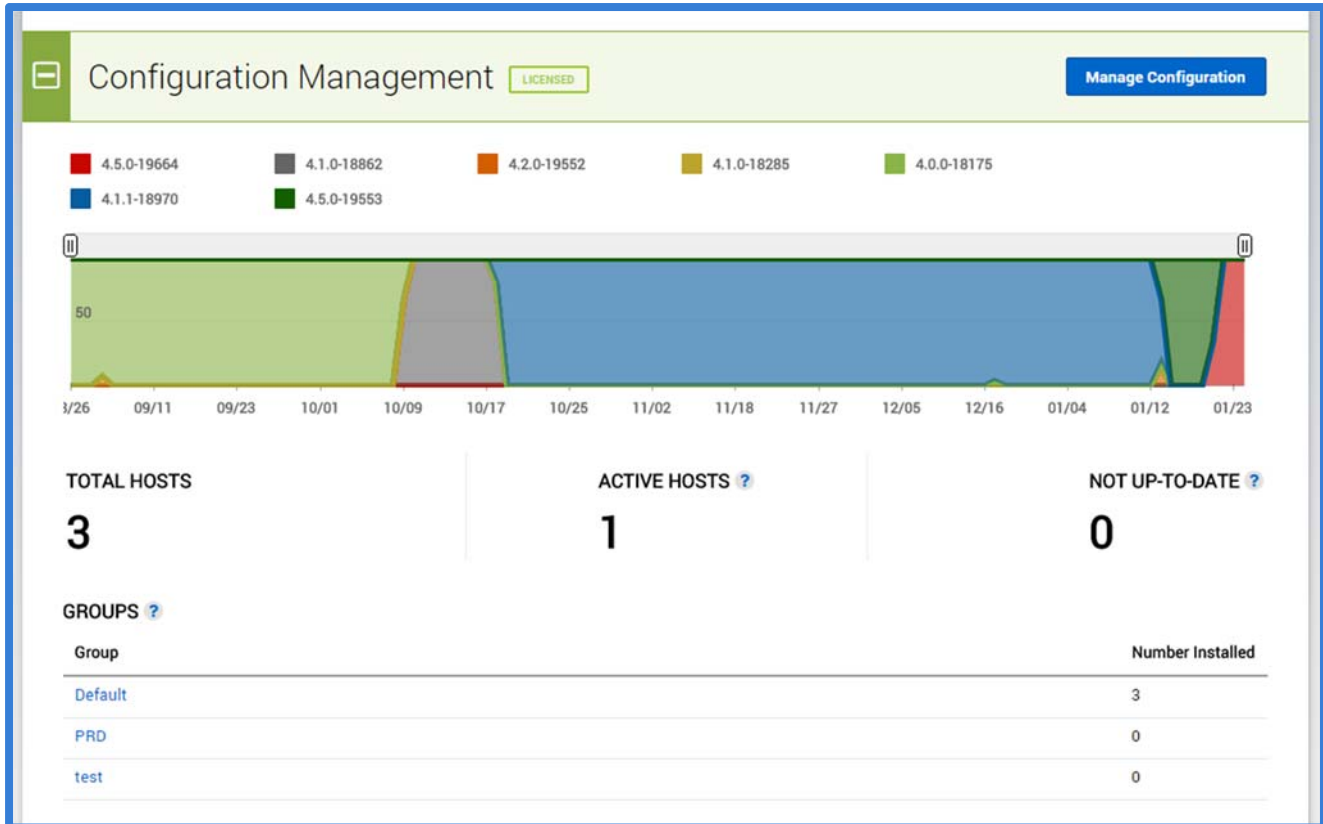
The display contains a graphical display showing the number of threat reports received per day, a chart of the most recent reports and a breakdown of the different report classifications for all reports in the Threat Data module.



Configuration Management Section

The Configuration Management section provides a brief overview of hosts that are being managed by the system. The section header contains a “Manage Configuration” button that will direct the user to the Config module.

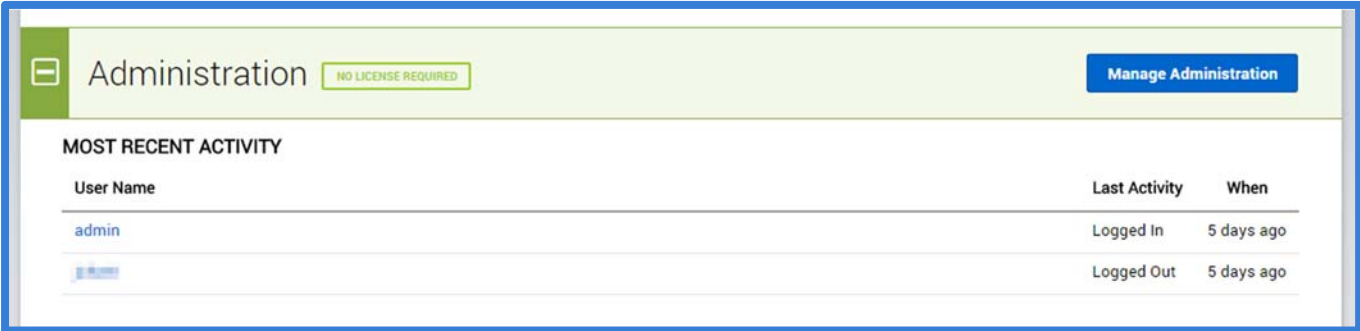
The display contains a graphical display showing the total number of hosts by version per day, a chart of the five groups with the most hosts and additional host-level statistics.



Administration Section

The Administration Section provides a brief overview of the DPWMS users. The section header contains a “Manage Administration” button that will direct the user to the Admin module.

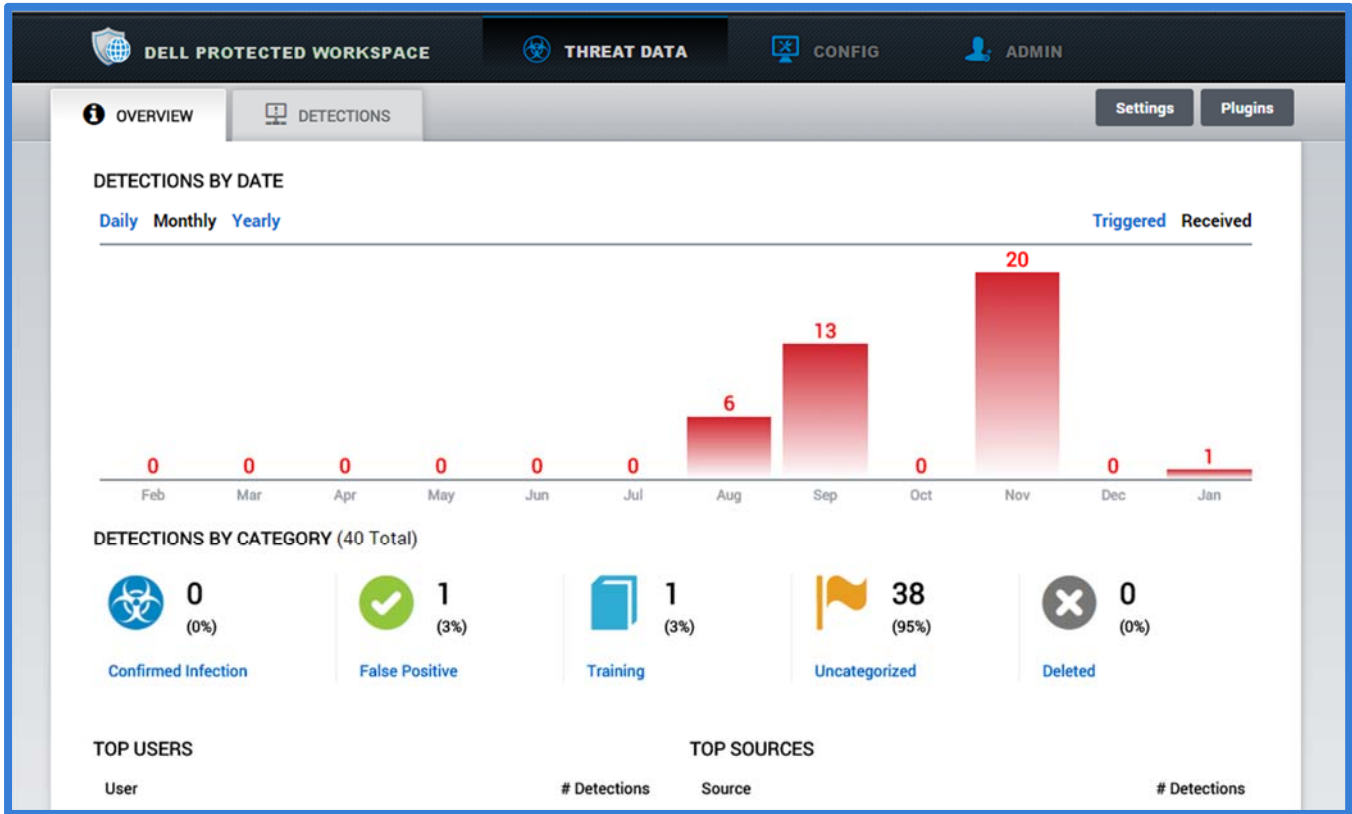
The display contains a chart showing the most recent user activity.



MOST RECENT ACTIVITY		
User Name	Last Activity	When
admin	Logged In	5 days ago
j.smith	Logged Out	5 days ago

Threats Module

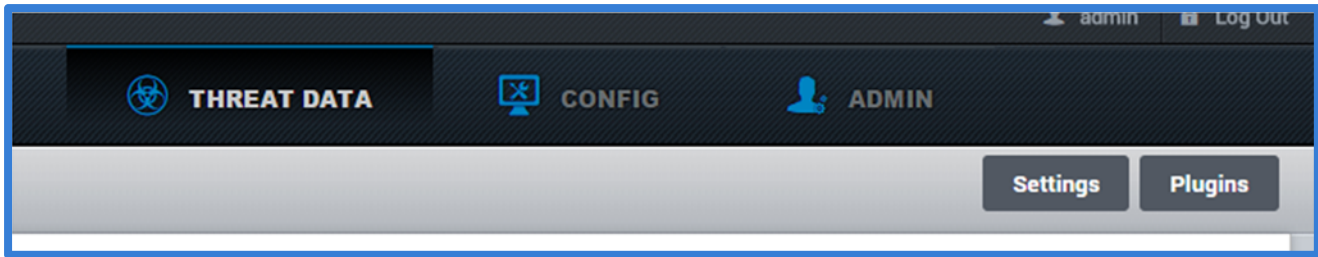
The Threats module is used to review Threat Reports that are reported by the Dell Protected Workspace client software. From this module, detailed analysis can be performed on the reports to determine the source and impact of the threat on the client system.



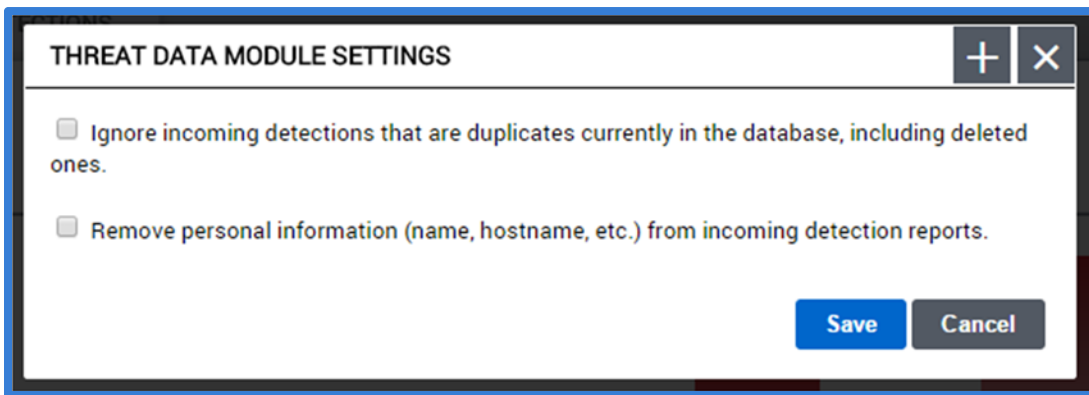
To access the Threats module, click on the Threat Data icon from the navigation bar of DPWMS. The main display for the Threats module includes two tabs, Overview and Detections.

Settings and Plugins

Additional settings for the Threat Server and for Plugins can be modified by accessing the Settings or Plugins configuration dialogs.



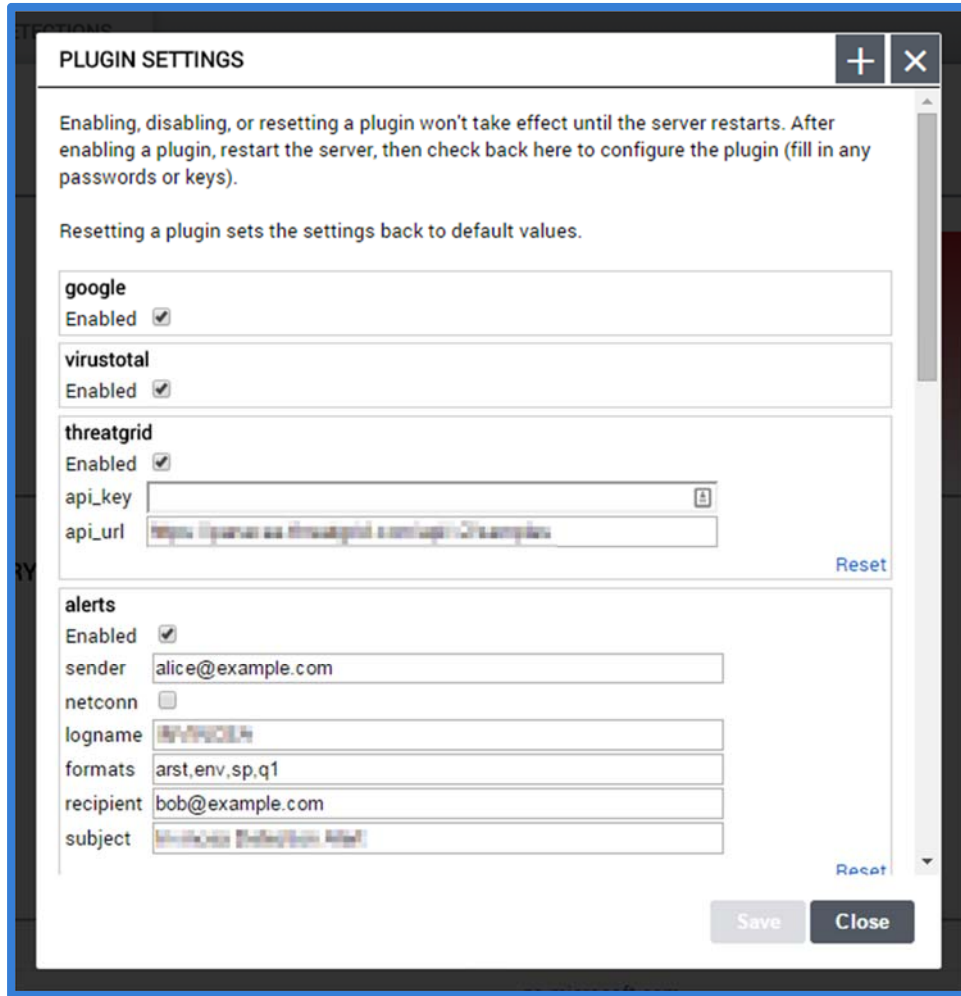
Threat Data Module Settings



Pressing the “Settings” button will display the “Threat Data Module Settings” dialog box. The following options can be configured in this dialog.

- Ignore incoming detections that are duplicates currently in the database, including deleted ones.
 - This setting ensures that if a duplicate report is sent to the system (in case a client tries to upload the report more than once) it will only be displayed once.
- Remove personal information (name, hostname, etc.) from incoming detection reports.
 - This setting allows personal information to be removed from the uploaded threat reports before they are displayed in the UI.

Plugin Settings



PLUGIN SETTINGS

Enabling, disabling, or resetting a plugin won't take effect until the server restarts. After enabling a plugin, restart the server, then check back here to configure the plugin (fill in any passwords or keys).

Resetting a plugin sets the settings back to default values.

google
Enabled

virustotal
Enabled

threatgrid
Enabled
api_key
api_url
[Reset](#)

alerts
Enabled
sender
netconn
logname
formats
recipient
subject
[Reset](#)

[Save](#) [Close](#)

Additional third-party plugins can be enabled to allow for integration with such providers as ReversingLabs, VirusTotal, ThreatGrid, Threat Stream, URLQuery, Google, Email Alerts, and iSightPartners. By enabling these plugins, additional tabs will be added to the threat report view.

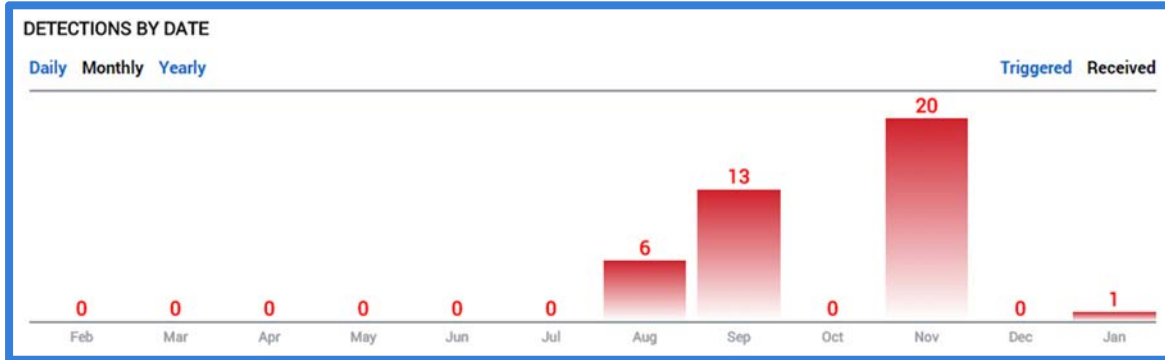
To enable a plugin, select the checkbox next to the plugin name. In order for plugins to be fully enabled, the DPWMS (ims2) service must be restarted. This can be done from the Dell Protected Workspace Home Module, under the Update History tab. Press the “Restart Server” option.

Some plugins may require additional information, such as account information. This information will need to be entered before the plugin will work properly.

Overview Tab

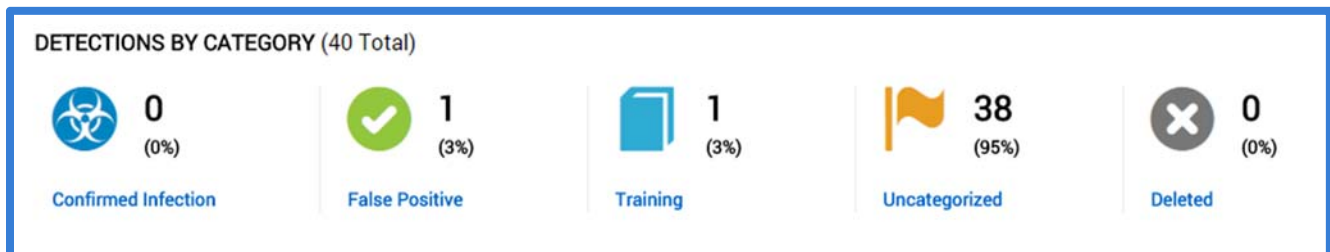
The Overview tab contains an overview of the threat reports that have been uploaded to the DPWMS. Graphs, charts and other information are provided to show statistical information about the threat reports. The overview tab is broken into four sections.

Detections by Date



This section will display incidents by 3 filters: daily, monthly, or yearly. There are also 2 other display filters on the right side of the section: triggered and received. Triggered will display when the incident occurred on the end user's machine. Received will display when the incident was uploaded to the Threat Data Module.

Detections by Category



This section displays the number of each type of incident by category.

- **Confirmed Infection** – The total number of threat reports that have been flagged as actual infections Dell Protected Workspace was able to protect the host system from.
- **False Positive** – The total number of threat reports that have been identified as false positives (by trusted processes not whitelisted in the Dell Protected Workspace default configuration).
- **Training** – The total number of threat reports marked for rules training, to create custom suppression rules for the Dell Protected Workspace detection engine.
- **Uncategorized** – The total number of threat reports that have yet to be categorized.
- **Deleted** – The number of threat reports that have been deleted from the Threat Data module.

Top Users and Top Sources

This section displays the number of incidents for the top users with the most threat reports sent to the Threat Data module and the top sources that existed in threat reports sent to the Threat Data module.

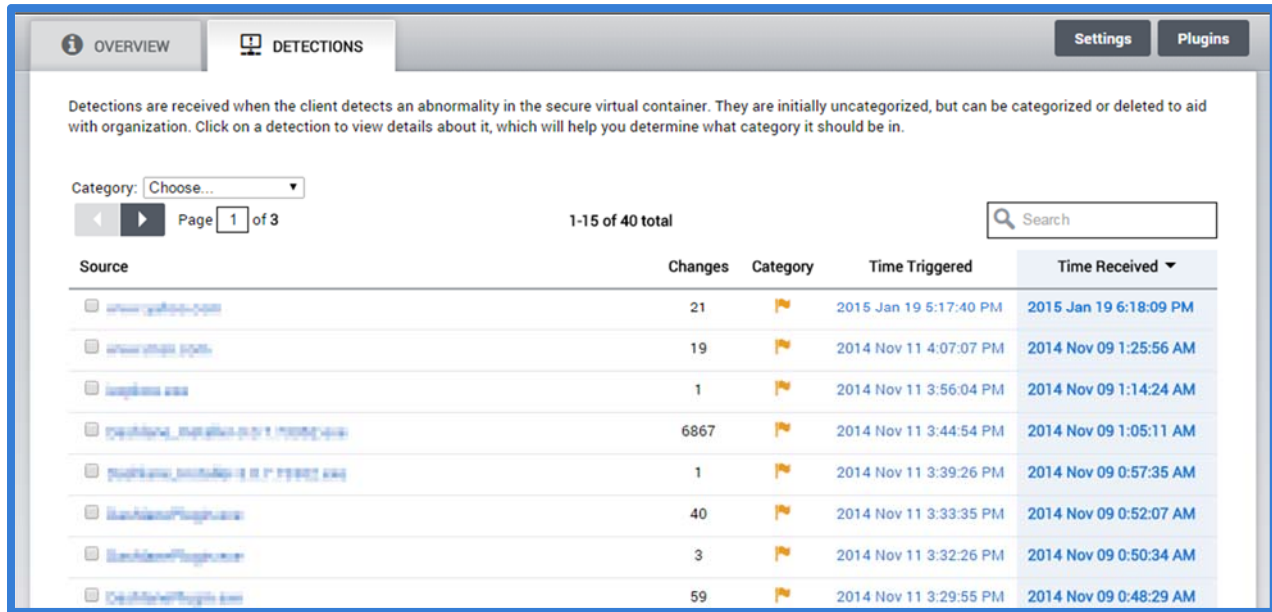
TOP USERS		TOP SOURCES	
User	# Detections	Source	# Detections
jamas.ihumanes@	40	http://www.foxit.com/	13
		http://microsoft.com/	5

Top Users – Displays the users in descending order based off of the number of threat reports that have been submitted to the Threat Data module.

Top Sources - Displays the most reported sources (websites, document file name, etc.) that have been in reports sent to the Threat Data module.

Detections Tab

The Detections Tab of the Threats module displays a summary of fifteen threat reports. The details of any report can be viewed by clicking on the source name for the selected report.



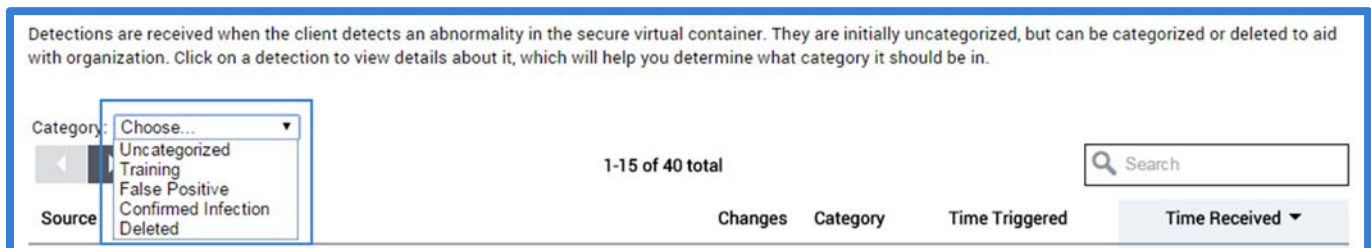
The screenshot shows the 'DETECTIONS' tab in the Threats module. It includes a 'Settings' and 'Plugins' button in the top right. Below the navigation tabs, there is a descriptive text: 'Detections are received when the client detects an abnormality in the secure virtual container. They are initially uncategorized, but can be categorized or deleted to aid with organization. Click on a detection to view details about it, which will help you determine what category it should be in.'

Below the text, there is a 'Category:' dropdown menu set to 'Choose...', a 'Page 1 of 3' indicator, and a '1-15 of 40 total' count. A search box is also present.

Source	Changes	Category	Time Triggered	Time Received
www.google.com	21	Uncategorized	2015 Jan 19 5:17:40 PM	2015 Jan 19 6:18:09 PM
www.google.com	19	Uncategorized	2014 Nov 11 4:07:07 PM	2014 Nov 09 1:25:56 AM
www.google.com	1	Uncategorized	2014 Nov 11 3:56:04 PM	2014 Nov 09 1:14:24 AM
www.google.com	6867	Uncategorized	2014 Nov 11 3:44:54 PM	2014 Nov 09 1:05:11 AM
www.google.com	1	Uncategorized	2014 Nov 11 3:39:26 PM	2014 Nov 09 0:57:35 AM
www.google.com	40	Uncategorized	2014 Nov 11 3:33:35 PM	2014 Nov 09 0:52:07 AM
www.google.com	3	Uncategorized	2014 Nov 11 3:32:26 PM	2014 Nov 09 0:50:34 AM
www.google.com	59	Uncategorized	2014 Nov 11 3:29:55 PM	2014 Nov 09 0:48:29 AM

The detections table can be filtered to only display certain categories of threat reports by selecting a category in the “Category” drop-down menu.

To filter the threats by category, use the drop-down box, and then select which category to display. The options are as follows: Uncategorized, Training, False Positive, Confirmed Infection, and Deleted.

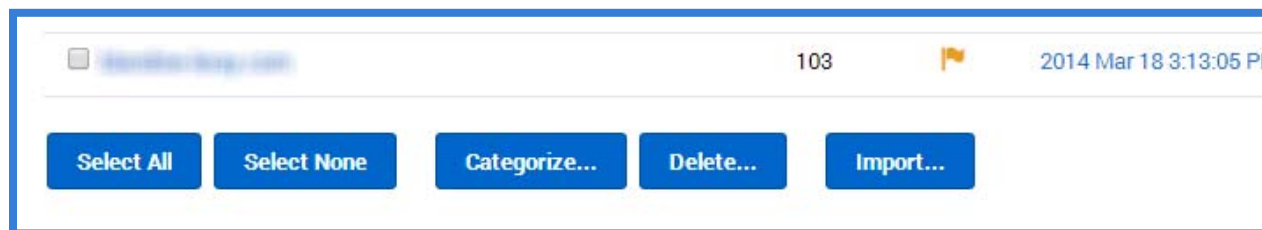


This screenshot shows the same interface as the previous one, but with the 'Category:' dropdown menu open. The menu options are: 'Uncategorized', 'Training', 'False Positive', 'Confirmed Infection', and 'Deleted'. The 'Source' column header is also visible.

Source	Changes	Category	Time Triggered	Time Received
1-15 of 40 total				

The column headings can also be used to sort the display view. Click on a column heading to sort by that column. Additionally, the search box can be used to search the threat report information for specific information, such as user, host name, source and other information.

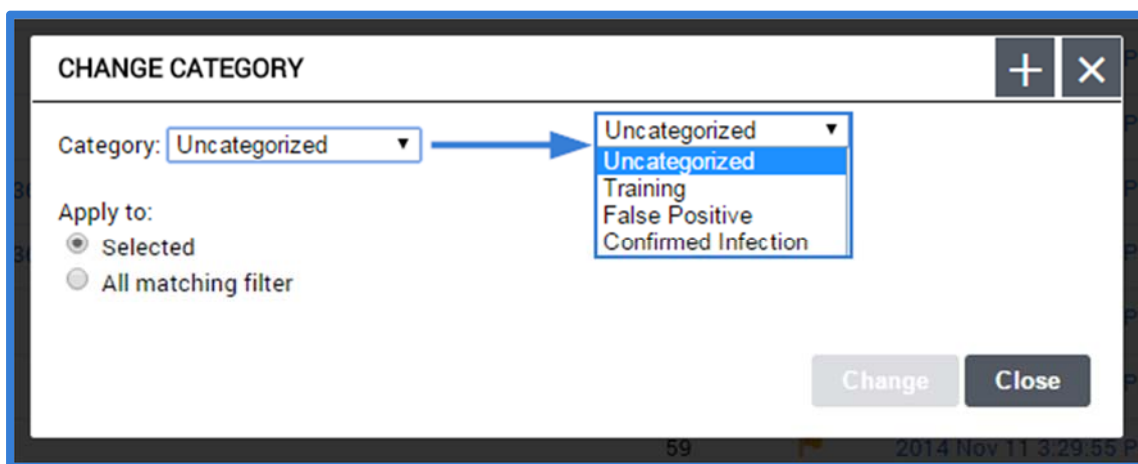
The detections tab provides the ability to manually import threat reports, modify threat report categories and delete threat reports from the DPWMS system through a series of buttons that exist below the incidents table.



The "Select All" and "Select None" buttons are used to work with the currently displayed page of threat reports. The "Select All" button will select the threat reports that are currently displayed in the table (up to 15 reports). The "Select None" button will unselect any reports that are currently selected. An individual report can also be selected or unselected at any time by clicking on the checkbox at the beginning of the threat reports line in the table.

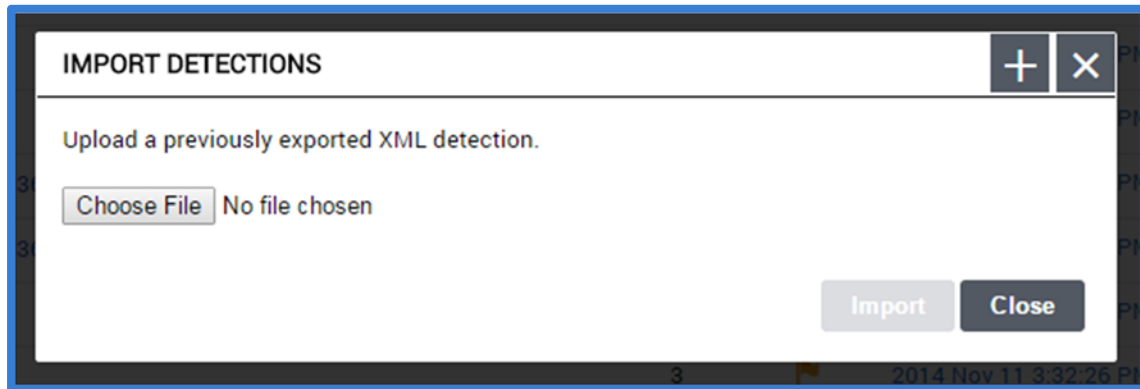
Threat Categories

Threat reports can be categorized in the Threats module to see which reports have been reviewed and what classification the report falls into. The Threat Data module has four different categories available for the threat reports. Every report must belong to one of these categories.



- *Uncategorized* – All threat reports which have not yet been categorized.
- *Training* – A threat report that is being used to create a custom set of threat detection rules to suppress a false positive report.
- *False Positive* – A threat report from a client machine that is a trusted action, but is not part of the default rule set in the Dell Protected Workspace Detection Engine.
- *Confirmed Infection* – A threat report that has been confirmed as an actual threat.

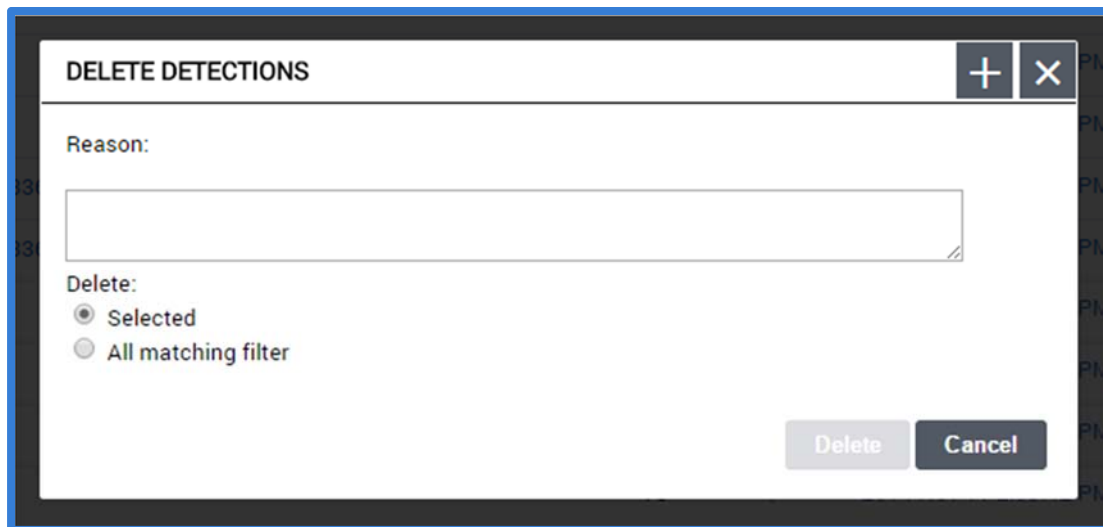
To manually import an infection report, click the “Import” button from the series of buttons below the threat reports table.



From the Import dialog box, press the “Choose File” button and locate the XML report file to upload. Once the file is selected, press the “Upload” button.

Once the report import has finished, the report will be displayed on the Detections tab.

The delete button allows a threat report to be deleted from the Threat Data Module. Before the report is deleted, a confirmation dialog will display and a reason for deletion of the report must be provided. Deleting a report removes that report from the UI, but retains some of the information in the database, along with the reason for deletion.



From the Delete Detections dialog, enter a reason for deleting the selected threat report and press the “Delete” button to remove the report from the system.

Report Overview Page

The details of a threat report can be viewed by clicking the Source hyperlink of the report in the incidents table. The reports details will then be displayed so that the threat report can be reviewed in detail.

The heading bar at the top of the report details provides a color code based on the category assigned to the report. To change the Category of a threat report, click the “Categorize...” button and select the desired category.

UNCATEGORIZED (#296)
Unauthorized Launch of a Monitored File: [www.abc.com](#) [Categorize...](#)

STATISTICS CONFIGURATION APPLICATIONS

Statistic	Total
Executables Written	4
Processes Launched	3
Connections Opened	2
System Changes	29

ANALYSIS EVENT TREE TIMELINE GEOGRAPHY THREATGRID REVERSINGLABS THREATSTREAM

- ▶ ● Files written to disk were launched as processes
- ▶ ● Internet Settings in the registry were modified
- ▶ ● Executable files were created on disk
- ▶ ● A listener for accepting network communications was set up on port 80
- ▶ ● Network communications were sent to Germany
- ▶ ● A suspect process was launched by Internet Explorer
- ▶ ● A file was written to the application data directory
- ▶ ● Files were written to the temporary directory
- ▶ ● Multiple processes wrote to the same file
- ▶ ● Network traffic was sent using the HTTP protocol
- ▶ ● The source website contained multiple iframes

From 2014 Apr 04 12:29:50 PM (Received on 2014 Apr 03 8:03:45 AM) [Export...](#) [Allow...](#) [Delete...](#)

The next section of the report is split into three different sections:

Statistics

This section contains statistics about the threat report, based on actions that occurred.

- Executables Written – Displays the number of executable files written to the container.
- Processes Launched – Displays the number of processes launched in the report.
- Connections Opened – Displays the number of network modifications (TCP connect, TCP listen) made to/from the system.
- System Changes – Displays the number of changes made to the container before the threat stopped or the container was restored.

Configuration

The Configuration section contains additional information about the host system and user that uploaded the Threat Report.

The screenshot shows the configuration details for an unclassified threat report. The page has a blue header with a flag icon, the text "UNCATEGORIZED (#296)", and "Unauthorized Launch of a Monitored File: www.dell.com". A "Categorize..." button is in the top right. Below the header are three tabs: "STATISTICS", "CONFIGURATION" (selected), and "APPLICATIONS". The main content is a table with two columns: "Property" and "Value".

Property	Value
Product	Invincea Enterprise
Version	3.3.1-17011
Protocol	1.8
Operating System	Windows 7 32-bit
User	Admin
Host	[REDACTED]
Local IP	[REDACTED]
Activation Key	[REDACTED]
Host Descriptor	.H6Cz4pc3KFpB.zm4Qi48Q.2yGnk4EFod0x2XX
Service Tag	
User Action	Restored
Delete Downloads	×
Delete Source	×
Infection Warning	✓
Rule Training	×

At the bottom of the page are several navigation tabs: "ANALYSIS" (selected), "EVENT TREE", "TIMELINE", "GEOGRAPHY", "THREATGRID", "REVERSINGLABS", and "THREATSTREAM".

Displayed Information:

Product – Displays which flavor of Dell Protected Workspace is running on the machine that reported the alert.

Version – Displays which version of Dell Protected Workspace is running on the machine that reported the alert.

Protocol – Displays the threat protocol number.

Operating System – Displays the Operating System of the machine at the time of the alert.

User – Displays the user ID of the user logged in during the time of the alerts (not available if the anonymize option is enabled).

Host – Displays the machine name of the machine at the time of the alert (not available if the anonymize option is enabled).

Local IP - Displays the IP address of the machine at the time of the alert (not available if the anonymize option is enabled).

Activation Key – Displays the activation key of the machine at the time of the infection, if available.

Host Descriptor – Displays the unique host identifier for the machine at the time of the alert.

Service Tag – Not currently used.

User Action – Displays what action was taken after the alert occurred (Restored/Ignored).

Delete Downloads – Displays a red X or a green checkmark depending on whether or not all downloads during that session were deleted.

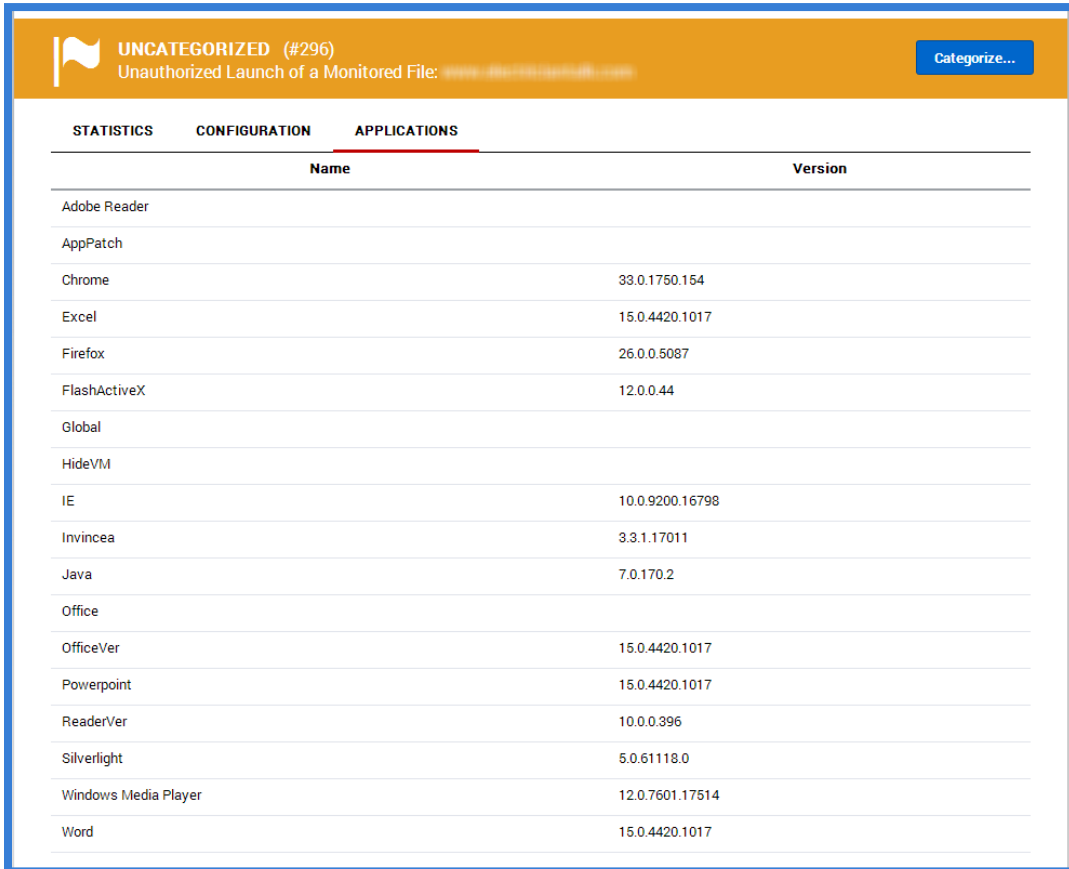
Delete Source – Displays a red X or a green checkmark depending on whether or not the document responsible for the infection during that session was deleted.

Infection Warning - Displays a red X or a green checkmark depending on whether or not the end user received a notification of infection.

Rule Training - Displays a red X or a green checkmark depending on whether or not this infection was categorized as Training.

Applications

The Applications section displays a list of the applications that were available in the secure container during the alert (apps are defined in the default product and custom apps file). The versions for the applications are displayed when they are available.



Name	Version
Adobe Reader	
AppPatch	
Chrome	33.0.1750.154
Excel	15.0.4420.1017
Firefox	26.0.0.5087
FlashActiveX	12.0.0.44
Global	
HideVM	
IE	10.0.9200.16798
Invincea	3.3.1.17011
Java	7.0.170.2
Office	
OfficeVer	15.0.4420.1017
Powerpoint	15.0.4420.1017
ReaderVer	10.0.0.396
Silverlight	5.0.61118.0
Windows Media Player	12.0.7601.17514
Word	15.0.4420.1017

Threat Report Analysis Tab

The Analysis tab provides the common display of the Threat report that a user can see from the Dell Protected Workspace product when the Threat is detected. This display categorizes the actions based on five severity levels: Red, Orange, Yellow, Green and Blue

Each categorized line can be expanded so that the contents can be reviewed.

The screenshot displays the 'ANALYSIS' tab of a threat report. The interface includes a navigation bar with tabs: ANALYSIS, EVENT TREE, TIMELINE, GEOGRAPHY, THREATGRID, REVERSINGLABS, and THREATSTREAM. The main content area shows a list of events, each with a colored icon indicating its severity level and a list of sub-items. The events are as follows:

- Files written to disk were launched as processes** (Red icon)
 - F2uwh.exe
 - zxmlsub.exe
- Internet Settings in the registry were modified** (Orange icon)
 - Internet Settings
 - Proxy
 - ZoneMap
- Executable files were created on disk** (Yellow icon)
 - F2uwh.exe
 - zxmlsub.exe
- A listener for accepting network communications was set up on port 80** (Yellow icon)
 - 80
- Network communications were sent to Germany** (Yellow icon)
 - Germany
- A suspect process was launched by Internet Explorer** (Yellow icon)
 - F2uwh.exe
- A file was written to the application data directory** (Green icon)
 - [Container]\user\current\AppData\Roaming\Invincea\Enterprise\IE5\L5GKA1ZF\F2uwh.exe
- Files were written to the temporary directory** (Green icon)
 - [Container]\user\current\AppData\Local\Temp\nscAAE0.tmp
 - [Container]\user\current\AppData\Local\Temp\setup.dat
 - [Container]\user\current\AppData\Local\Temp\zxmlsub.exe
- Multiple processes wrote to the same file** (Green icon)
 - inv_hook.log
- Network traffic was sent using the HTTP protocol** (Green icon)
 - HTTP
- The source website contained multiple iframes** (Blue icon)
 - <http://caploz.in.ua/5butqfk/?2>
 - http://googleads.g.doubleclick.net/pagead/ads?client=ca-pub-8808028116415421&format=600x225&output=html&h=225&adk=2123412315&w=600&imt=1396628966&tfs=16&channel=1322520813&color_link=%2300:help-ibew-apprentice-test-1877%2F&uiv=1&dt=1396628966314&bpp=24&shv=r20140401&cbv=r20140311&saldr=sa&prev_fmfs=600x225%2C600x225&prev_slotnames=85694764897734-17&u_tz=-240&u_his=3&u_java=1&u_h=938&u_w=1875&u_ah=898&u_aw=1875&u_cd=24&u_nplug=0&u_nmime=0&dff=times%20new%20roman&dfs=13&a-help-ibew-apprentice-test-1877%252F%26ei%3D490-U5StDaGr2QWeh4HwDg%26usg%3DAFqjCNFHqUE_k0D3Ino-

Threat Report Event Tree Tab

The Event Tree tab window provides a hierarchical view of the threat. The display shows parent and sub-events. The display has the ability to be filtered, so specific event types (Process, File, Registry, Network and Module Load) can be displayed. By default, all filters are displayed except for the Module Load filter.

The screenshot displays the 'EVENT TREE' tab in the Threat Report interface. The 'Type' filter is set to 'Process'. The event tree shows a sequence of process launches:

- Process Launch: [Invincea]\Sandbox\Start.exe
 - Process Launch: [Invincea]\Sandbox\SandboxRpcSs.exe
 - Process Launch: [CommonAppData]\Invincea\Enterprise\Bin\InvProtectAgent.exe
 - Process Launch: [CommonAppData]\Invincea\Enterprise\Bin\InvProtectAgent.exe
 - Process Launch: [Firefox]\firefox.exe
 - Process Launch: [Firefox]\firefox.exe
 - Process Launch: [IE]\iexplore.exe
 - Process Launch: [IE]\iexplore.exe
 - Process Launch: [Invincea]\Sandbox\SandboxCrypto.exe
 - Process Launch: [Invincea]\Sandbox\SandboxCrypto.exe
 - Process Launch: [Java]\bin\javaw.exe
 - Process Launch: [Java]\bin\javaw.exe
 - Process Launch: [Java]\bin\javaw.exe
 - Process Launch: [Java]\bin\jp2launcher.exe
 - Process Launch: [Silverlight]\agcp.exe
 - File Create: [Container]\user...\F2uwh.exe
 - File Write: [Container]\user...\F2uwh.exe
 - Process Launch: [Container]\user...\F2uwh.exe**
 - File Create: [Container]\user\current\AppData\Local\Invincea
 - File Create: [Container]\user\current\AppData\Local\Invincea\Enterprise
 - File Create: [Container]\user\current\AppData\Local\Invincea\Enterprise\Shared
 - File Create: [Container]\user...\inv_hook.log
 - File Write: [Container]\user...\inv_hook.log
 - File Create: [Container]\user\current\AppData\Local\Temp\nscAAE0.tmp
 - File Create: [Container]\user\current\AppData\Local\Temp\zxmlsub.exe
 - File Write: [Container]\user\current\AppData\Local\Temp\zxmlsub.exe
 - File Create: [Container]\user\current\AppData\Local\Temp\setup.dat
 - File Write: [Container]\user\current\AppData\Local\Temp\setup.dat
 - Process Launch: [Container]\user\current\AppData\Local\Temp\zxmlsub.exe**
 - File Write: [Container]\user...\inv_hook.log

Events are grouped on a second-by-second basis and a prefix with the event type (process launch, file written, URL, etc.). Clicking on a specific event brings up the details of that event.

The screenshot shows the 'PROCESS LAUNCH' details window. The properties and values are as follows:

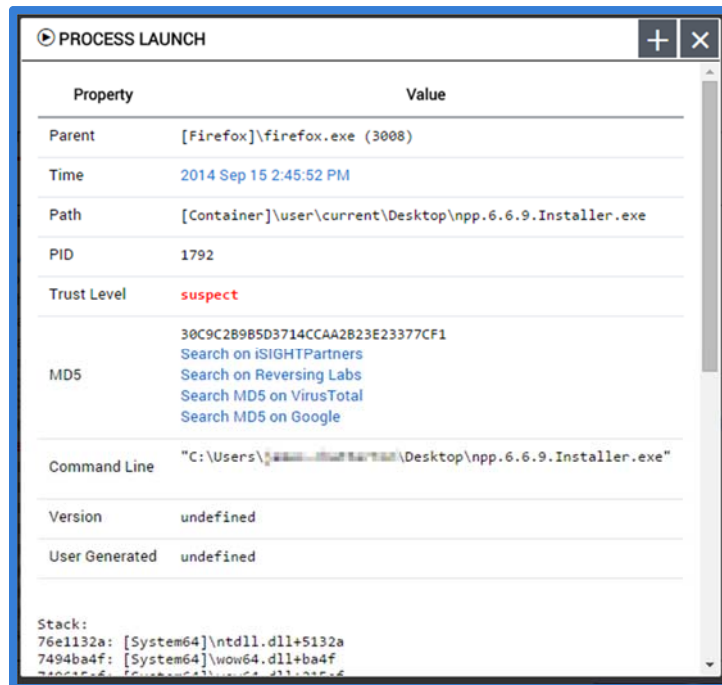
Property	Value
Parent	[IE]\iexplore.exe (3740)
Time	2014 Apr 04 12:28:58 PM
Path	[IE]\iexplore.exe
PID	2396
Trust Level	untrusted
MD5	Unknown Search MD5 on VirusTotal
Command Line	undefined
Version	undefined
User Generated	undefined

Stack:
 77805784: [System32]\ntdll.dll+45784
 77470eff: [System32]\kernel32.dll+50eff
 1d1968: [Invincea]\Sandbox\SboxD11.dll+31968
 1d2cea: [Invincea]\Sandbox\SboxD11.dll+32cea
 77455a2c: [System32]\kernel32.dll+35a2c
 76ffd7f1: [System32]\iertutil.dll+fd7f1
 76ff6f90: [System32]\iertutil.dll+f6f90

For threat reports that were triggered by an untrusted process, the triggering process (that caused the threat report) will be displayed in Red to help easily identify it.



All process entries contain additional details about the process (some will display options used during the process launch). When third-party integration is enabled for the Threat Data module, these plugins can be used to for additional analysis.



Threat Report Timeline Tab

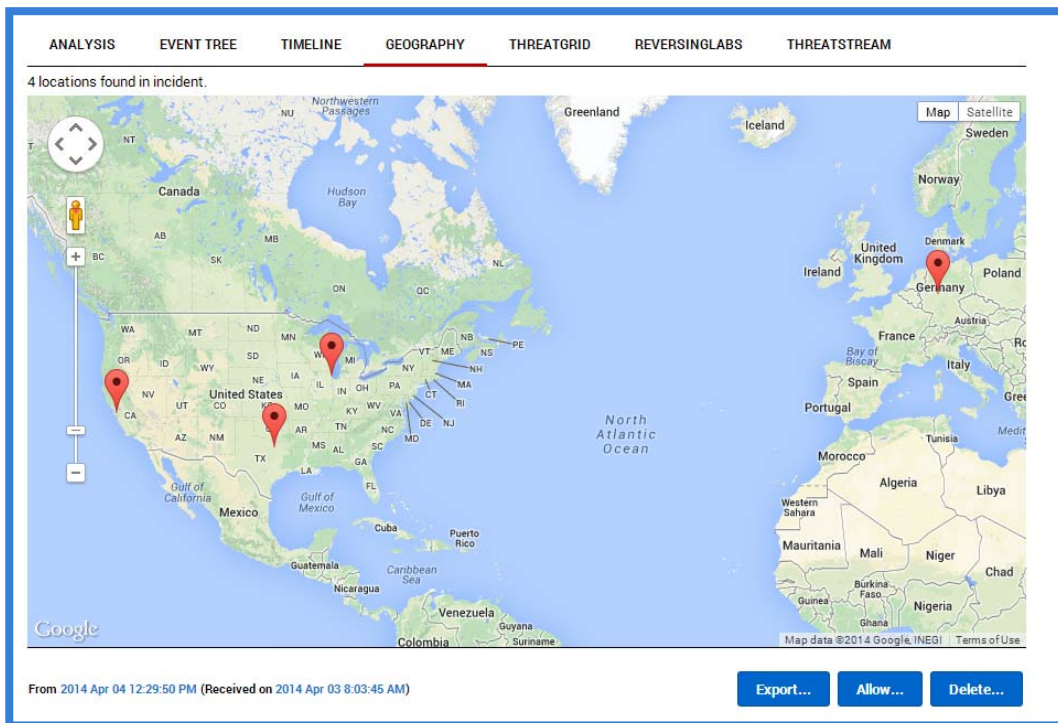
The Timeline tab provides the time-based display of all the actions that occurred during the threat. The display has the ability to be filtered, so specific event types (Process, File, Registry, Network and Module Load) can be displayed. By default, all filters are displayed except for the Module Load filter.

THREATSTREAM	THREATGRID
Type: <input checked="" type="checkbox"/> Process <input checked="" type="checkbox"/> File <input checked="" type="checkbox"/> Registry <input checked="" type="checkbox"/> Network <input type="checkbox"/> Module Load	
2014 Apr 11 9:43:53 AM	Process Launch: [Invincea]\Sandbox\Start.exe Process Launch: [Invincea]\Sandbox\SandboxRpcSs.exe Process Launch: [Invincea]\Sandbox\SandboxDcomLaunch.exe
2014 Apr 11 9:43:55 AM	Process Launch: [CommonAppData]\Invincea\Enterprise\Bin\InvProtectAgent.exe Process Launch: [CommonAppData]\Invincea\Enterprise\Bin\InvProtectAgent.exe
2014 Apr 11 9:44:01 AM	Process Launch: [IE]\iexplore.exe
2014 Apr 11 9:44:02 AM	Process Launch: [IE]\iexplore.exe
2014 Apr 11 9:44:03 AM	Process Launch: [System32]\dllhost.exe
2014 Apr 11 9:44:05 AM	Process Launch: [System32]\dllhost.exe Process Launch: [Invincea]\Sandbox\SandboxCrypto.exe Process Launch: [Invincea]\Sandbox\SandboxCrypto.exe Process Launch: [Invincea]\Sandbox\SandboxCrypto.exe Process Launch: [Invincea]\Sandbox\SandboxCrypto.exe
2014 Apr 11 9:44:06 AM	Process Launch: [Invincea]\Sandbox\SandboxCrypto.exe Process Launch: [Invincea]\Sandbox\SandboxCrypto.exe Process Launch: [Invincea]\Sandbox\SandboxCrypto.exe
2014 Apr 11 9:44:17 AM	Process Launch: [System32]\rundll32.exe Process Launch: [System32]\rundll32.exe Process Launch: [System32]\rundll32.exe
2014 Apr 11 9:44:20 AM	Process Launch: [System32]\dllhost.exe Process Launch: [System32]\dllhost.exe
2014 Apr 11 9:44:23 AM	Process Launch: [IE]\iexplore.exe
2014 Apr 11 9:44:26 AM	Process Launch: [IE]\iexplore.exe
2014 Apr 11 9:46:53 AM	Process Launch: [System32]\cmd.exe

Similar to the Event Tree display, each line contains a hyperlink which displays additional information.

Threat Report Geography Tab

The geography tab displays a geo-lookup view of the threat to identify where any outbound connections that were made by the threat are located on a map. A connection line will display between these connections and the DPWMS home location.

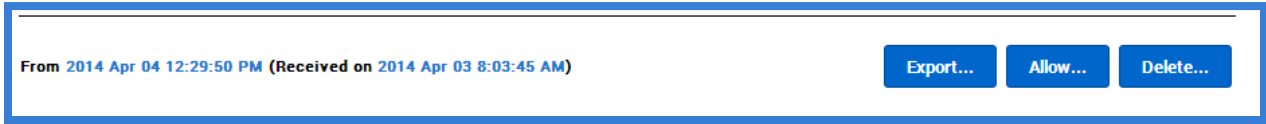


Threat Report Plugin Tabs

Additional tabs may also be displayed, based on which Threat Data module plugins have been enabled.

Threat Report Actions:

There are several additional actions that can be done with a threat report. The following outlines what the available actions are.



From 2014 Apr 04 12:29:50 PM (Received on 2014 Apr 03 8:03:45 AM)

Export...

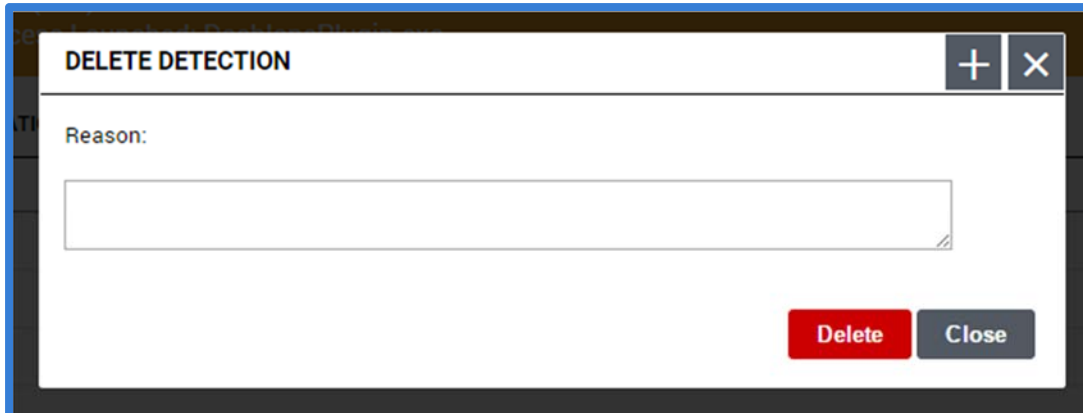
Allow...

Delete...

Export – The Export Detection dialog menu provides the option to export the threat report. Available formats are XML, CSV, and JSON. There is also an option to view the export in a new tab instead of downloading.

Allow – The allow button displays a custom rule snippet to allow the displayed detection to not be triggered in the future. This partial snippet can be added to a custom_app snippet that contains all of the necessary information needed to allow an application to run within Dell Protected Workspace.

Delete – The delete button allows a threat report to be deleted from the Threats Module. Before the report is deleted, a confirmation dialog will display and a reason for deletion of the report must be provided. Deleting a report removes that report from the UI, but retains some of the information in the database, along with the reason for deletion.



DELETE DETECTION

Reason:

Delete Close

Configuration Module

The Configuration Module provides the ability to control client configuration files and software versions from a centralized system. Client machines can be separated into different groups to allow for custom configurations on the group level. The follow section reviews the Configuration Module and its functions.

Hosts

The Configuration Module creates a unique descriptor for each host entry, regardless of the user or hostname of the system. However, the last reported hostname is used as the display name for a host entry to allow admins to identify the host in the DPWMS. A host is added to the DPWMS database on installation of the Enterprise client, if the client software is configured to connect to a DPWMS and the DPWMS is available. It will display in the UI in the Default group after installation or after the first successful heartbeat into the DPWMS. A host will remain in the UI, regardless of whether the client system still has the software installed. If a host needs to be removed from the system, it can be deleted.

Groups

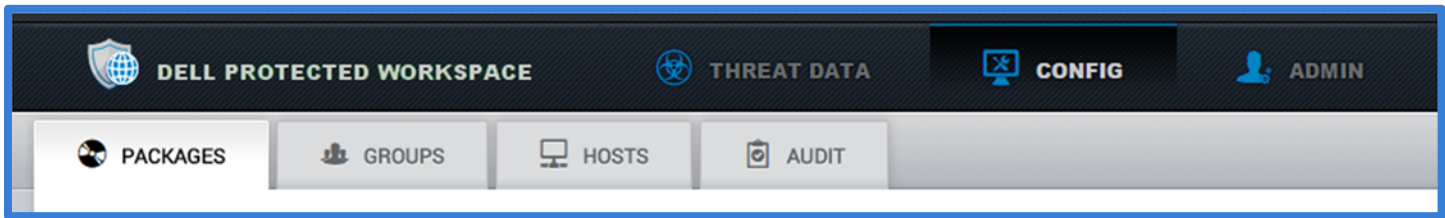
The Configuration Module applies configuration files on a per group basis. This allows for the administrator to group together hosts that will require the same configuration. The system includes one Default group (which cannot be deleted). The Default group will be the group that new clients are added to at time of installation; therefore it is important that this group always contains a valid configuration. If all clients will receive the same configuration, the Default group can be used and no additional groups need to be created.

Packages

Starting with DPWMS 2.0, the concept of a package is introduced. In previous versions of the DPWMS, when a new version of the client software was added to the DPWMS, only the product installer was used. This allowed for mismatched client software and configuration versions. As of DPWMS 2.0, instead of only the product installer, the entire installation kit, or “package”, is now uploaded to the system. This allows the DPWMS to associate specific configuration files with the correct version of the client software and ensures that there are no further mismatches between client software and configuration versions.

Accessing the Configuration Module

The Configuration Module is accessed by clicking on the “Config” button in the navigation bar.

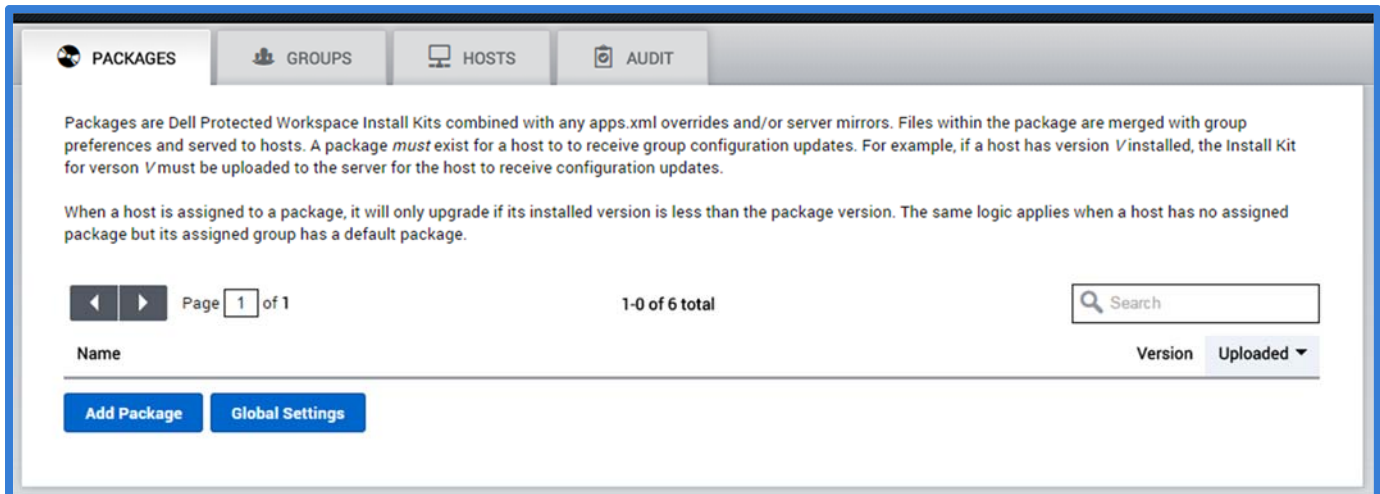


Configuration Module Interface

Packages Tab

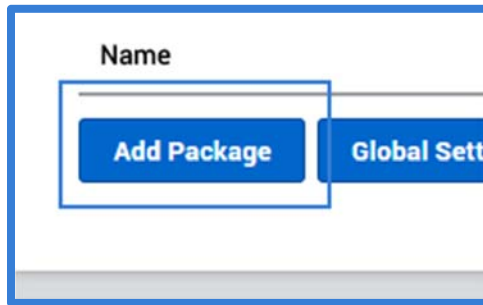
Packages are Dell Protected Workspace Install Kits combined with apps.xml overrides and/or server mirrors for the product installer files. The files that are within the package are merged with settings defined on the group level (as an overlay of the default settings) and served to hosts. **A package must exist on the DPWMS for a host to receive group configuration updates.** For example, if a host has version X installed, the Install Kit for version X must be uploaded to the server for the host to receive configuration updates. Hosts that are running client version software that is not uploaded to the DPWMS will still display the correct group and revision number in the About window, however the configuration files will not be sent to the client. Software version updates will be applied if they are greater than the installed client version.

The package tab provides a list of all currently uploaded packages, plus the ability to add additional packages and modify global settings.

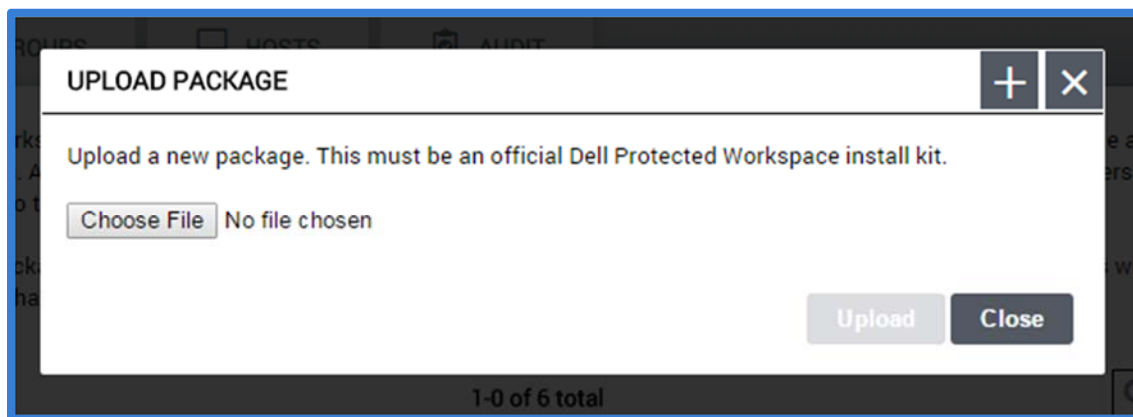


Adding a Package to the DPWMS

To add a new package to the DPWMS, press the “Add Package” button.



When the Upload Package dialog box is displayed, press the “Choose File” button and select the installation kit to upload.



Once the file has been selected, press the “Upload” button.

The dialog box will display “Uploading...” in the bottom left corner during the upload process, and will close when the process is complete. The uploaded installation kit will now be listed in the Packages list.

Name	Version	Uploaded
dellsetup_kit_4.5.0-19621.exe	4.5.0-19621	2015 Jan 24 12:44:25 PM

Page 1 of 1 1-7 of 7 total Search

Viewing package details

To view the details of a package, click on the package name in the packages list.





The screenshot shows the details for the package **dellsetup_kit_4.5.0-19621.exe**. It includes the following information:

- Version:** 4.5.0-19621
- Uploaded:** 2015 Jan 24 12:44:25 PM
- Modified:** Never

Two buttons are visible: **Download the original kit** and **Delete this package...**

FILES

These are the original install kit files and do not contain global setting overrides. These are for reference and typically do not need to be used for anything, except for the installer which you may want to host on a mirror.

File Name	Size	Description
 custom_apps.xml	10 KB	Extends apps.xml with custom isolation rules.
 preferences.xml	4 KB	Defines various configurable values.
 trustedsites.txt	4 KB	Defines host/guest redirection behavior.
 DellSetup_4.5.0-19621.exe	59 MB	The installer file, used to install or upgrade the client.

OVERWRITE APPS.XML

If Dell has updated the apps.xml for a previously released version, this is where to upload it.

None set

INSTALLER MIRROR

You may want to mirror the installer file over another network in order to speed up delivery. If you have done so, please specify the URL here so that it can be distributed for software updates.

No mirror (use [this server](#))

The package details view provides several different options. Below the display name, the product version, date of upload and the last modified date are displayed.

dellsetup_kit_4.5.0-19621.exe

Version: 4.5.0-19621

Uploaded: 2015 Jan 24 12:44:25 PM

Modified: Never





To the right of this information are two buttons. The “Download the original kit” button allows the user to download a copy of the kit that was uploaded, in its original form. The “Delete this package...” button removes a package from the system.

The files section contains the original configuration files for the installation kit, along with the product installer. Each of the icons can be clicked on to download a copy of the original file included with the installation kit.

Clicking on the client installer icon is a recommended way to verify that an upload was completely successful, as the provided link is the one the client software will use to download the software from the DPWMS. If, after clicking on the installer icon, an error is displayed, rather than beginning a download of the installer, delete the package and attempt to upload it again.

FILES

These are the original install kit files and do not contain global setting overrides. These are for reference and typically do not need to be used for anything, except for the installer which you may want to host on a mirror.

 custom_apps.xml (10 KB) Extends apps.xml with custom isolation rules.	 preferences.xml (4 KB) Defines various configurable values.	 trustedsites.txt (4 KB) Defines host/guest redirection behavior.	 DellSetup_4.5.0-19621.exe (59 MB) The installer file, used to install or upgrade the client.
--	--	---	---

The Override Apps.xml section is used to upload (or replace) a new apps.xml configuration file to extend or modify the default configuration file included with this version of the product being viewed. This is often used to add support for new browser versions that are not supported in the default configuration. Apps.xml override files are available on the DPW Support landing page (<http://www.dellprotectedworkspace.com/support>), when needed.

If no override exists for the selected package, press the “Upload” button to select a new override file. If a previous override is in place, press the “Replace” button to upload a new version or the “Delete” button to remove the override.

VERRIDE APPS.XML

If Dell has updated the apps.xml for a previously released version, this is where to upload it.

None set

VERRIDE APPS.XML

If Dell has updated the apps.xml for a previously released version, this is where to upload it.

apps.xml (148 KB)

The last section is the Installer Mirror section. This section allows for the product installer to be downloaded by the clients from an alternate location, such as an internal NAS or public CDN. The address provided must be a HTTP or HTTPS address, and must include the full path to the installer, not the full installation kit. The installer can be downloaded from the installer icon on this page, and uploaded to an external source.

NOTE: It is HIGHLY recommended that an Installer Mirror be used for any deployment over 500 clients.

INSTALLER MIRROR

You may want to mirror the installer file over another network in order to speed up delivery. If you have done so, please specify the URL here so that it can be distributed for software updates.

No mirror (use [this server](#))

[Set mirror...](#)

To add a mirror link, press the “Set mirror...” button and paste the URL to the alternate source. Once set, the URL will display on the page. The URL can be modified by pressing the “Change...” button or removed by pressing the “Delete...” button.

INSTALLER MIRROR

You may want to mirror the installer file over another network in order to speed up delivery. If you have done so, please specify the URL here so that it can be distributed for software updates.

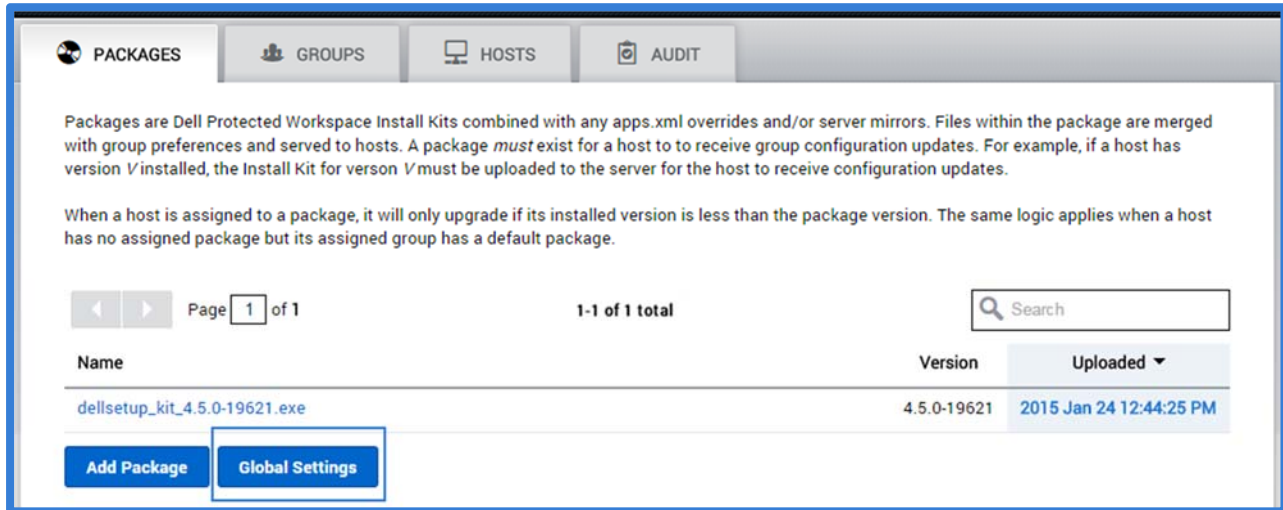
https://internal-nas.dpw.local/enterprise/DellSetup_4.5.0-19621.exe

[Change...](#)

[Delete...](#)

Entering the Client Software Activation Key

The DPWMS is now able to provide a global activation key that will be used for all clients that connect to the DPWMS system. In order to enable this feature, the client activation key needs to be entered into the Global Settings. To access the Global Settings, click the Global Settings button at the bottom of the Packages tab.



The screenshot shows the 'PACKAGES' tab in the DPWMS interface. The top navigation bar includes 'PACKAGES', 'GROUPS', 'HOSTS', and 'AUDIT'. Below the navigation bar, there is a descriptive text about packages and their installation logic. A table lists the installed packages, and a 'Global Settings' button is highlighted.

Packages are Dell Protected Workspace Install Kits combined with any apps.xml overrides and/or server mirrors. Files within the package are merged with group preferences and served to hosts. A package *must* exist for a host to receive group configuration updates. For example, if a host has version *V* installed, the Install Kit for version *V* must be uploaded to the server for the host to receive configuration updates.

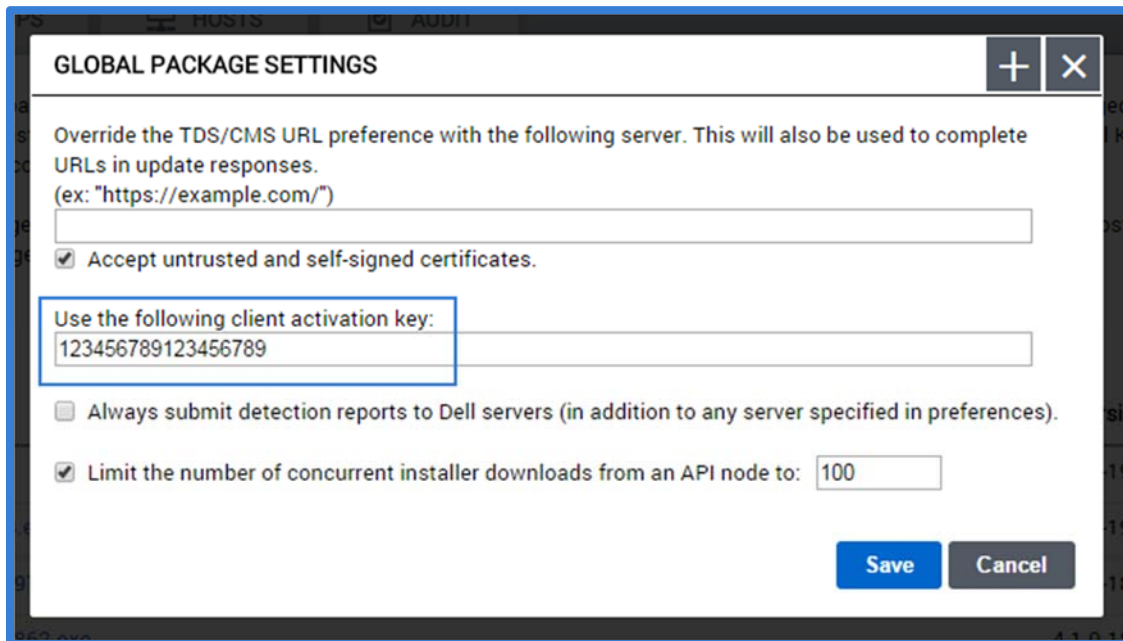
When a host is assigned to a package, it will only upgrade if its installed version is less than the package version. The same logic applies when a host has no assigned package but its assigned group has a default package.

Page 1 of 1 1-1 of 1 total Search

Name	Version	Uploaded
dellsetup_kit_4.5.0-19621.exe	4.5.0-19621	2015 Jan 24 12:44:25 PM

Add Package **Global Settings**

To apply the client activation key, enter it into the “Use the following client activation key” text box on the Global Package Settings dialog. Press the “Save” button to save the setting.



The screenshot shows the 'GLOBAL PACKAGE SETTINGS' dialog box. It contains several configuration options, including a text box for the client activation key, which is highlighted with a blue box.

GLOBAL PACKAGE SETTINGS + X

Override the TDS/CMS URL preference with the following server. This will also be used to complete URLs in update responses.
(ex: "https://example.com/")

Accept untrusted and self-signed certificates.

Use the following client activation key:

Always submit detection reports to Dell servers (in addition to any server specified in preferences).

Limit the number of concurrent installer downloads from an API node to:

Save **Cancel**

Additional Global Package Settings

The Global Package Settings dialog box provides three other global setting options, which affect the entire DPWMS. The first option is used to override the config_server and report preference URLs for all groups. By default, any new group will be automatically populated with the FQDN of the DPWMS system. However, this may not be the desired address for clients to use. By overriding the default setting here, the provided URL will be used instead of the FQDN of the DPWMS. This may be useful if using a “vanity” URL for client connections, such as <https://dpw.mycompany.local>, rather than the FQDN of the system or if a load balancer is being used in front of the DPWMS API servers. It is also important to check the “Accept untrusted and self-signed certificates” check box if using an SSL cert that is not publically signed (by a public CA).



GLOBAL PACKAGE SETTINGS + X

Override the TDS/CMS URL preference with the following server. This will also be used to complete URLs in update responses.
(ex: "https://example.com/")

Accept untrusted and self-signed certificates.

Note: The config_server and report lines can still be modified for an individual group. This setting only modifies the default value that will be provided for new groups.

The next option on the Global Packages Setting dialog is a check box to enable sending threat reports to the Invincea public servers, as well as the specified local server. Some customers are required to have this option enabled per their license agreements.

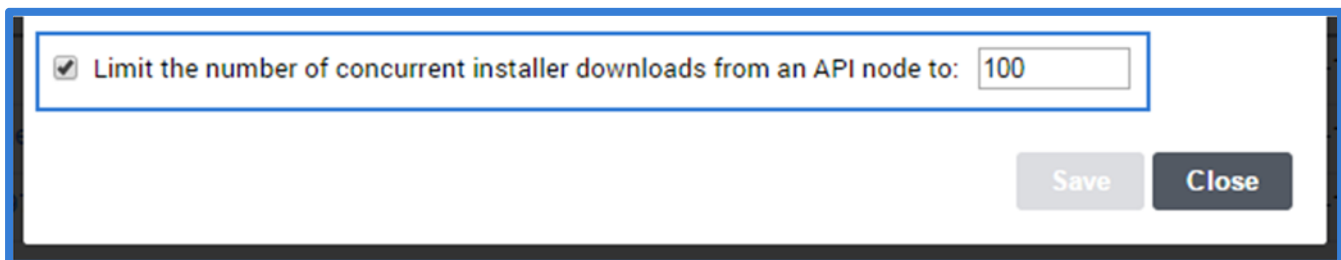


123456789123456789

Always submit detection reports to Dell servers (in addition to any server specified in preferences).

Limit the number of concurrent installer downloads from an API node to: 100

The final option in the Global Settings dialog is the “Limit number of concurrent downloads” option. This option is used to control the number of client machines that will be able to download a new update package from the DPWMS at one time. This option can be modified based on the load placed on the server for a specific environment. It is recommended that this option be left enabled for most deployments.

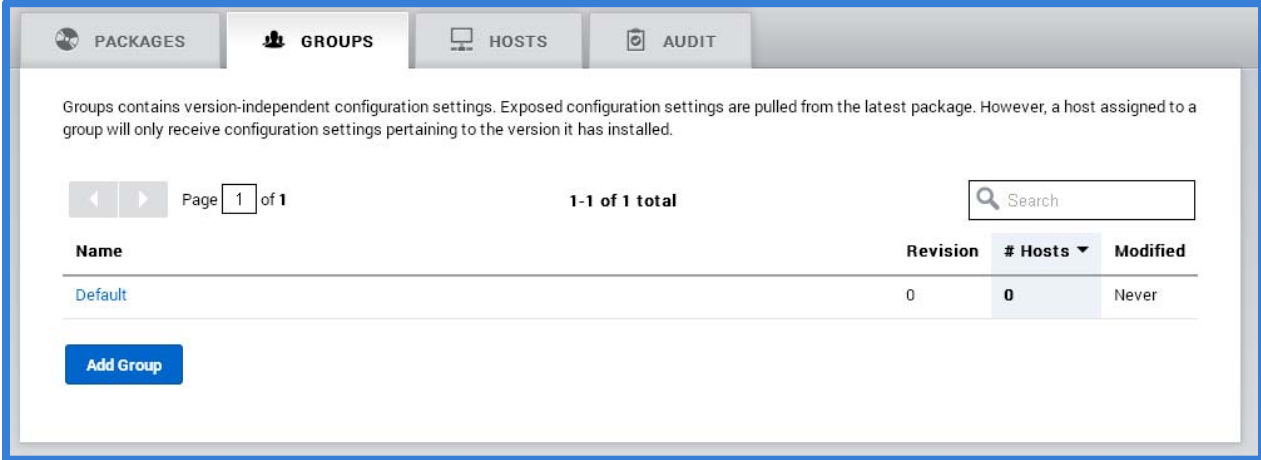


Limit the number of concurrent installer downloads from an API node to: 100

Save Close

Groups Tab

The Groups Tab displays a list of all available groups on the system. By default, the display lists the group with the largest number of hosts first. Along with the group name, the current revision number for that group is displayed, along with the total number of hosts assigned to the group, and the date of the last modification of that group.



The screenshot shows the 'GROUPS' tab selected in a navigation menu. Below the menu is a text block explaining that groups contain version-independent configuration settings. Below this is a navigation area with left and right arrow buttons, a 'Page 1 of 1' indicator, and a '1-1 of 1 total' count. To the right is a search box labeled 'Search'. Below the navigation is a table with the following data:

Name	Revision	# Hosts	Modified
Default	0	0	Never

At the bottom left of the main content area is a blue 'Add Group' button.

The column headers can be clicked on to sort the list by any of the selected headers. The search box can also be used to search for a specific group.

When more than 10 groups are present, the groups will span multiple pages. The arrow buttons can be used to advance to the next or return to the previous page of Groups. Additionally, the Page number can be entered into the Page Number box to jump to a specific page. The total number of groups is listed in the center of the navigation tools.

Creating a New Group

To add a new group to the DPWMS, press the “Add Group” button. In the Add Group dialog, enter a name for the new group, and select an existing group to copy the configuration from. It is recommended that an existing group always be used as a template for any new group. If the None option is selected, the group will contain only the default settings.

Press the “Create” button to finish the process. The dialog box will close and return to the Groups tab.

Name	Revision	# Hosts ▾	Modified
Default	0	0	Never
Production	0	0	Never

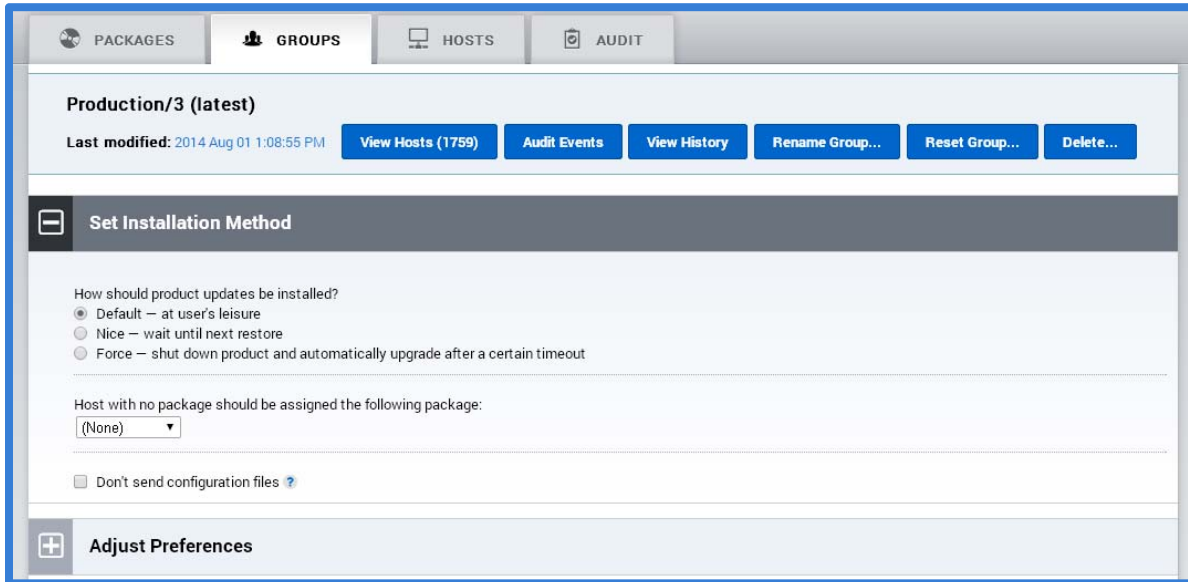
Renaming a Group

Added with the release of DPWMS 2.2 is the ability for the name of a group to be modified after it has been created. In order to rename a group (with the exception of the “Default” group), click on the group name in the Groups table. From the Group details screen, press the “Rename Group...” button.

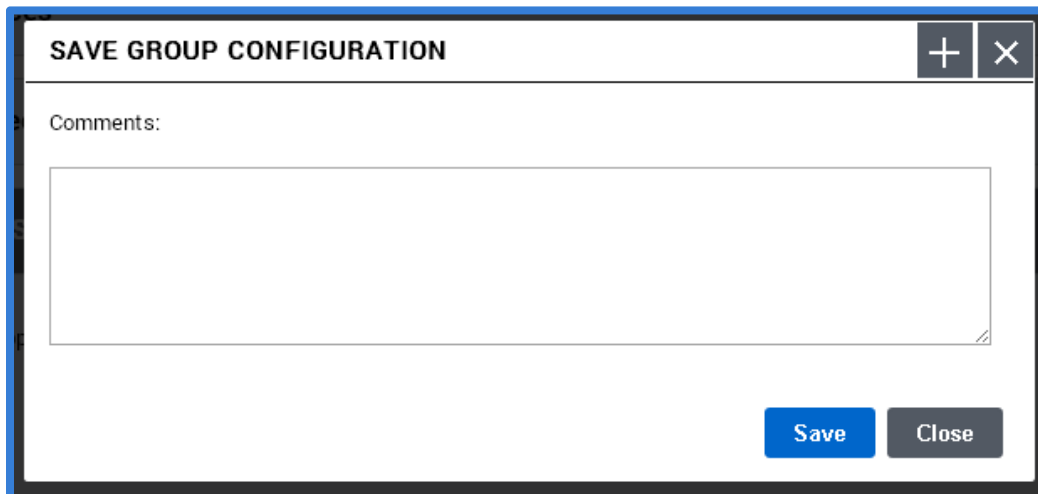
When the “Rename Group” dialog box is displayed, enter the new name for the group, then press the Rename button.

Group Details View

The Group Details View provides a view of the currently selected group that shows the current configuration options, current software deployment options, plus history information and a link to the list of hosts that are currently assigned to the group.



Once customizations have been made to any section of the Group Detail View (Install Method, Preferences, Trusted Sites or Custom Apps), they need to be saved before they will be sent to the clients. Pressing the “Save” button at the bottom of the view will display a confirmation dialog.



An optional comment can be saved to indicate what changes were made during this revision. Pressing the “Save” button on the dialog will commit the changes and publish them to the clients. Any comments can be reviewed on the “View History” tab for the group. Pressing the “Close” button on this dialog will cancel the save action.

The “Clear” button at the bottom of the view can also be used to remove any pending changes and revert back to the last saved state.

The Group navigation bar provides information about the Group, including the name of the currently selected group, and the date and time of the last revision.

Production/0 (latest)**Last modified:** Never

There are also six buttons available in the navigation bar that allow the current hosts assigned to the group to be listed, the audit events log for the current group to be displayed, the revision history of the group to be reviewed, provide the ability to reset a group to its default configuration, rename a group and finally allow a group to be deleted from the system.

View Hosts (1759)**Audit Events****View History****Rename Group...****Reset Group...****Delete...**

Pressing the “View Hosts” button will switch the display to the Hosts tab, with the correct filter applied (in the image below the “Production” group filter is applied) for the group that is currently selected. To return to the group, go back to the Groups tab and select the group from the list.

Pressing the “Audit Events” button will switch the display to the Audit tab, with the correct filter applied (in the image below the “Production” group filter is applied) for the group that is currently selected. To return to the group, go back to the Groups tab and select the group from the list.

Pressing the “View History” button will switch the display to view the revision History for the currently selected group.

History of **Production**

Page 1 of 1 1-2 of 2 total

Revision	Date	Comment	Author	Actions
1	2014 Apr 10 5:42:23 PM	Updated server URLs	admin	View Changes / Revert...
0	2014 Apr 10 5:27:19 PM	Group created.	admin	View Changes / Revert...

Any comments that were noted while saving a revision will be displayed on the Comment section of that revision.

Date	Comment
Apr 10 5:42:23 PM	Updated server URLs
Apr 10 5:27:19 PM	Group created.

Clicking the “View Changes” link on a revision will provide a detail of whatever changes were made during the selected revision.

Author	Actions
admin	View Changes / Revert...
admin	View Changes / Revert...

Changes from **Default/1**

View history

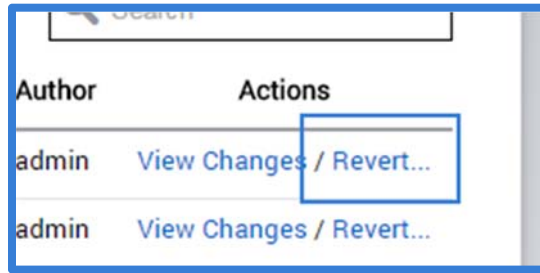
On 2014 Aug 26 2:39:22 PM admin wrote:

```

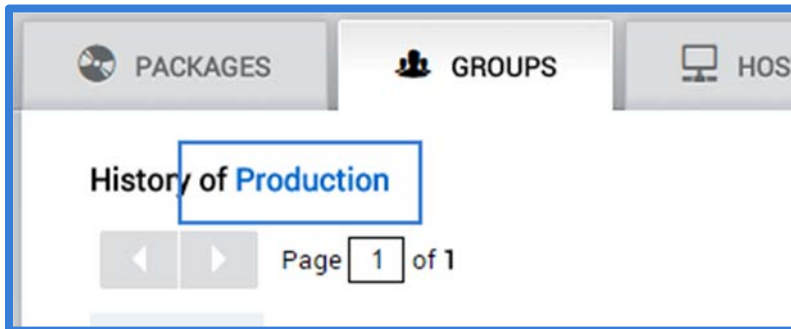
--- Default/0
+++ Default/1
@@ -1,5 @@
- {}
+ {
+   "default_package": "4.0.0-18075",
+   "install_type": "default",
+   "no_config": false
+ }

```

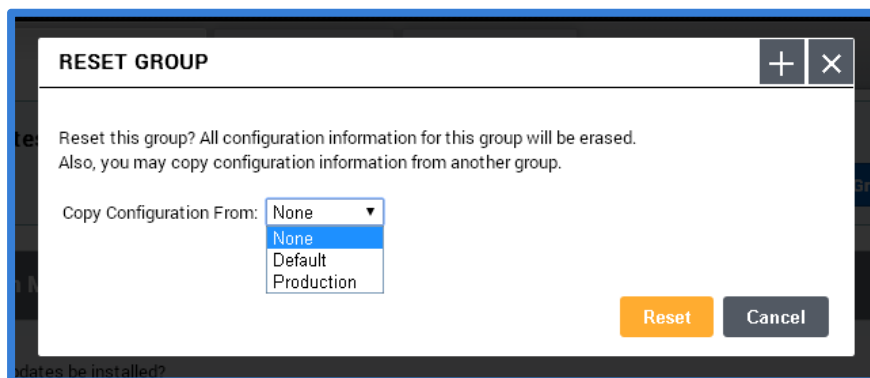
Clicking on the “Revert” link on a revision with reset the group settings back to what was published in this revision.



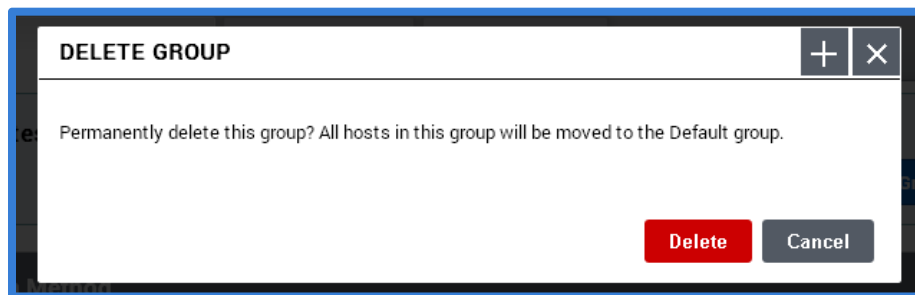
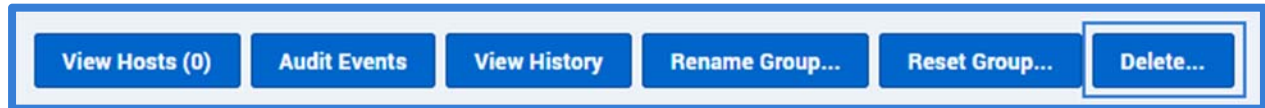
To return to the Group, click on the Group Name link in the title.



Pressing the “Reset Group...” button on the group details page will prompt the user to select where the group should be reset. The user can select the current configuration of another group, or can go back to all default settings by selecting “None”.



Finally, pressing the “Delete...” button will prompt the user to confirm deletion of the selected group.



Set Installation Method

The next section of the Group Details View is the “Set Installation Method” section.

While the DPWMS is not able to do initial installations of client software, it can provide software updates once the clients are managed. The “Set Installation Method” provides options for how client updates should be applied.

When a DPWMS group is assigned with a specific software version, it is then able to ensure that all clients that are assigned to the group are running this specific version, or greater, of the client software. For example, if the Group is assigned v3.3.4 and a client is running v3.3.0, the client will be upgraded. However, if the client is running v3.3.5, it will not be downgraded.

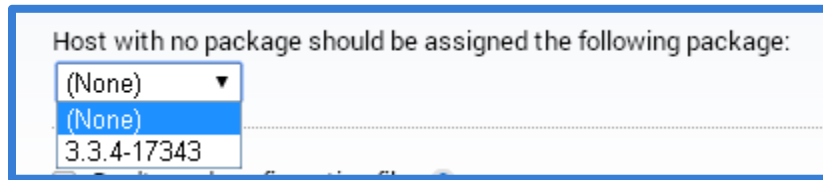
The first section deals with the user experience during the software upgrade process. One of three options needs to be selected when a software version is specified.

The “Default” method will provide the user with a Dell Protected Workspace Alert over the system tray, after the upgrade file has finished downloading to the staging area on the client machine, with the option to either “Install Now” or “Install Later”. By choosing Now, the user will immediately be exited out of all protected applications and the upgrade process will take place immediately. The Later option will put the upgrade into a pending state and it will automatically apply the next time the client software is restored or restarted.

The “Nice” method does not alert the user at all, but after the upgrade file has finished downloading to the staging area on the client machine, the upgrade will be in a pending state, and it will automatically apply the next time the client software is restored or restarted.

Finally, the “Force” method will provide the user with a Dell Protected Workspace Alert over the system tray, after the upgrade file has finished downloading to the staging area on the client machine that indicates a five (5) minute countdown until the software is forcibly upgraded. Once the timer has expired, all protected applications will close and the upgrade will be processed.

The next section provides a drop-down that allows for the selection of the software version to be used for the client upgrades.



A screenshot of a software management interface. At the top, the text reads "Host with no package should be assigned the following package:". Below this text is a dropdown menu. The dropdown menu is currently open, showing three options: "(None)" at the top, "(None)" in the middle (highlighted with a blue background), and "3.3.4-17343" at the bottom.

New to DPWMS 2.0 is the ability to directly assign a package upgrade to an individual host. If a package has been assigned directly to a host, that host will not receive a package upgrade assignment from the Group it is part of until the package assignment has been removed. The text above the package assignment for the group specifies "Host with no package" as a reminder. You can tell if a host has had a package assigned by searching for the host in the Hosts table and seeing what value is in the "Package" column. This column needs to display (None) for the host to receive software upgrades from the group level settings.

Adjust Preferences

The Adjust Preferences section is used to set the client software preferences. This UI is automatically created based on the latest version of the client software loaded into the system.

The screenshot shows the 'Adjust Preferences' window with a sidebar on the left containing tabs: GENERAL, SECURITY, PRIVACY, DIALOGS, NETWORK, and OTHER. The 'GENERAL' tab is selected. The main content area is titled 'Autorestore ?' and contains the following settings:

- enabled: true false
- user_modifiable: true false
- allow_cancel: true false
- day_of_week:
- grace_period_seconds:
- hours:
- minutes:
- randomize_minutes:
- type:

Below these settings is a section for 'Default Browser ?' with an 'enabled' radio button set to 'true'.

The preferences are broken into several sections to help group together the different preferences by functionality. By clicking on the tabs along the left hand side, the different sections are displayed.

There are two different types of preference selection: radio button and text box. Preferences attributes that have a predefined true or false option will display as a radio button. All other preferences display as a text box where a specific value needs to be entered, based on the preference being set. Please reference the client software documentation for descriptions of each preference and allowed values for the text box fields.

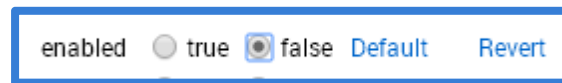
Additionally, the “?” next to the name of each preference may provide some additional information about the preference, if it is available. This information may contain valid entries for text box fields, however the comprehensive information can be found in the client software documentation.

This screenshot shows the same 'Adjust Preferences' window as above, but with a tooltip box overlaid on the 'Autorestore ?' heading. The tooltip contains the following text:

- Controls the settings for the auto-restore feature.
- Valid values for **type**: "daily", "weekly", "elapsed".
- Valid values for **day_of_week**: "*" (when not using type weekly), spelled out day of week (i.e. "Monday", "Tuesday"...).

The background settings are partially visible, showing the 'enabled' radio button set to 'true' and 'user_modifiable' set to 'false'.

Preferences all start with the default values that are set in the client software installation kit. When a value has been changed from the default option, an additional option will now be present on the same line.

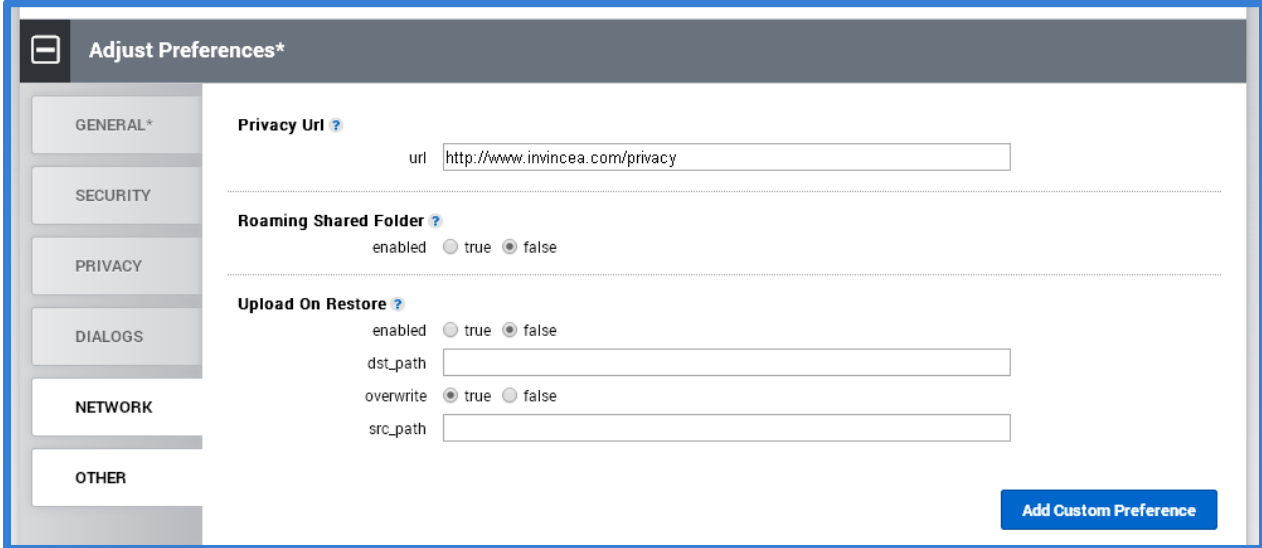


The word “Default” being displayed next to a preference attribute indicates that the preference is no longer set to the default value in the client installation kit. If the Default option is clicked, the value will be reset back to what it was in the client installation kit.

Additionally, the word “Revert” is displayed. Clicking this link will revert the value back to what it was the last time the group was saved. This can be used if a value was changed by accident and the previous setting is not known.

Adding Custom Preferences / Attributes

In some cases, a custom preference may need to be added to enable a new preference, or to add additional attributes to a default preference. To add a new preference or attributes, switch to the “other” tab of the Adjust Preferences menu and press the “Add Custom Preference” button.

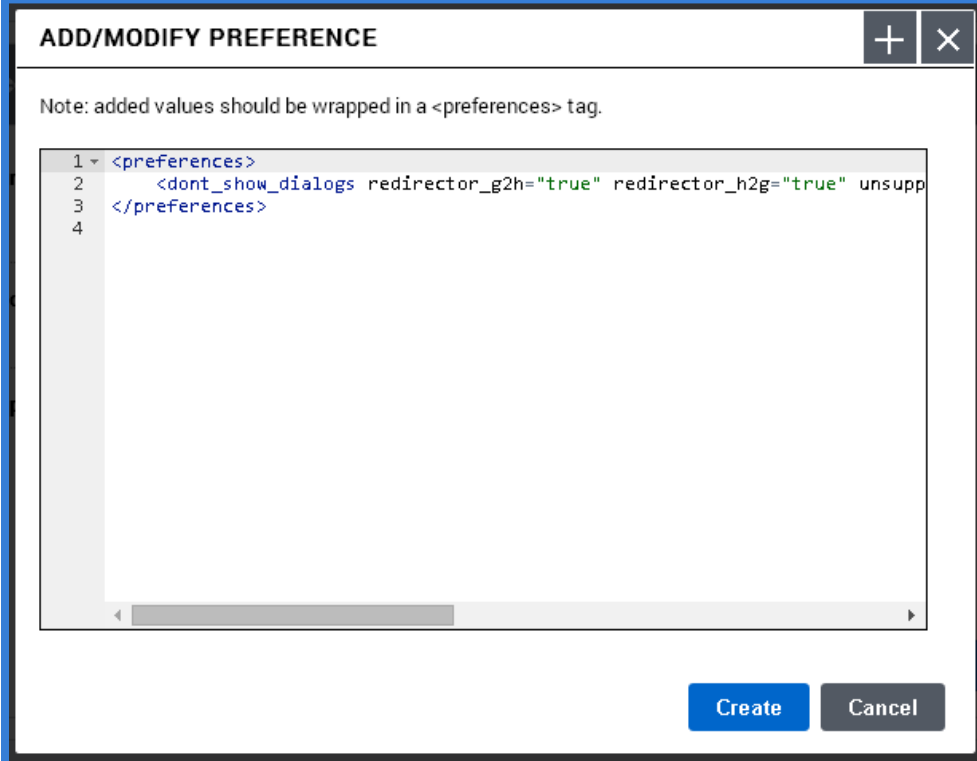


The screenshot shows the 'Adjust Preferences*' dialog box with the 'OTHER' tab selected. The dialog has a sidebar with categories: GENERAL*, SECURITY, PRIVACY, DIALOGS, NETWORK, and OTHER. The main content area is divided into sections:

- Privacy Url ?**: A text input field with the value 'http://www.invincea.com/privacy'.
- Roaming Shared Folder ?**: A section with 'enabled' and two radio buttons: 'true' and 'false' (selected).
- Upload On Restore ?**: A section with 'enabled' and two radio buttons: 'true' and 'false' (selected). Below this are three text input fields: 'dst_path', 'overwrite' (with 'true' selected), and 'src_path'.

An 'Add Custom Preference' button is located at the bottom right of the dialog.

When the Add/Modify Preference dialog is displayed, copy the new preference or updated preference XML snippet into the dialog box. Be sure to include the <preferences> tag before the snippet and the </preferences> tag after the snippet. Press the “Create” button to confirm the change.

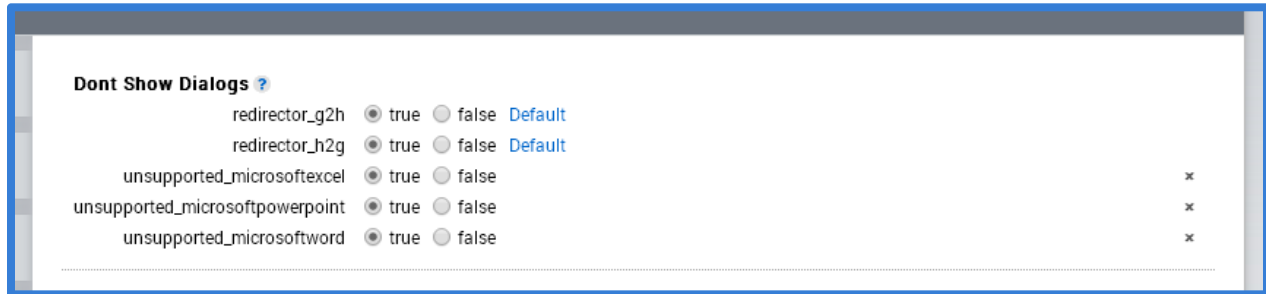


The screenshot shows the 'ADD/MODIFY PREFERENCE' dialog box. It has a title bar with a plus sign and a close button. Below the title bar is a note: "Note: added values should be wrapped in a <preferences> tag." Below the note is a text area containing the following XML snippet:

```
1 <preferences>
2   <dont_show_dialogs redirector_g2h="true" redirector_h2g="true" unsupp
3 </preferences>
4
```

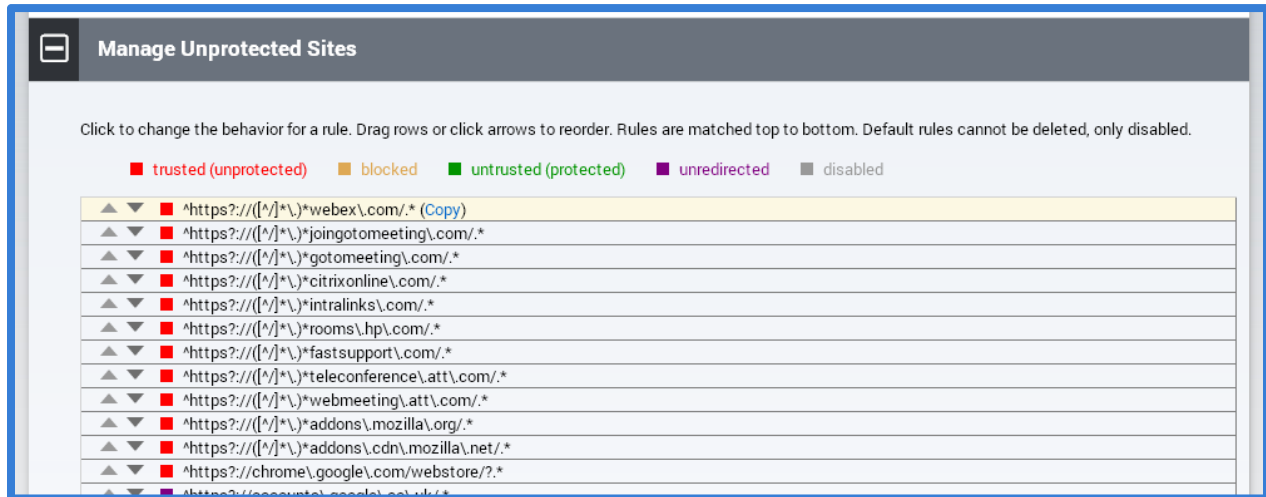
At the bottom of the dialog are two buttons: 'Create' and 'Cancel'.

Locate the new or modified preference to ensure it has been added or modified. Modifications that are not part of the default configuration file will contain an “x” at the end of the line to allow for removal of the modification, and to act as an indicator that it is a custom entry. For modified preferences, this only applies to attributes that are not part of the default configuration file. Once added to the UI, these new preferences can be modified the same as any other preference.



Manage Unprotected Sites

The next section on the Group Detail View is the Manage Unprotected Sites section. This section is used to enter regex values for URLs that should be added to the trusted sites list for the client software.



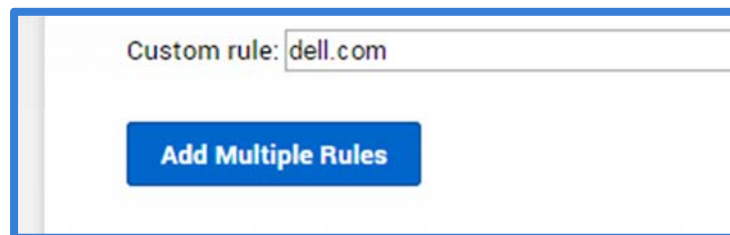
When a new group is created, this section is populated with the default entries included in the installation kit. These entries cannot be removed from the list, however they can be disabled as described below. Custom entries can be added to the list using the “Add Custom Rule” entry box at the bottom of the list. Enter the desired regex entry into this box, then press the “Add Rule” button to add it to the list.



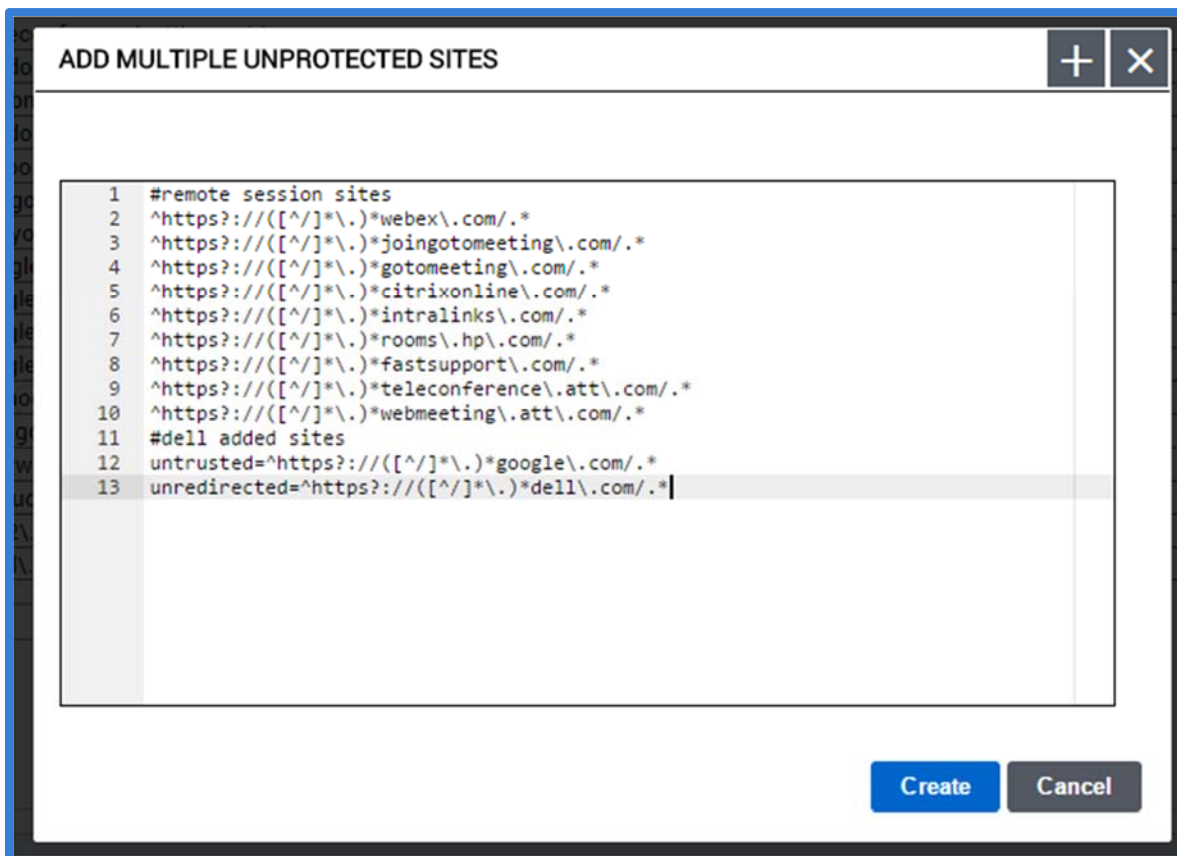
The “Quick Add Domain” feature can be used to add a standard regex for a simple domain, such as example.com. By entering the domain into the rule text box, and pressing the “Quick Add Domain” button, a regex will be auto-created and added.



The “Add Multiple Rules” button, located below the Custom Rule section, allows for a multi-rule regex file to be pasted into the provided dialog to allow for a bulk upload of regex entries.



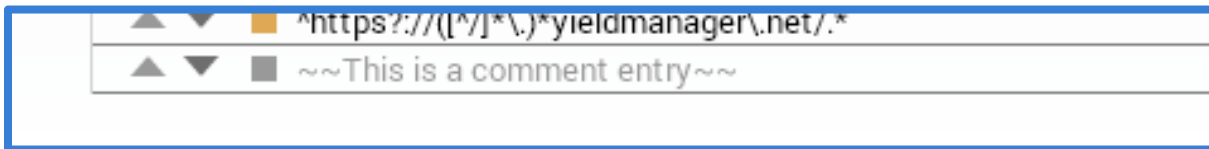
Within the “Add Multiple Unprotected Sites” dialog box, paste a list of regex entries, one per line, then press the “Create” button to add them. Comments can also be added within the bulk upload by adding a hashtag “#” at the beginning of the line.



Each entry in the list must be classified with one of five different classifications. By default, all new entries are classified as “trusted (unprotected).”

- Red - trusted (unprotected) – indicates that any matching URL will open in an unprotected browser, outside of the secure container.
- Gold - blocked – indicates that any matching URL will not be allowed to open in an unprotected browser; however, if the URL is entered into the unprotected browser it will not be redirected. The only method for accessing a blocked URL is to access it via a protected browser directly. This is mostly used to block third-party embedded ad URLs that are on trusted sites, to prevent the ad URLs from opening in a protected browser. This feature is no longer valid after the release of Dell Protected Workspace 4.0.
- Green - untrusted (protected) – indicates that any matching URL will open in the protected browser. This feature is used when certain subdomains (such as a publically facing website) should be forced to open in the protected browser, while the rest of the domain is allowed to open in an unprotected browser. It is important that untrusted entries be listed above any associated trusted entries, as the trusted sites list is evaluated from top down.
- Purple – unredirected – indicates that any matching URL will be allowed to stay in whatever browser (protected or unprotected) it is accessed from. This is important for sites like Google account sites, to allow users to be able to log into both the protected and unprotected Chrome browsers.

- Grey – disabled – indicates that the entry is not active and will be skipped. The disabled option can also be used to place comments within the trusted sites list to indicate what a certain section of regex values may relate to. If a comment is entered, it is extremely important to make sure it is disabled.



To change the classification of an entry, click on the colored square at the beginning of the line until it displays the desired color of the classification needed. Entries can also be reordered by using the up and down arrows at the beginning of each line, or by clicking and dragging the entry to the desired location (not supported with all browsers). A custom entry can also be removed completely by clicking on the “x” at the end of its line.

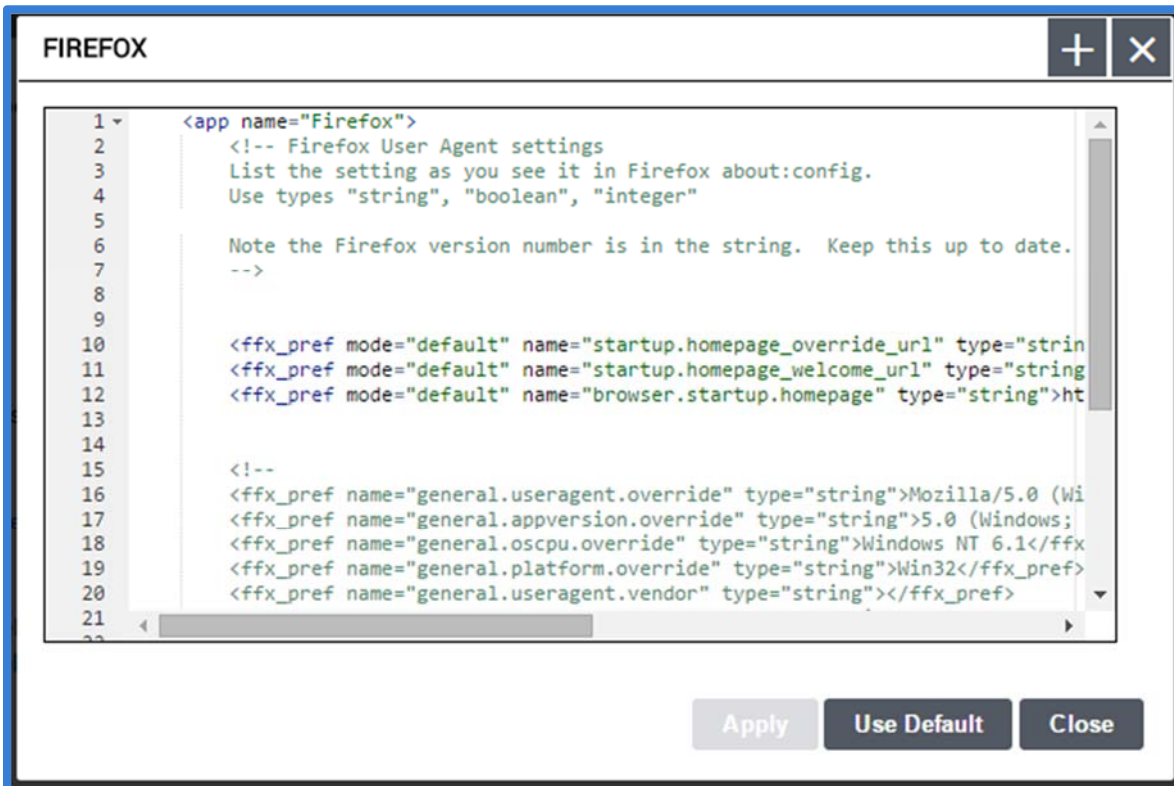
Customize App Settings

The Customize App Settings section of the Group Details View allows the default custom_apps.xml that is included with the installation kit to be displayed as individual apps so that those individual apps can be enabled or disabled and/or modified from their default values. Additionally, it also allows for additional custom apps snippets to be added.



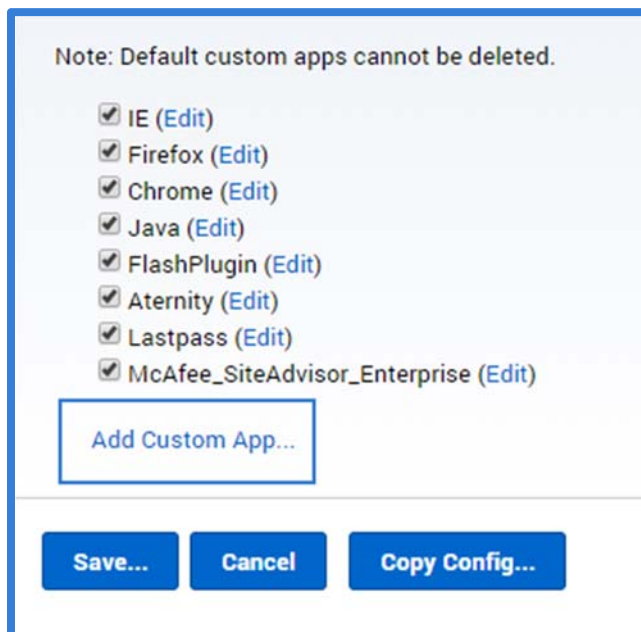
Each custom app is listed based on the name supplied within the <app> tag of the snippet. From this list, an app can be enabled or disabled by checking or unchecking the checkbox next to the app name. The default custom_apps cannot be deleted.

To view or modify one of the default custom_apps, click on the “edit” link to display the XML snippet.



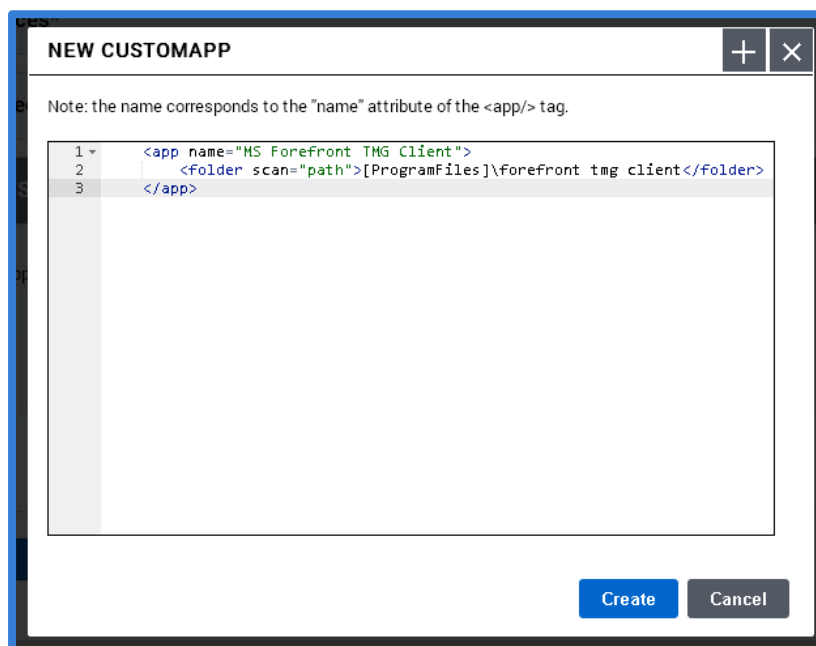
The XML editor allows for the XML snippet to be modified as necessary. Once finished, press the “Apply” button. For custom_apps included with the installation kit, press the “Use Default” button to return the snippet to its default setting. This should also be used when a new version of the client software is added to the system, to ensure the latest version of the snippet is being used. Once the “Use Default” button has been pressed and the new version is displayed, any customizations can be re-entered.

To add a custom_app to click on the “Add Custom App” link below the list of custom_apps.

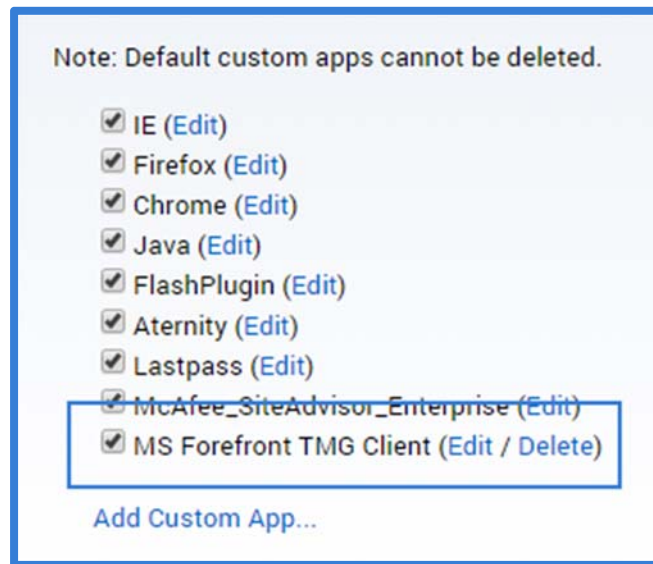


When the New Custom App dialog is displayed, paste the XML snippet into the dialog box, making sure to include the <app> tag at the beginning and the </app> tag at the end. Press the “Create” button to finish adding the snippet.

Additionally, multiple custom app snippets can be added at one time by copying them all into the New Customapp dialog box. Individual app snippet will be created after the “Create” button is pressed.

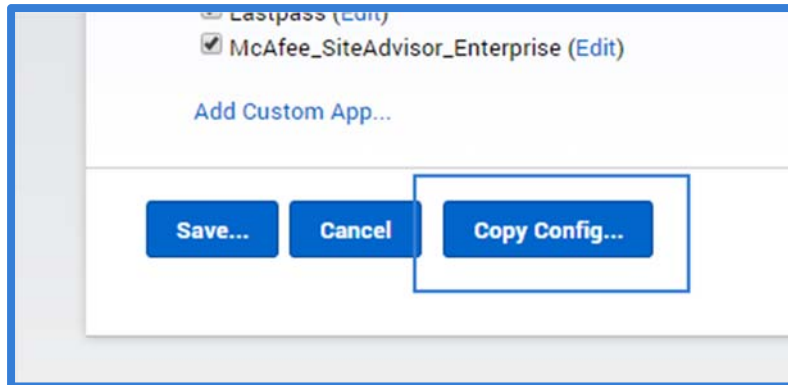


Once the new snippet has been added, it will display in the list of available apps. From the list, it can also be enabled or disabled and edited, same as the default apps. Additionally, custom snippets can be deleted from the system.



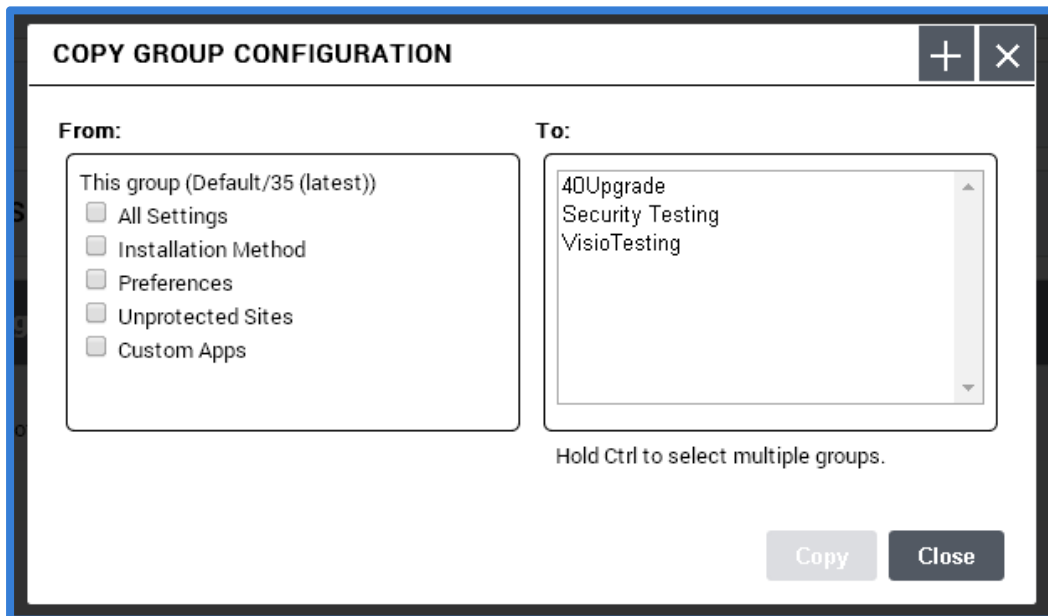
Copy Configuration File(s)

The final option on the Group Details page is the “Copy Config...” button. This button is used to copy a set of configuration files between groups.



To copy one or more configuration files to one or more groups, start by browsing to the source group to be copied from, and press the “Copy Config...” button.

The “Copy Group Configuration” dialog allows an admin to select which configuration files/settings to copy, and to select which group(s) to copy to. Once the appropriate selections are made, press the “Copy” button to apply these settings. A confirmation dialog will display, outlining the changes that are about to be made. Press the “Overwrite” button to commit the changes. Once copied, the changes immediately go into effect on the destination groups.



Hosts Tab

The Hosts Tab displays a list of all hosts currently being managed by the Config module. This tab can be used to display all hosts and details. The display can also be filtered on several different criteria to display a subset of the hosts.

Each host corresponds to a machine with the Dell Protected Workspace client installed. Hosts can be assigned to groups to change their configuration settings, and/or assigned to packages to upgrade their client version. Hosts are created when a client first heartbeats in.

Group: Choose... Package: Choose... Host Status: ? Choose... Hosts Per Page: 20

Page 1 of 1 1-3 of 3 total Search

Hostname	User	IP	Install Status	Installed	Package	Group	Revision	Last Beat
...	james.robustson	...	Installed	4.5.0-19664	4.5.0-19664	Default	245	2015 Jan 25 7:10:13 AM
...	admin	...	Uninstalled	4.1.1-18970	(None)	Default	232	2015 Jan 07 10:18:07 PM
...	james.robustson	...	Installed	4.1.0-18862	(None)	Default	145	2014 Oct 14 2:52:32 PM

The table displays the Hostname, IP address, last reported status, product version currently installed, currently assigned package, current group, and the last time a heartbeat was received for each host displayed. Clicking on the column heading for any of these options will sort the table by the selected column. By default, the table displays the first 20 results, sorted by most recent heartbeat. The number of results can be changed by selecting a different host count in the “Hosts Per Page” drop-down.

Hosts Per Page: 20

10
20
50
100

Search

Revision Last Beat

245 2015 Jan 25 7:10:13 AM

The table can also be filtered based on the drop-down menus above the table.

Group: Choose... Package: Choose... Host Status: ? Choose...

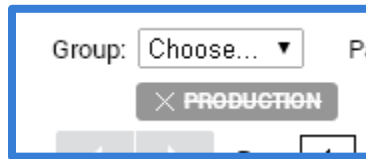
The Group filter is used to display hosts from a specific group. The drop-down will contain a list of all the groups currently on the system. Selecting one of the options from the drop-down selects that filter. Multiple groups can be selected at once.

Group: Choose... P

Default
Production

1

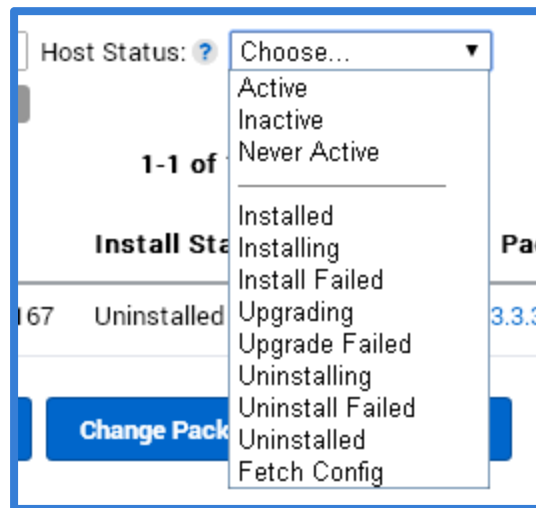
Once a filter has been selected, it will display below the drop-down. To remove a filter, click on the “x” next to the filter name.



The packages drop-down allows the table to be filtered by the assigned package version. The drop-down will include all software versions that have been added to the package tab. When a version is selected, only hosts that are currently assigned to that package version will display. The assigned package is not the currently installed version.

Hostname	User	IP	Install Status	Installed	Package	Group	Revision	Last Beat
			Installed	4.5.0-19664	4.5.0-19664	Default	245	2015 Jan 25 7:10:13 AM

The final filter available is the Host Status filter. This option will display all hosts with the selected filter based on the following options:



Activity Options:


- Active – a host is active when during a heartbeat to the server a protected application was running. A host needs to have reported in an active state within the last 7 days.
- Inactive – a host is inactive when all heartbeats in the last 7 days occurred while no protected application were running.
- Never Active – a host is never active if it has never reported an active state since it first was added to the system as a host.

Install Status Options:

All of the following actions are reported in the heartbeats received from the client:

- Installed – a software install has finished successfully
- Installing – a software install has started, but not yet finished
- Install Failed – a software install finished, but not successfully
- Upgrading – a software upgrade has started, but not yet finished
- Upgrade Failed – a software upgrade finished, but not successfully
- Uninstalling – a software uninstall has started, but not yet finished
- Uninstall Failed – a software uninstall has finished, but not successfully
- Uninstalled – a software uninstall has finished successfully
- Fetch Config – the latest available configuration from the assigned group was requested

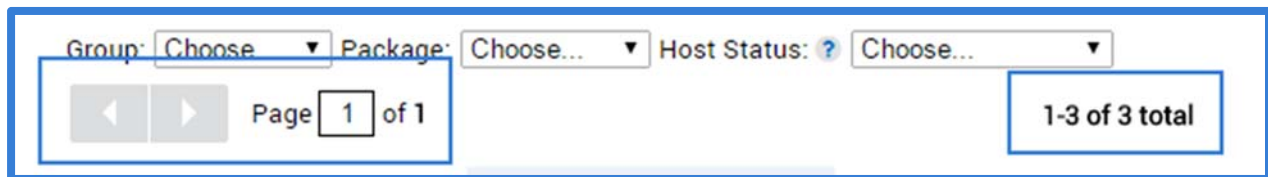
The last filter option is the search box. The search box allows an admin to create a custom filter based on hostname, IP address or user name.



The screenshot shows the Hosts tab interface with the following elements:

- Filters: Group: Choose..., Package: Choose..., Host Status: ? Choose...
- Navigation: Page 1 of 1, 1-1 of 1 total
- Search Box: admin
- Table Headers: Hostname, User, IP, Install Status, Installed, Package, Group, Revision, Last Beat
- Table Row: admin, Uninstalled, 4.1.1-18970, (None), Default, 232, 2015 Jan 07 10:18:07 PM

For all filtered displays, up to ten results are displayed in the table. If more than ten hosts meet the filtered criteria, multiple table pages will be displayed and can be traversed from the navigation bar.



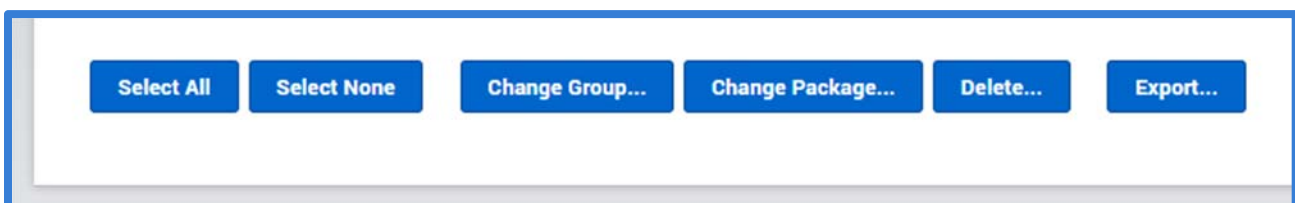
The screenshot shows the Hosts tab interface with the following elements:

- Filters: Group: Choose..., Package: Choose..., Host Status: ? Choose...
- Navigation: Page 1 of 1, 1-3 of 3 total

The left and right navigation buttons can be used to move one page at a time between the different available pages. The “Page X of X” indicates the current page number that is being displayed and the total number of pages that exist for the filter. To jump to a specific page, enter the page number into the Page box and press enter.

The center title of the table will indicate the total number of hosts that meet the current criteria and number of hosts that are currently displayed. For page 1, hosts 1-10 are displayed, for page 2, 11-20, etc.

At the bottom of the Hosts tab are additional actions that can be performed based on the filtered display of hosts in the table.



The screenshot shows the Hosts tab interface with the following action buttons:

- Select All
- Select None
- Change Group...
- Change Package...
- Delete...
- Export...

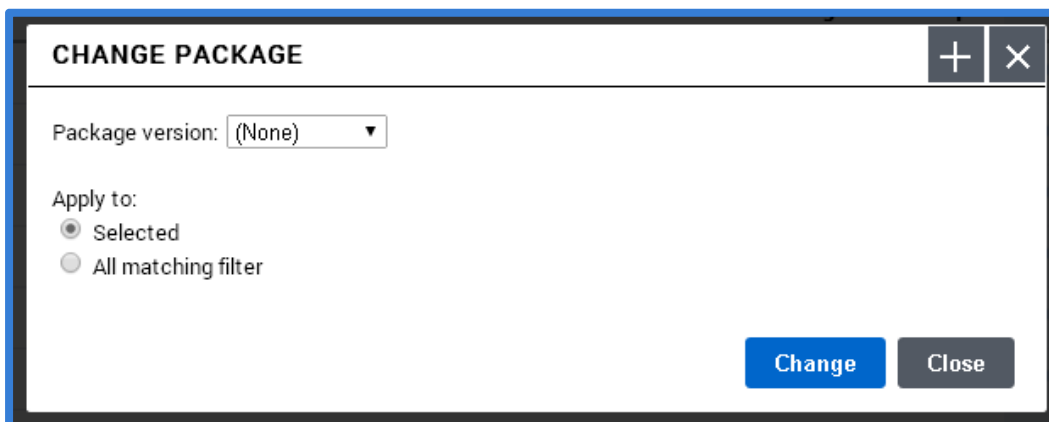
The “Select All” and “Select None” buttons are used to select all of the currently displayed hosts or to clear the currently selected hosts. These buttons only apply to the currently displayed page, and not all hosts within the current filter if there are multiple pages.

The “Change Group...” button is used to reassign selected hosts (or filtered hosts) to a new group. Once the hosts or filter are selected, press the “Change Group...” button to assign a new group.



When the Change Group dialog box is displayed, select the new group that the hosts are to be moved to. Next, select whether the change will apply only to the hosts that are currently selected (up to ten hosts on the current page) or to all hosts that are in the current filter. When finished, press the “Change” button. To cancel the action, press the “Close” button.

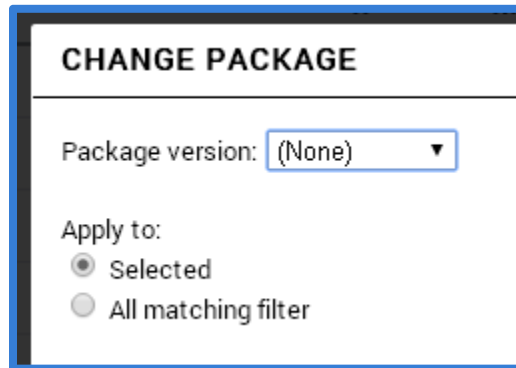
The “Change Package...” button is used to manually assign a new package to a host, rather than letting it receive a new package from the group it is currently assigned to. This is useful when testing a new version of the client software to ensure that it successfully works with all settings in a specified group. Once the hosts or filter are selected, press the “Change Package...” button to assign a new package.



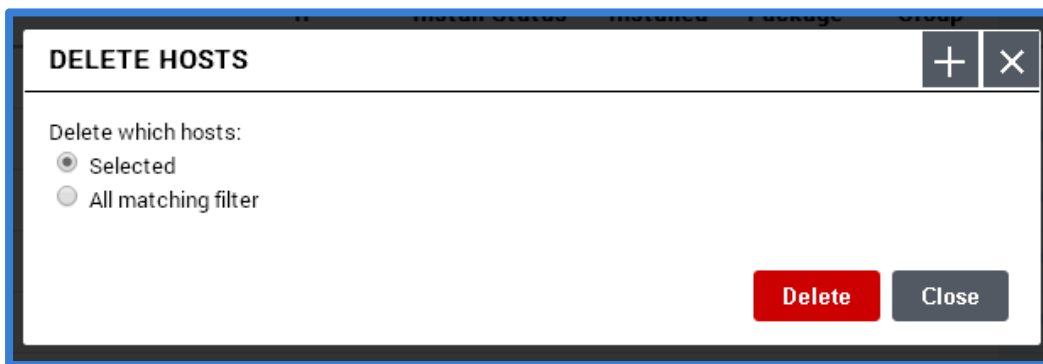
When the Change Package dialog box is displayed, select the new package to assign to the selected hosts. Next select whether the change will apply only to the hosts that are currently selected (up to ten hosts on the current page) or to all hosts that are in the current filter. When finished, press the “Change” button. To cancel the action, press the “Close” button.

Once a package has been assigned to a host, it will no longer receive package updates from the group it is assigned to. It will still receive configuration updates based on the group it is currently assigned to, unless that group is not sending

configuration updates to any clients. To enable a host to receive package updates based on the group level settings, set the host back to the (None) assignment.

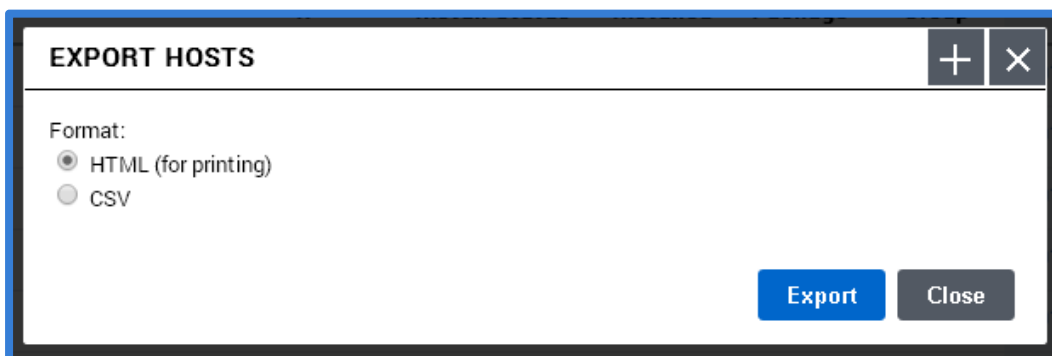


The “Delete...” button is used to remove the currently selected or filtered hosts from the system. This not only removes the host, but all history for the host. However, this does not remove the client software from the host system. If a host is deleted from the DPWMS, but the client software is still running, the host will be recreated within the DPWMS on the next heartbeat that it performs. To delete hosts from the system, select them from the table, or filter the table to display all hosts that should be deleted, then press the “Delete...” button.



When the Delete Hosts dialog box is displayed, select whether the delete action will apply only to the hosts that are currently selected (up to ten hosts on the current page) or to all hosts that are in the current filter. When finished, press the “Delete” button. To cancel the action, press the “Close” button.

The final option available is the “Export...” button. This option is used to export the current filter to a HTML or CSV report.

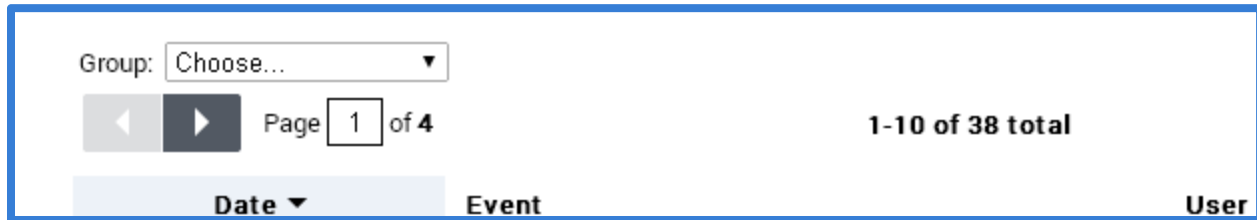


The exported report will include the same information that is displayed in the hosts table based on the currently selected filter.

Audit Tab

The Audit Tab is used to display client audit events (such as using the Unprotect Current Page option) that were sent to the server. The table will show all audit events, with the most recently received displayed at the top by default. In order for the DPWMS to receive audit events, the client software has to be configured to point to this DPWMS.

For the audit events table, up to ten results are displayed on a single page. If more than ten events are in the audit table, multiple table pages will be displayed and can be traversed from the navigation bar.



The left and right navigation buttons can be used to move one page at a time between the different available pages. The “Page X of X” indicates the current page number that is being displayed and the total number of pages that exist for the filter. To jump to a specific page, enter the page number into the Page box and press enter.

The center title of the table will indicate the total number of audit events that meet the current criteria and which audit events are currently displayed. For page 1, events 1-10 are displayed, for page 2, 11-20, etc.

Similar to the Hosts table, the Audits table can also be filtered and searched. The Group drop-down allows the events to be filtered to display only the audit events for a specific group. The group information for a reported event is based on of the host that submitted the event. The group will be the group that host was assigned to at the time of the event, not necessarily its current group. Multiple groups can be displayed at the same time when selected from the drop-down. To remove a group from the filter, press the “x” next to the group name.

The screenshot shows the full Audit Tab interface. It includes a search bar on the right, a navigation bar with 'Page 1 of 6' and '1-10 of 57 total', and a table with the following data:

Date	Event	User	Hostname	Group
2015 Jan 30 10:26:17 AM	untrust: *https?://([a-zA-Z]*).com.*	[username]	[hostname]	Default
2015 Jan 30 10:25:35 AM	trust (permanent): http://www.dell.com/	[username]	[hostname]	Default

The Audit event table contains the following information:

- Date – the date and time the audit event was reported to the server
- Event – details about the type of event recorded, plus any additional information about the event, including user comments if available
- User – username of the user that reported the event
- Hostname – hostname of the host that the event was reported from
- Group – the group that the host was part of when the event was reported

These column headings can be used to sort the table based on the selected column header. By default, the Date column is selected to display the most recent event at the top of the table.

The search box can also be used to search the audit table for specific information.

Finally, the currently displayed table, based on selected filter, can be exported to an HTML or CSV report by pressing the “Export...” button at the bottom of the table.

Contacting Dell Support

For assistance with the Dell Protected Workspace Management System, please contact Dell Support at:

<http://support.dell.com>

DPWMS updates, DPW apps.xml updates and Installation Kit downloads can all be found at:

<http://www.dellprotectedworkspace.com/support>