OPSWARE INC
Automating IT™

# Opsware® SAS 5.5.3

# Release Notes

**Corporate Headquarters**

599 North Mathilda Avenue Sunnyvale, California 94085 U.S.A.

T + 1 408.745.1300 F +1 408.745.1383 www.opsware.com

# Table of Contents

# Introduction to Opsware SAS 5

Opsware Server Automation System (SAS) 5 provides new features, performance enhancements and several bug fixes. This document describes the new features found in Opsware SAS 5.5, 5.5.1, 5.5.2, and 5.5.3. This document provides information about the most significant bug fixes, and, in some cases, workarounds for known problems.

Opsware SAS 5.5 includes major improvements to the following existing features:

- Patch Management for Windows
- Direct SSH access to the Opsware Global Shell
- Global Shell audit trail
- OCC Client UI improvements
- New features in DCML Exchange Tool (DET) 2.5
- New features in DCI 1.8
- Support for new operating systems in Opsware SAS 5.5

# Improvements in Opsware SAS 5.5

## Patch Management for Windows

In this release, the new Patch Management for Windows feature enables you to more easily identify, install, and remove Microsoft® Windows patches and maintain a high level of security across managed servers in your organization. With the OCC Client, you can identify and install patches that protect against security vulnerabilities for the Windows 2000, Windows 2003, and Windows NT4.0 operating systems. These patches include Service Packs, Update Rollups, and hotfixes. You can use the OCC Client or a shell script to automatically import these patches from Microsoft.

To provide flexibility in how you identify and distribute patches to managed servers, Patch Management allows you to create patch policies that define groups of patches you need to install. By creating one or more patch policies and attaching it to a server or server group; you can effectively manage which patches get installed where in your organization. If you need to include or exclude a patch from a patch installation, Patch Management allows you to deviate from a patch policy by specifying that individual patch in a patch policy exception.

While Patch Management allows you to react quickly to newly discovered security vulnerabilities, it also provides support for strict testing and standardization of patch installation. After you have identified patches you need to install, Patch Management allows you to simulate (preview) the installation before you actually install a patch. This preview process tells you whether the servers you selected for the patch installation already have that patch installed. The preview process also reports on patch dependency and supersedence information, such as patches that require certain Windows products, and patches that obsolete other patches or are obsoleted by other patches.

Patch Management allows you to perform conformance tests (compliance checks) against managed servers and public server groups to determine whether all patches in a policy and a policy exception were installed successfully. You can schedule patch compliance scans to determine whether servers comply with their attached policies and exceptions, and then remediate non-compliant servers.

## Direct SSH Access to the Opsware Global Shell

This feature enables a direct SSH login to the Opsware Global Shell without requiring the OCC Client. The user name and password are the same as the user's Opsware user name and password.  This feature supports scp, sftp, and rsync over SSH. Support for sftp, for example, allows many third-party code deployment systems to push code onto the Opsware Global File System (OGFS). Another example is the use of rsync over an SSH channel to push code to and from the OGFS or a managed server's file system.

## Global Shell Audit Trail

When a user accesses or modifies a managed server with the Global Shell feature, Opsware SAS records the event in an audit log. The Global Shell audit logs contain information about the following events:

Logins and logouts with Global Shell and Remote Terminal sessions

File system operations (such as create and remove) on managed servers

Commands and scripts that run on managed servers through the Remote Opsware Shell (rosh)

These logs enable security administrators to find answers to the following questions:

What actions were performed on this managed server with the Global Shell or Remote Terminal?

Who performed these actions?

Which servers did a specific user log into and what did the user do?

The shell stream and script log files contain digital signatures and fingerprints, which are generated with the RSA-SHA1 algorithm. The Security Administrator can verify the signature and fingerprint of these log file.

By periodically removing the shell stream and script log files, Opsware SAS prevents these files from filling up the available disk space. The Opsware Administrator can set parameters that specify the removal of the log files based on file size or age.

## OCC Client UI

The OCC Client user interface has undergone a major redesign for ease of use and feature accessibility, including such changes as:

- An expandable "accordion" navigation pane (similar to Microsoft Outlook or Visio), giving you single click access to all major feature categories
- New Preview pane that shows a preview of the selected feature object, such as the hardware information of a server, patch policies for patches, and so on
- Window-based "Task Help" which provides context sensitive task-level help for individual steps of the new Patch Installation, Uninstallation, and Reconcile wizards – which allow you to install, reconcile, and uninstall Microsoft patches
- Improved menu organization. For example, depending upon which feature you have selected in the Navigation panel, the Actions menu allows you to perform numerous functions related to all main OCC Client features.

## New Features in DCML Exchange Tool (DET) 2.5

- New Patch Policy content filter allows you to export user defined patch policies from a mesh.
- "Synchronizing Multimaster Meshes with Deltas" shows you how to use three new command line options (--baseline, --incremental, and --delete) for

performing ‘incremental” exports and imports. These new options help you keep the content in your multimaster meshes synchronized and up to date.

- Email notification for export and import.
- customerName nested element supported for Application, Service Level, Server Group, and Template Filters, plus new examples to illustrate how filters work.
- New Preview option on import allows you to see all content deletions, modifications, additions that will be occur before you perform an import.
- packageType filter element now supports "Unknown" as a valid value.
- MRLs are now created with their correct location.

## New Features in DCI 1.8

- In the 'Recent Jobs by Date' report, there is a new job type named 'Reconcile Patches'.
- These two new OS versions are supported:

  SunOS 5.10 X86

  SuSE Linux Enterprise Server 9 X86_64

These two OS versions support these reports:

Patch Catalog

Package Catalog reports

Ad Hoc Reporting/Software and Patches

## Support for New Operating Systems in Opsware SAS 5.5

Opsware SAS 5.5 now supports the following operating systems for Opsware Agents:

- Solaris 10 (Niagara)
- Solaris 10 (64 bit x86)

- SUSE Linux Enterprise Server 9 (64 bit x86)

## Upgrade to Opsware SAS 5.5

In Opsware SAS 5.5, you can upgrade your Opsware installation to this release.

Opsware SAS 5.5 supports the following upgrade paths:

Upgrading a Standalone Core from 5.2 to 5.5

Upgrading a Multimaster Mesh from 5.2 to 5.5

Upgrading Opsware Satellites from 5.2 to 5.5

Upgrading a Standalone Core from 5.3 to 5.5

Upgrading a Multimaster Mesh from 5.3 to 5.5

Upgrading an Opsware Satellite from 5.3 to 5.5

Performing a rolling mesh upgrade from 5.2 to 5.5

Contact your Opsware Support Representative for information about upgrading to Opsware SAS 5.5.

# Improvements in Opsware SAS 5.5.1

## Support for OS Provisioning for Red Hat Linux 3 AS/ES/WS on Itanium

Opsware SAS 5.5.1 provides OS provisioning support for Red Hat Linux 3 AS/WS/ES on Itanium.

The procedure for setting up the OS provisioning feature is similar to the one documented for Linux OS provisioning in the Opsware SAS 5 Configuration Guide.

This section discusses the additional information required to perform OS provisioning on Red Hat Linux 3 AS/WS/ES on Itanium.

- When you create an image for the Linux Boot CD for Red Hat Linux 3 AS/WS/ES on Itanium, run the `mkia64cdrom.sh` script from the following location: `/cust/buildscripts/linux/bootstrap/cdrom`.

  For all other Linux servers, you need to run the `mkcdrom.sh` script to create a image for the Linux Boot CD.

- When you boot a Linux server with PXE or a CD, the following menu options are available:

  ```
  linux     - Linux Build Agent
  linux-txt - Linux Build Agent for serial consoles.
  ```

For Linux servers with serial consoles, select the `linux-txt` option.

See “Booting a Windows or Linux Server with PXE” in the Opsware SAS 5 User’s Guide for more information.

- For Linux servers with serial consoles, Opsware, Inc. recommends that you add the following custom attribute to an OS Definition to avoid a blank console.

name: kernel_arguments

value: console=ttyS0 nofb

See “Adding Custom Attributes to an OS Definition” in the Opsware SAS 5 Configuration Guide for information on how to add custom attributes to an OS Definition.

## DCI Report Update

For the Server reports Patch Catalog and Package Catalog, and for Ad Hoc report Software and Patches, you are now able to choose the following new operating systems versions as part of the report parameters:

- Red Hat Enterprise Linux AS 3 IA64
- Red Hat Enterprise Linux ES 3 IA64
- Red Hat Enterprise Linux WS IA64

The Patch Catalog and Package Catalog reports are located in the Server Reports / Software and Patch State folder.

The Software and Patches report is located in the Ad Hoc Reporting / Software and Patches folder.

## Upgrade to Opsware SAS 5.5.1

In Opsware SAS 5.5.1, you can upgrade your Opsware installation to this release.

Opsware SAS 5.5.1 supports the following upgrade paths:

Upgrading a Standalone Core from 5.2 to 5.5.1

Upgrading a Multimaster Mesh from 5.2 to 5.5.1

Upgrading Opsware Satellites from 5.2 to 5.5.1

Upgrading a Standalone Core from 5.5 to 5.5.1

Upgrading a Multimaster Mesh from 5.5 to 5.5.1

Upgrading an Opsware Satellite from 5.5 to 5.5.1

Contact your Opsware Support Representative for information about upgrading to Opsware SAS 5.5.1.

# Platform and Environmental Support

## Supported Operating Systems, Package Types, and File Types

The following table shows the operating systems, package types, and file types that Opsware SAS 5.5.3 supports. For complete information on package types and file types, see Chapter “Package Management” in the *Opsware SAS 5 Configuration Guide*.

| Operating System and Version | Package Type | File Types |
|---|---|---|
| **SPARC-processor-based hardware (sun4u, sun4us)** | | |
| Solaris 6, 7, 8, 9, and 10 | Solaris Package | uncompressed datastream |
| | Solaris Patch | .zip, .tar, .tar.Z, .tar.gz, .tgz, .jar |
| | Solaris Patch Cluster | .zip, .tar, .tar.Z, .tar.gz, .tgz |
| | RPM | .rpm |
| **UltraSPARC T1 -processor-based hardware (sun4v)** | | |
| Solaris 10 | Same as above | Same as above |
| **x86-processor-based hardware** | | |
| Solaris 10 | Same as above | Same as above |
| **X86-64-bit-processor-based hardware** | | |
| Solaris 10 | Same as above | Same as above |
| **x86-processor-based hardware** | | |
| Red Hat Linux (6.2, 7.1, 7.2, 7.3, 8.0), | RPM | .rpm |

| Operating System and Version | Package Type | File Types |
|---|---|---|
| Red Hat Enterprise Linux 2.1 AS/ES/WS,<br>Red Hat Enterprise Linux 3 AS/ES/WS,<br>Red Hat Enterprise Linux 4 AS/ES/WS, | | |
| SUSE Linux (Enterprise Server 8.0, Standard Server 8.0, Enterprise Server 9.0) | RPM | .rpm |
| Microsoft Windows (NT 4.0, Windows 2000 Server Family, Windows Server 2003) | Hotfix | .exe |
| | Service Pack | .exe |
| | MSI | .msi |
| | ZIP | .zip |
| | Security Patch | .exe |
| | Windows Utility | .exe |
| | Microsoft Patch Database | .xml, .cab |
| **x86-64-bit-processor-based hardware** | | |
| Microsoft Windows 2003 (64 bit) | Same as above | Same as above |
| **Itanium-processor-based hardware** | | |
| Red Hat Enterprise Linux 3 AS/ES/WS | RPM | .rpm |
| **IBM-POWER-processor-based hardware** | | |
| IBM AIX (4.3, 5.1, 5.2, 5.3) | RPM | .rpm |
| | LPP | .bff |
| | Base Fileset | N/A |
| | Update Fileset | N/A |
| | APAR | N/A |
| | Maintenance Level | N/A |
| **HP PA-RISC-processor-based hardware** | | |
| HP-UX (10.20, 11.00, 11.11, 11i v2) | Depot | .tar |
| | Product | N/A |
| | Fileset | N/A |

| Operating System and Version | Package Type | File Types |
|---|---|---|
| | Patch Product | N/A |
| | Patch File | N/A |
| **HP PA-Itanium-processor-based hardware** | | |
| HP-UX 11i v2 | Depot | .tar |

*Note****: Patch files for HP-UX 10.20 are packaged like other software files, and are not specified as patch file types. Consequently, you cannot install patches for HP-UX with the Patch Wizard; you can only install them with the Install Software Wizard.***

*Note:* ***For the supported operating systems for Opsware Agents, Opsware SAS supports Red Hat Linux 3 AS/WS/ES and Red Hat Linux 4 AS/WS/ES on both 32 bit and 64 bit x 86 architecture. All other versions of Red Hat Linux are supported on 32 bit architecture only.***

# Supported Core Operating Systems

The following table lists the supported operating systems for the Opsware SAS 5.5 core components (other than the Global File System Server). The Global File System server can be installed only on Red Hat Enterprise Linux 3 AS. Therefore, a single-server installation is supported only on Red Hat Enterprise Linux 3 AS.

| Supported Operating System for Opsware Core | Versions |
|---|---|
| Sun Solaris | Solaris 8 (on SPARC)<br>Solaris 9 (on SPARC) |
| Red Hat Linux | Red Hat Enterprise Linux 3AS (32 bit) |

The following table lists the supported operating systems for the Opsware Satellite.

| **Supported Operating System for Opsware Satellite** | **Versions** |
|---|---|
| Sun Solaris | Solaris 9 (on SPARC) |
| Red Hat Linux | Red Hat Enterprise Linux 3AS (32 bit) |
| SUSE Linux | SUSE Linux Enterprise Server 9 (32 bit) |

The Data Center Intelligence Server runs on Windows 2000 and 2003.

# Operating System Deprecation

When a managed operating system is “end of life” by the operating system vendor, Opsware marks the operating system as deprecated as an indication that the operating system might be dropped from the list of supported managed operating systems in a future release of the SAS product.

Deprecated operating systems are supported in the current release of the product in the same way non deprecated operating systems are.

Opsware monitors operating systems usage by its customers on an ongoing basis and base the operating system retirement decisions on operating system usage by current customers.

If you have any questions related to the Opsware operating system deprecation policy, please contact Opsware support or your account manager.

The following operating system versions are being deprecated in Opsware SAS 5.5.

Red Hat Linux 6.2

Red Hat Linux 7.1

Red Hat Linux 7.2

Red Hat Linux 7.3

Red Hat Linux 8.0

## Supported Installations for 5.5.1

The Opsware SAS 5.5.1 release supports the following installations:

- New installations of a standalone core
- New installations of a multimaster core
- New installations of a Satellite
- Automated Upgrade from Opsware SAS 5.2 to Opsware SAS 5.5.1 or Opsware SAS 5.5 to Opsware SAS 5.5.1. Contact your Opsware Support Representative for information about upgrading to Opsware SAS 5.5.1

## Documentation for 5.5.1

This release comes with the following documentation:

- *Opsware SAS 5.5.1 Release Notes*
- *Planning Deployments for Opsware SAS 5*
- *Opsware SAS 5 Deployment and Installation Guide*
- *Opsware SAS 5 Configuration Guide*
- *Opsware SAS 5 Administration Guide*
- *Opsware SAS 5 User's Guide*
- *Opsware Data Center Intelligence 1.8 Administrator’s Guide*
- *Opsware SAS DCML Exchange Tool 2.5 Reference Guide*
- *Opsware SAS Web Services API 2.2 Guide*
- *Opsware SAS Intelligent Software Module (ISM) Development Kit 2.0 Guide*
- *OCLI 2.0 Reference Guide*
- *CML Tutorial for Opsware SAS 5*

The Opsware SAS documentation is available online at https://download.opsware.com/kb/category.jspa?categoryID=20

Ask your Opsware administrator for the user name and password to access the site.

# Opsware Agent Compatibility

The majority of the Opsware Command Center features for Opsware SAS 5.5.1 are compatible with Opsware Agents 4.5 and later.

The Agent compatibility testing of Opsware SAS 5.5 features with Opsware Agent versions prior to 5.5.1 yielded the following results for the features in the Opsware Command Center Client.

## OCC Client Features

The following feature in the OCC Client is compatible with Opsware Agents 4.5 and later:

- Patch Management for Windows

To use the Reconcile Patches functionality in the Patch Management for Windows feature, you must upgrade to Opsware Agent 5.5.

The following features in the OCC Client are compatible with Opsware Agents 5.1 and later:

- Application Configuration
- Visual Packager
- Server Browser
- Server Compliance
- Global Shell
- OCC Client Scheduler

To access the Services functionality in the Server Browser feature, you must upgrade to Opsware Agent 5.2 or later.

# What's Fixed in Opsware SAS 5.5

The following bugs have a severity level of Critical or Major and are fixed in Opsware SAS 5.5.

## DCI

**Bug ID:** 25730

**Description:** DCI View Reports Link Didn’t Lead to Reports Home Page

**Subsystem:** DCI

**Platform:** Independent

**Resolution:** Previously, when you clicked the View Reports link on the Opsware Command Center homepage, the Server Reports page was displayed, rather than the Reports Home page, as indicated in the Navigation pane Reports links.

Now, when you click the View Reports link on the Opsware Command Center homepage, the DCI Reports homepage is displayed, giving you access to all report categories.

**Bug ID:** 31627

**Description:** Windows Patch and Patch Policies Created in the OCC Client

**Subsystem:** DCI

**Platform:** Independent

**Symptom:** Windows Patch Management policies created in the OCC Client may behave differently than what is expected for the following reports:

*Server Groups Without Patch Policies*

If you attach a patch policy to a server in the OCC Client without reconciling it, the server will still appear on the Server Without Patch Policies report.

Similarly, once a Windows patch policy is reconciled onto a server, if you detach the policy from the server without uninstalling the patch, the server will also not appear on the Servers Without Patch Policies report.

*Servers Without Patch Policies*

If you attach a patch policy to a server group in the OCC Client without reconciling it, the server group will still appear on the Server Groups Without Patch Policies report. Similarly, once a Windows patch policy is reconciled onto a server group, if you detach the policy from the server group without uninstalling the patch, the server group will also not appear on Servers Without Patch Policies reports.

*Unreconciled Software and Patches*

If you attach an OCC Client Windows patch policy to a server without reconciling it, the Unreconciled Software and Patches report under Ad-Hoc Reporting will display 'no variances'.

## Opsware Installer

**Bug ID:** 30668, 30693, 30692

**Description:** The Unix users (such as twist) created by the Opsware Installer should not have a password expiration date.

**Platform:** Independent

**Subsystem:** Opsware Installer

**Resolution:** Fixed. The expiration date of the twist user, for example, is 31 Dec. 2030.

## OS Provisioning

**Bug ID:** 30727

**Description:** Provisioning of Red Hat Enterprise Linux 3 WS x86_64 fails on certain types of hardware (Dell SC1425).

**Subsystem:** OS Provisioning

**Platform:** Redhat Linux x86_64

**Resolution:** Fixed. Updated the PXE/boot images with the latest set of drivers and hardware support from RedHat.For information on how to fix this problem in the field, see the following URL:
http://cetool.corp.opsware.com/owiki/UpdatingRedHatProv

**Bug ID:** 30864

**Description:** Unable to provision Windows 2003 if Service Pack 1 is slipstreamed into the media.

**Platform:** Windows 2003

**Subsystem:** OS Provisioning

**Resolution:** Fixed. The calls to the System Management BIOS (SMBIOS) program were replaced with calls to a Windows Management Instrumentation (WMI) script.

## Opsware Command Center

**Bug ID:** 29971

**Description:** Opsware Command Center does not state that non-ASCII passwords are invalid.

**Subsystem:** Opsware Command Center

**Platform:** Independent

**Resolution:** Fixed. The Change My Password window includes this text: “The password must be at least 6 ASCII characters long.”

## OCC Client

**Bug ID:** 27806

**Description:** Previously, it was possible to push an invalid value set from the Opsware Command Center Client to a managed server without a warning.

**Platform:** Platform Independent

**Subsystem:** OCC Client - Application Configuration Management

**Resolution:** This has been fixed.

**Bug ID:** 29211

**Description:** If an Opsware core contained multiple versions of a configuration file, and when you reverted one of the versions of the configuration file to a previous state, a backup of the configuration file was created in the Opsware-managed server. If you wanted to revert the other versions of the same configuration file, revert would fail if the managed server contained the backup configuration file.

**Subsystem:** OCC Client - Application Configuration Management

**Platform:** Independent

**Resolution:** This has been fixed.

**Bug ID:** 30630

**Description:** Two ports required between Opsware core and a Windows machine for RDP.

**Platform:** Windows

**Subsystem:** OCC Client, Remote Terminal

**Resolution:** Fixed. Just one port (1002) needs to be open on the managed server. Port 3389 does not have to be open for this feature to work. For more information, see the section "Open Ports" in chapter 2 of the Installation Guide.

## Opsware Web Services API

**Bug ID:** 29058

**Description:** Duplicate server IDs specified for the addServers operation of the ServerGroup Web Service are not ignored and an exception is thrown.

**Subsystem:** Server Groups Backend

**Platform:** Independent

**Resolution:** Fixed. When the addServers operation is invoked, duplicate server IDs are ignored.

**Bug ID:** 30504

**Description:** A user with read-only permission to a specific customer and to all node stacks can associate the customer with a node.

**Subsystem:** Core - Web Services Data Access Engine

Platform: Independent

**Resolution:** Fixed. An exception is thrown when the user does sufficient permissions to perform setCustomers or detachCustomers operations of the NodeWebService.

# What's Fixed in Opsware SAS 5.5.1

The following bugs have a severity level of Critical or Major and are fixed in Opsware SAS 5.5.1

## DET

**Bug ID:** 32750

**Description:** Deletions fail on nodes exported with 'path' directive.

**Subsystem:** DCML Exchange Tool (DET)

**Platform:** Independent

**Resolution:** Previously, when an export contained nodes marked for deletion that were originally exported using the 'path' directive and the nodes were not at the 2nd level of a stack, the deletions on import would fail strangely. Some deletions succeeded but deleted the wrong node, while others would not be locatable. Nodes may have also printed in the logs and output with the incorrect names.

This has been fixed. However, any exports created with versions of DET previous to Opsware SAS 5.5.1 with this type of node marked deleted will still cause problems on import. You should create a new export file using the new version DET with these nodes marked deleted in order for them to be deleted correctly in the destination mesh.

## OS Provisioning

**Bug ID:** 32828

**Description:** In Opsware SAS 5.5, you were unable to provision a Solaris V490 server.

**Subsystem:** OS Provisioning

**Platform:** Solaris

**Resolution:** Fixed. The fix was achieved by rebuilding the detect_hardware.sparc for the Solaris buildscripts.

**Bug ID:** 32802

**Description:** OS provisioning for the Sun V1280 (Netra T12) failed on Opsware SAS 5.2, 5.3 and 5.5.

**Subsystem:** OS Provisioning

**Platform:** Solaris

**Resolution:** Fixed. The fix was achieved by assigning the right boot kernel to the machine in the dhcp configuration.

## Opsware Command Center

**Bug ID:** 32844

**Description:** In the Opsware Command Center, if there were more than 10 shared scripts entries only 10 shared scripts entries were displayed to the user. You were unable to access the other scripts by paging down.

**Subsystem:** Opsware Command Center

**Platform:** Independent

**Resolution:** Fixed.

## Opsware Command Center Client

**Bug ID:** 30118

**Description:** If a browser proxy setting was used to launch the OCC Client, you received an error in the Java Web Start log. You were unable to launch the Remote Terminal functionality in the OCC Client. Also majority of the other OCC Client functionality which depended on the OGFS, were disabled.

**Subsystem:** OCC Client - OGFS

**Platform:** Platform Independent

**Resolution:** Fixed. You can use the browser proxy settings to launch the OCC Client. Make sure that the proxy server is configured to port 8080.

**Bug ID: 32753**

**Description:** The populate-opsware-update-library script does not include an option for uploading files from a path.

**Platform:** Independent

**Subsystem:** OCC Client - Windows Patch Management, Backend

**Resolution:** Fixed. The script has a new option:

```
--upload_from_update_root <path>
```

This option enables you to upload files from the specified path (directory) instead of from the vendor's website. This option is ignored if `--download_only` is also specified. If a patch is not in the specified path, the script skips the patch. If `--verbose` is specified, the script displays on stdout which patches have been skipped during the upload.

For more information about the script, see the section "Automatically Importing Windows Patches" in the Opsware SAS 5 Administration Guide.

**Bug ID:** 32892

**Description:** The Opsware Global File System (OGFS) Server logs were being rotated once every five minutes, even if the log files were empty. Also after 100 log files were created, the logging for the OGFS was disabled.

**Subsystem:** OCC Client - Global Shell

**Platform:** Platform Independent

**Resolution:** Fixed. In Opsware SAS 5.5.1 the OGFS Server logs are rotated only when they reach their maximum size or if there changes to the OGFS configuration file.

**Bug ID:** 32894

**Description:** The reconcile patches process failed when a patch policy contained one or more patches and the following conditions existed:

The Error Options check box in the Reconcile Options step ("Attempt to continue running if an error occurs") was not selected.

The reboot option for the patch reconcile was set to "Reboot servers after each patch install or uninstall".

At least one of the patches failed to install or uninstall.

The reconcile patches process finished with a "Completed with Errors" message and the patches were not installed on the server.

**Subsystem:** OCC Client - Patch Management for Windows

**Platform:** Windows

**Resolution:** Fixed.

## Opsware Satellite

**Bug ID:** 32869

**Description:** When the Admin port is configured to use SSL then a race condition can occur. The condition is that the Admin port thread closes a socket before the SSL shutdown. The SSL shutdown may inject a SSL shutdown message into a closed (harmless) or newly open socket.

Since the race was very tight it was only observed on multi-cpu servers. One observed side-effect was the SSL shutdown message was injected into the TCP stream of an ident port query.

**Subsystem:** Opsware Gateway

**Platform:** Independent

**Resolution:** Fixed. The fix was achieved by not allowing multiple threads to access the Opsware Gateway ident port at the same time.

# Known Problems, Restrictions, and Workarounds in Opsware SAS 5.5

This section describes the workarounds to known problems in Opsware SAS 5.5.

## Access and Authentication

**Bug ID:** 23457

**Description:** Changes to permissions are not reflected in the current session of the Opsware Command Center Client.

**Platform:** Platform Independent

**Subsystem:** Access and Authentication

**Symptom:** As an Opsware administrator, when you make changes to permissions in a user group, the changes are not propagated to the Server Explorer if a server browser is currently open in the Opsware Command Center Client.

**Workaround:** Close the server browser and open a new server browser.

**Bug ID:** 27445

**Description:** The addition of an Application or Service Level node to Patch Install Order Tab fails with access denied error.

**Platform:** Platform Independent

**Subsystem:** Access and Authentication

**Symptom:** When you try to add an Application or Service Level node to Patch Install Order Tab, the operation fails with the following error:

```
Error ID:   16640444
Error Name:       Twist Method Error
Exception Info:   com.opsware.exception.TwistException
```

```
<message=''> <message=' <Access denied>
```

**Workaround:** To add an Application node to Patch Install Tab, you need the following permission:

| Permission | Description |
|---|---|
| Model: Applications | Manage Application Nodes |

To add a Service Level node to Patch Install Tab, you need the following permission:

| Permission | Description |
|---|---|
| Model: Service Levels | Manage Service Level Nodes |

To obtain the required permissions, contact your Opsware administrator.

**Bug ID:** 27675

**Description:** For delegated authentication, client certificates are not supported.

**Platform:** Platform Independent

**Subsystem:** Access and Authentication

**Symptom:** If the external LDAP server is configured to require client certificates, then the Opsware SAS is unable to successfully communicate with the external LDAP server. Specifying client certification properties in the twist.conf file does not help, because the external LDAP server expects a distinct client certificate per user.

**Workaround:** When connecting to an external LDAP server, use either of the following approaches:

- Simple bind over cleartext.
- Simple bind over anonymous SSL (no client certificate).

## Code Deployment

**Bug ID:** 27529

**Description:** Run sequence fails if the user is not assigned to the CDS History Viewer group.

**Platform:** Platform Independent

**Subsystem:** Code Deployment

**Symptom:** When a user belonging to the CDS Production Sequence Performer group attempts to run a sequence, the sequence fails leading to the following error:

The input you entered was invalid or you tried to access a resource not available to you. Please check the URL entered or click the back button and check your input.

**Workaround:** In order to successfully run a sequence the user must be assigned to the CDS History Viewer group.

## Configuration Tracking

**Bug ID:** 22674

**Description:** Adding a Configuration Tracking Policy entry to a server with an existing entry leads to an error.

**Platform:** Platform Independent

**Subsystem:** Configuration Tracking

**Symptom:** When you try to add a Configuration Tracking Policy entry to a server, which already has an existing entry, you get the following error:

```
OpswareError: spin.usage [ module: spinobj.py, method:
setBPD, line: 18749, hostname: m131.dev.opsware.com,
timestamp: 03/Mar/2005 230818, msg: Cannot overwrite
existing backup policy directive /etc/hosts:FILE ]
```

**Workaround:** Locate the server which already has the backup policy you are trying to set. Remove that backup policy from the server and try the operation again.

## Core

**Bug ID:** 30663

**Description:** The Apache Proxy used by the Opsware Command Center allows SSLv2 clients.

**Subsystem:** Core

**Platform:** Independent

**Symptom:** The security community has been advising against SSLv2. However, the Apache Proxy has been built with openssl 0.9.7i and hence is not vulnerable to the "rollback vulnerability" cited in the advisory. In addition, the SSLv2 ciphers are not permitted by the server.

**Workaround:** To completely disable SSLv2 connections, add the following directive to the configuration file: "SSLProtocol all -SSLv2".

**Bug ID:** 31510

**Description:** The Web Services Data Access Engine (twist) allows SSLv2 clients to connect to it on port 1032.

**Subsystem:** Core

**Platform:** Platform Independent

**Symptom:** The security community has been advising against SSLv2 due to known vulnerabilities. The application server used by the Web Services Data Access Engine uses certicom SSL libraries which are not known to be vulnerable against "version-rollback" attacks.

**Workaround:** Ensure that any client connecting to the Web Services Data Access Engine is capable of negotiating SSLv3 or TLSv1.

**Bug ID:** 32577

**Description:** The hub hangs on shutdown.

**Subsystem:** Core

**Platform:** Platform Independent

**Symptom:** In a multi-box core, the hub and the Software Repository (word) are installed on different boxes.  On the Software Repository box, either the OS or the NFS service is shut down. The hub becomes non-responsive, OGSH sessions stop working, and the hub can not be shut down with "/etc/init.d/OPSWhub stop". Any OGSH sessions, /etc/init.d/OPSWhub script executions, and java processes for OPSWhub are stuck waiting to access the NFS share from the Software Repository box, and will not respond to kill -9.

**Workaround:**Start the NFS service on the Software Repository box,
or unmount the NFS systems on the hub box using the following commands:

```
umount -f /var/opt/OPSWmnt/store
umount -f /var/opt/OPSWmnt/audit
```

## Content

**Bug ID:**  28117

**Description:**  Application Configurations will not restart services not already running.

**Platform:**  Unix/Linux

**Subsystem:**  Content – Application Configuration

**Symptom:** At this time, application configurations will not start services that are not already running. In the event you wish to configure a Unix or Linux service that is not already running on a system, please start the service before using application configurations or you may get an error from the application configuration post-script execution. This error can be ignored, as the configuration has in fact been pushed to the server, but the service has not been started.

**Workaround:**  Please start the service before using application configurations or you may get an error from the application configuration post-script execution.

## DCML Exchange Tool

**Bug ID:** 25383

**Description:** Importing a template containing a Service Level or Application node with a special character ”/” in its name field results in the Service Level or Application node not being attached to the template.

**Platform:** Platform Independent

**Subsystem:** DET

**Symptom:** If you Import a template containing a Service Level or Application node with a special character ”/” in its name field, the template is imported but the Service Level or Application node is not attached to the template.

**Workaround:** None. Do not create a Service Level or Application node with special character”/” in its name field.

**Bug ID:** 27940

**Description:** Special characters in Custom Attribute Value in XML export document causes error.

**Platform:** Platform Independent

**Subsystem:** DET

**Symptom:** Importing an XML export document containing any object strings that resemble XML tags (for example, </string>) in a Custom Attribute value leads to the following error:

```
Command Error Message: rethrew: {E301} XML document
structures must start and end within the same entity.
[root@copper1 joe]#
```

**Workaround**: When Importing an XML export document, do not use special characters containing any object strings that resemble XML tags (for example, </string>) in a Custom Attribute value.

**Bug ID:** 28775

**Description:** Export Package Filter Windows Hotfix and Service Pack Issue

**Platform:** Windows Packages

**Subsystem:** DCML Exchange Utility (DET)

**Symptom:** For Microsoft Hotfixes and service packs, it is possible that the Microsoft package you want to export has not yet had its binary file uploaded, even though the package shows as existing in the core. For example, a user may have uploaded the Microsoft Patch Database to the core, but not yet uploaded the actual binary file of the package. In this case, a unit record for the package will have been created in the Opsware model, but there is no content to export. In this case, if you try to export the package content using the Package Export Filter, the content of the Microsoft package will not be exported.

**Workaround:** Make sure that before you export a Microsoft Hotfix package or Service Pack package the package has previously been uploaded to the core you are exporting the content from.

**Bug ID:** 30021

**Description:** Non-ASCII characters in the target directory name for Configuration Tracking are not displayed properly after a DET import.

**Platform:** Platform Independent

**Subsystem:** DET

**Symptom:** If you try to use the DET import to import an application node with configuration tracking policy set and if the target file or the directory name has non-ASCII characters, then after the import, the file or directory name containing the non-ASCII characters is not displayed correctly.

**Workaround:** None.

**Bug ID**: 30600

**Description:** Import error occurs during custom fields import when target core has same custom field name.

**Platform**: Any

**Subsystem**: DET Import

**Summary**: When importing a custom field, the error "OpswareError:spin.DBUniqueConstraintError" may be returned if the target core already has a custom field with the same display name.

**Workaround**: Ensure there is are no conflicting display names, or rename the display name prior to importing.

**Bug ID:** 31423

**Description:** Using the DET to do an export that includes a Solaris-based OS from a Linux-based core, and trying to import this on Solaris-based core might fail in certain cases.

**Platform:** Sun OS_5.10_X86 OS

**Subsystem:** DCML Exchange Tool (DET)

**Workaround (partial):** Replace the tar binary (/usr/bin/tar) available on the target core (specifically the machine running the package repository) with a GNU tar binary for the target OS. This should only be done for the duration of the import, and the original tar binary should be restored afterwards. Take case to confirm that the permissions and ownership on the binary is the same after restoring it than before replacing it.

We recommend using the workaround only if you run into this problem.

For your reference: The workaround doesn't fix all problems associated with the root cause of this bug, but at least will allow you to complete the import successfully.

**Bug ID:** 32028

**Description:** DET Import output information inconsistent with preview summary when overwriting container packages, when the import package is a superset of the destination package.

**Platform:** Independent

**Subsystem:** DET Import

**Symptom:** When trying to overwrite an existing container package (HP Depot, AIX LLP, and Solaris packages) where the package being imported is a superset of the container package in the import destination, the preview of the import (using the --noop option) will correctly show the new packages as being "created," but the output information after import will incorrectly show "overwrite" for the newly created packages.

**Workaround:** None.

**Bug ID:** 32032

**Description:** Import Preview (--noop) presenting incorrect summary information when overwriting container packages, when the import package is a subset of the destination package.

**Platform:** Independent

**Subsystem:** DET Import

**Symptom:** When trying to overwrite an existing container package (HP Depot, AIX LLP, and Solaris packages) where the package being imported is a subset of the container package in the import destination, the preview of the import (using the --noop option) incorrectly shows existing package with "overwrite" instead of "duplicate".

**Workaround:** None.

**Bug ID:** 32601

**Description:** If Windows MBSA patch definitions in the source mesh and target mesh are not in sync, Windows patches that are not defined in both meshes will not get imported into the target mesh.

**Platform:** Windows

**Subsystem:** DCML Exchange Tool (DET)

**Symptom:** If the Windows MBSA patch definitions in a source mesh do not match the Windows MBSA patch definitions in the target core you are importing the patch into, any patches from the source mesh that are not defined in the target mesh will not be imported.

**Workaround:** Make sure that the Windows MBSA patch definitions are the same for both the source mesh and the destination mesh, or undefined Windows patches will not get imported.

## Installer

**Bug ID:** 27268

**Description:** Linux portmapper can assign Opsware ports to Network File System (NFS) services.

**Platform:** Linux

**Subsystem:** Installer

**Symptom:** In Linux, the portmapper can assign Opsware ports to Network File System (NFS) service which can cause the installation of Opsware SAS to fail since the ports are not available.

**Workaround:** During installation add an entry for the component name and the port in the `/etc/services` file to prevent the portmapper from assigning Opsware ports to Network File System (NFS) services.

**Bug ID:** 28663

**Description:** Installation of an Opsware Satellite fails if you try to reinstall the Satellite after uninstalling it.

**Platform:** Platform Independent

**Subsystem:** Installer

**Symptom:** After uninstalling an Opsware Satellite, if you try to reinstall the Satellite again without deactivating the Opsware Agent from the core, the installation fails with the following error:

```
OpswareError:
args:  ()
error_name:  spin.permissions
faultCode:  9
```

```
faultString:  spin.permissions
hostname:  thunder1.thunder.qa.opsware.com
line:  6861
method:  updateDevice
module:  spinmethods.py
params:  {'msg': 'Attempt to register server with bootstrap
cert after crypto has been generated and with allow_recert
set to 0.'}
```

**Workaround:** After you uninstall an Opsware Satellite, log in to the Opsware Command Center and deactivate the server before reinstalling the Satellite again.

**Bug ID:** 28730

**Description:** Error when installing the OCC component on Solaris

**Platform:** Solaris

**Subsystem:** Installer

**Symptom:** This problem occurs when the Opsware Installer is installing the Opsware Command Center component on a core server. Although it successfully installs the occapp package, the Opsware Installer displays these lines and exits:

```
package occapp is not installed
<time-stamp> Component installation script encountered an
error
```

**Workaround:** Check to see if the executable rpm (or a symbolic link) exists in one of the following directories:

```
/bin
/usr/bin
/sbin
/usr/sbin
/usr/local/bin
```

If does exist in one of these directories, remove or rename the file and run the Opsware Installer again.

**Bug ID:** 28824

**Description:** Cannot connect to a Windows 2003 server using the Remote Terminal option of the OCC Client.

**Subsystem:** Installer

**Platform:** Independent

**Symptom:** From the OCC Client select the server and from the Actions menu select Remote Terminal. The following error message is displayed:

```
The connection was ended because of a network error.
```

**Workaround:** This error occurs if the EgressFilter entry in the core Opsware Gateway properties file is incorrect. (The entry in the Gateway properties file provided by the Opsware Installer is correct, so this error occurs only if you've edited the file manually.) To fix this error, log into the core server running the Opsware Gateway and edit this file:

```
/var/opt/OPSWgw/cgw0-<facility>/opswgw.properties
```

Include the following entry in the properties file:

```
opswgw.EgressFilter=tcp:*:3389:HUB:
```

Restart the Opsware Gateway:

```
/etc/init.d/opswgw-cgw-<facility> restart
```

**Bug ID:** 29041

**Description:** Uninstaller fails if it uses a response file with no oi.components.

**Subsystem:** Installer

**Platform:** Independent

**Symptom:** When uninstalling a core, the uninstaller might generate the following traceback message:

```
Traceback (innermost last):
  File "./manage_opsware.py", line 183, in manage_opsware
  File "./manage_opsware.py", line 344, in validateParams
  File "./manage_opsware.py", line 325, in getComponentParams
KeyError: oi.components
[time-stamp] Opsware Installer has encountered an error:
[time-stamp] Error Type : exceptions.KeyError
[time-stamp] Error Value: oi.components
[time-stamp] Exiting Opsware Installer.
```

**Workaround:** Perform the following steps:

1. Add an oi.components section to the response file. For example:
   %oi.components docs
2. Run the uninstaller again.
3. After the uninstall completes, remove the oi.components section you just added. If you don't remove the oi.components section, problems may occur if you try to use the response file in the future without an action file.

**Bug ID:** 29161

**Description:** During the installation of the Opsware Global File System (OGFS), `ogfs.store.host` and `ogfs.audit.host` parameters cannot be set to any host.

**Subsystem:** Installer

**Platform:** Linux

**Symptom:** This problem occurs during the installation of the OGFS for the core, and the `ogfs.store.host` or `ogfs.audit.host` parameter is set to a host other than the OGFS or the Software Repository (theword).In this case, the Opsware Installer fails to install the OGFS and displays the following error message:

```
Running script hub/pre.
Mounting /var/opt/OPSWmnt/store mount:
<ip>:/cust/ogfs/store failed,
reason given by server: No such file or directory
[timestamp]
```

```
Component installation script encountered an error (exit
status 32)
[timestamp] Exiting Opsware Installer.
```

**Workaround:** For the `ogfs.store.host` and `ogfs.audit.host` parameters, use the default values or specify the host of either the OGFS or the Software Repository.

## Intelligent Software Module (ISM) Development Kit

**Bug ID:** 30106

**Description:** The ismusertool cannot upload an ISM from a managed server that communicates with the core through an Opsware Gateway.

**Subsystem:** IDK

**Platform:** Independent

**Symptom:** The upload displays a traceback that includes the following lines:

```
  . .
File "/usr/local/ismtool/lib/ismtoollib/ismusertool.py",
line 293,
  in cmdline()
File "/usr/local/ismtool/lib/ismtoollib/ismusertool.py",
line 269,
  in cmdline checkIsmUpdateRole()
. . .
```

Could not set up a tunnel through any of [(<ip-address>, 3002)]

**Workaround:** Run ismusertool as the Opsware admin user on a server
that does not communicate with the core through a Gateway.

**Bug ID:** 30156

**Description:** Setting allowservers on an uploaded ISM causes a data integrity error.

**Subsystem:** IDK

**Platform:** Independent

**Symptom:** The following example commands show how this problem might occur:

- Create an ISM node with a multi-level opswpath such as

  /System Utilities/${NAME}/${VERSION}/${PLATFORM}.
- ismtool --addPathProp allowservers --propValue 1 ismx
- ismtool --upload ismx
- Run a data integrity test on the core.

The test reports an error because the parent node of ismx has an allowservers value of 0. That is, the parent node does not allow servers to be assigned to it.

**Workaround:** Make sure that the allowservers values
of the uploaded ISM node and the parent node are the same.

## Operating System Provisioning

**Bug ID:** 26125

**Description:**

**Platform:** Platform Independent

**Subsystem:** OS Provisioning

**Symptom:** When you reprovision a server, the Opsware Command Center (OCC) uses the display name when displaying a server, whereas the Opsware Command Center Client (OCC Client) uses the hostname when displaying a server.

By default, when you first install an OS on a server, the Opsware Command Center populates the display name field with the hostname of the server. If a user resets this name after OS installation or when reprovisioning the server with a new OS, the name displayed in the Opsware Command Center and the name displayed in the OCC Client will not match.

**Workaround:** None

**Bug ID:** 30844

**Description:** Re-provision of SUSE Linux Enterprise Server 9 (SLES) x86_64 fails.

**Subsystem:** OS Provisioning

**Platform:** SLES-9-x86_64

**Symptom:** This problem occurs only when the first partition is swap. During the re-provisioning, the mini-agent downloads successfully, but the progress stalls at "Waiting for ... reboot" and eventually times out. The server never reboots.

**Workaround:** To prevent this problem, do not build SLES9 x86_64 servers with swap as the first partition. If you encounter this problem, the workaround is to provision the server the way you normally would with Opsware SAS: Deactivate the server, then boot it into the Server Pool via PXE or a boot CD. Then, continue with the process as specified in the Opsware SAS User's Guide.

## Opsware Agent

**Bug ID:** 26747

**Description:** The Agent Installer fails to create the registry key on a Win2K server if MS AntiSpyware is installed on the server.

**Platform:** Windows

**Subsystem:** Agent

**Symptom:** When you install an Opsware Agent on a Win2K server, the Agent Installer fails to create the registry key if MS AntiSpyware is installed on the server. As a result, the Opsware Agent is not installed successfully.

**Workaround:** In order to install an Opsware Agent successfully on a Win2K server with MS AntiSpyware, disable the MS AntiSpyware before installing the Opsware Agent.

**Bug ID:** 27590

**Description:** Unable to access the C drive on Windows NT4 TSE server after installing an Opsware Agent.

**Platform:** Windows NT

**Subsystem:** Agent

**Symptom:** After installing an Opsware Agent on Windows NT4 TSE server, the C drive is not accessible via the Opsware Global Shell.

**Workaround:** None.

**Bug ID:** 28176

**Description:** ogshcap.dll file is not available if an Opsware Agent is uninstalled and reinstalled without restarting the server.

**Platform:** Windows

**Subsystem:** Opsware Agent

**Symptom:** During Opsware Agent uninstallation on a Windows server, the Agent Installer tries to remove the ogshcap.dll file from the following location:

%SystemRoot%\system32\ogshcap.dll

If the file is open or is in use, the Agent Installer is unable to remove the ogshcap.dll file. The Agent Installer then prompts you to restart the server and removes the file after restart.

After uninstalling the Opsware Agent, if you reinstall it without restarting the server, the ogshcap.dll file does not get copied. During the next reboot you will not be able to access the server's file system since ogshcap.dll file is no longer available.

**Workaround:** Restart the server after the uninstalling the Opsware Agent and before reinstalling the Opsware Agent.

**Bug ID:** 28950

**Description:** Unable to Deploy Opsware Agents to Windows server after manually uninstalling and reinstalling the Opsware Agent on the Windows Agent Deployment Helper server.

**Platform:** Windows

**Subsystem:** OCC Client - ODAD

**Symptom:** If you manually uninstall the Opsware Agent on a server that is the Windows Agent Deployment Helper, and then reinstall the Opsware Agent on that server, the Opsware Discovery and Agent Deployment (ODAD) feature will be unable to deploy agents to Windows servers. Deployment to UNIX-based servers will not be affected.

**Workaround:** After uninstalling an Opsware Agent perform the following steps:

1. On the Agent Deployment Helper server, log in and use "Add/Remove Programs" to remove the Windows Agent Deployment Helper application.
2. If you did not deactivate and delete the server from Opsware SAS, two servers registered with the same hostname. The status of the old server will be UNREACHABLE. With the OCC and deactivate, then delete the old server
3. Exit any OCC Client applications that may be running.
4. Perform the procedure for installing the Windows Agent Deployment Helper. See “Installing Windows Agent Deployment Helper” in the Opsware SAS Deployment and Installation Guide for step by step instructions on how to install Windows Agent Deployment Helper.
   After these steps are performed, the ODAD feature should be able to deploy to Windows servers.

**Bug ID:** 29075

**Description:** ODAD fails to deploy Opsware Agents to a Windows server which previously had the Windows Agent Deployment Helper installed

**Platform:** Windows

**Subsystem:** OCC Client – ODAD

**Symptom:** Deploying an Opsware Agent using the Opsware Discovery and Agent Deployment (ODAD) feature to a Windows server which previously had the Windows Agent Deployment Helper installed fails with an error.

**Workaround:** Perform the following steps before you deploy Opsware Agents to a Windows server which previously had the Windows Agent Deployment Helper installed:

1. Log in to the Windows Server
2. Navigate to Control Panel > Network and Dial up Connections.

3. Disable the adapters created by Windows Agent Deployment Helper. These adapters will be labeled as “ADT Helper <n>, where <n> is a number”.

**Bug ID:** 29395

**Description:** Opsware Discovery and Agent Deployment feature is unable to discover a realm, if the display name of the realm is changed.

**Subsystem:** OCC Client - ODAD

**Platform:** Platform Independent

**Symptom:** If the display name of a realm is changed, then the Opsware Discovery and Agent Deployment feature is unable to discover the realm. As a result in the OCC Client the realm is not displayed in the Scan in drop-down list.

**Workaround:** None. Do not the change the display name of the realm.

**Bug ID:** 29735

**Description:** The Unmanaged Server page appears, when you open a managed server in the Agent Deployment – OCC Client page.

**Subsystem:** OCC Client - ODAD

**Platform:** Platform Independent

**Symptom:** After successfully deploying Opsware Agents using ODAD, the status of the server in the server list is updated to a managed server. In the Agent Deployment – OCC Client page when you open the managed server the Unmanaged Server page for that server appears.

**Workaround:** None.

**Bug ID:** 29748

**Description:** Opsware Discovery and Agent Deployment (ODAD) fails if sudo or su is not in the user’s PATH on the unmanaged server.

**Subsystem:** OCC Client - ODAD

**Platform:** Platform Independent

**Symptom:** When you use sudo to log in to an unmanaged server, deploying Opsware Agents using ODAD fails, if sudo or su is not in your PATH on the unmanaged server.

**Workaround:** None. When you use sudo to log in to an unmanaged server, verify that the sudo or su is in your PATH on the unmanaged server.

**Bug ID:** 29934

**Description:** ODAD may not accurately AIX 5.3 during a network scan.

**Subsystem:** OCC Client - ODAD

**Platform:** Platform Independent

**Symptom:** While performing a network scan to identify servers in which to install an Opsware Agent, ODAD may not be able to identify AIX 5.3 accurately.

**Workaround:** None.

**Bug ID:** 30303

**Description:** Sometimes Opsware Discovery and Agent Deployment reports a server to be managed by Opsware, even though it not managed by Opsware.

**Subsystem:** OCC Client - ODAD

**Platform:** Platform Independent

**Symptom:** A server is considered to be under Opsware management if the Opsware Discovery and Agent Deployment feature discovers that it is listening for TCP connections on port 1002. In some cases, this information can be incorrect.

For example, if some other software is installed and listening on port 1002, the server will be identified as managed by Opsware, when in fact it is not.

Conversely, if a server is under Opsware management, but its Opsware Agent was shut down at the time the server was scanned, the server will not be identified as managed by Opsware.

**Workaround:** None.

## Opsware Command Center

**Bug ID:** 22865

**Description:** Uploading a large file in a custom field results in an error.

**Platform:** Platform Independent

**Subsystem:** OCC **-** Manage Servers

**Symptom:** When you upload a large file in a custom field to associate the file with a server, you may receive a java.lang.OutOfMemoryError.

**Workaround:** None. Be cautious when you upload a file in a custom field. Opsware recommends not uploading a large file in a custom field.

**Bug ID:** 24470

**Description:** The results of a second server search in a Wizard are displayed in a new window.

**Platform:** Platform Independent

**Subsystem:** OCC **-** Wizards

**Symptom:** In any Wizard, when you search for servers, by clicking the search tab, the search results are displayed in the same window. When you perform a second search, the search results are displayed in a new window. This behavior is observed when you access the Opsware Command Center using the FireFox browser.

**Workaround:** Perform the following steps to display the second server search results in the same window:

1. After you perform the first server search in a Wizard, click the Previous button and then the Next button in the wizard. The Select Server page appears.
2. Select the search criteria. The search results are displayed in the same window.

**Bug ID:** 25772

**Description:** A warning dialog appears when you perform an operation on a server from the Manage Server page.

**Platform:** Platform Independent

**Subsystem:** OCC **-** Manage Servers

**Symptom:** When you perform an operation on a server from the Manage Server page, you may see the following warning dialog:

```
You are about to leave a secure Internet connection. It
will be possible for others to view information you send.
Do you want to continue?
```

This behavior is only exhibited when you access the Opsware Command Center using Internet Explorer.

**Workaround:** To turn off this warning dialog, select the "In the future, do not show this warning." Checkbox and then click the Yes button.

Or

1. Open Internet Explorer.
2. In the Home Page, Select Tools > Internet Options.
3. In the Internet Options page, click the Advanced tab.
4. Uncheck “Warn if changing between secure and not sure mode.”
5. Click Apply.

**Bug ID:** 26120

**Description:** The Network Reports Links is not visible under Reports in the navigation panel after Data Center Intelligence Reporting (DCI) is installed.

**Platform:** Platform Independent

**Subsystem:** OCC - System Configuration

**Symptom:** The Network Reports Link is not visible under Reports in the navigation panel after Data Center Intelligence Reporting (DCI) is installed.

**Workaround:** To make the Network Report link visible, perform the following steps:

1. From the Opsware Command Center Home Page, Click Administration > System Configuration from the navigational panel. The System Configuration: Set Configuration parameters page appears.

2. Click Save. The Network Reports link is now visible under Reports in the navigation panel.

**Bug ID:** 26382

**Description:** The Opsware Command Center does not allow server groups to be deleted from My Servers page.

**Platform:** Platform Independent

**Subsystem:** OCC **-** Server Groups

**Symptom:** In the Opsware Command Center, you cannot delete server groups from the My Servers Page.

**Workaround:** None.

You can delete servers from the Manage Servers Page. To delete a server group, perform the following steps:

In the Manage Servers Page, click the check box next to the server group you want to delete.

From the Edit menu, choose Delete Group. A confirmation message appears, detailing the number of servers and server groups in the server group that you want to delete.

Click OK to complete the deletion of the server group.

The screen refreshes, showing the list of servers and groups without the deleted server group.

**Bug ID:** 27345

**Description:** Unable to create a Service Level and associate it with Customer = Not Assigned.

**Platform:** Platform Independent

**Subsystem:** OCC **-** Service Levels

**Symptom:** In the Opsware Command Center, the user is unable to create a Service Level and associate the Service Level to Customer = Not assigned.

**Workaround:** Create a Service Level and associate the Service Level to Customer = Customer Independent. Edit the Service Level and reassign it to Customer = Not assigned.

**Bug ID:** 27718

**Description:** Twist exception appears during cloning of servers when the customer and platform on the master server does not match the target server.

**Platform:** Platform Independent

**Subsystem:** OCC **-** Manage Servers

**Symptom:** In the Opsware Command Center when you clone a server, the source server (master server) and the target servers need to have the same platform and the same customer. A twist exception appears if the master server and the target server do not have the same customer and same platform.

**Workaround:** Before cloning a server, reassign the customer and platform on the target server to that of the master server.

**Bug ID:** 27854

**Description:** Running a communication Test on a server in an unreachable Satellite throws a 5000 error.

**Platform:** Platform Independent

**Subsystem:** OCC **-** Communication Test

**Symptom:** Running a communication Test on a server in an unreachable Satellite and viewing the results of the job leads to the 5000 error:

```
Error Summary
Name: Standard 500 Error
Description: 500 Internal Server Error
Message Text: The server encountered an unexpected
condition which prevented it from fulfilling the request.
Exception Info:
java.util.NoSuchElementExceptionjava.util.LinkedList$ListI
```

```
tr.next(LinkedList.java:490)
<<< traceback here >>>
```

**Workaround:** None. It is not possible to retrieve job specific results for a Communication Test for a server in an unreachable Satellite. The results are recorded in the "current" communication test status for a server in an unreachable Satellite, which is visible from the server properties page or from the communication test view in the server list.

**Bug ID:** 29160

**Description:** When you log into the Opsware Command Center, the browser prompts you twice to accept the certificate.

**Subsystem:** Opsware Command Center

**Platform:** Independent

**Symptom:** When you access the OCC, you are prompted twice to accept the certificate. The first prompt is related to authentication and the second one is related to the certificate name not matching the Opsware core URL.

**Workaround:** To access the OCC, accept the certificate twice.

**Bug ID:** 29201

**Description:** Unable to add packages to the OS definition using the Prepare Operating System Wizard.

**Subsystem:** Opsware Command Center - Wizard

**Platform:** Linux

**Symptom:** While creating an OS definition for Red Hat Linux using the Prepare Operating System wizard, adding packages to the OS definition in the in the Review Packages page may fail in one of the following ways:

- An error occurs when you confirm the package to add in the Review Packages page. This error asks you to retry your login.

- Only the new packages added are saved. The existing packages are not saved.

**Workaround:** Close the Prepare Operating System wizard. Navigate to Software - Operating System and select the created OS definition which you just created. Select the Packages tab and then add the additional packages.

**Bug ID:** 29293

**Description:** Microsoft Excel fails to open CSV files containing non-ASCII characters.

**Subsystem:** OCC

**Platform:** Platform Independent

**Symptom:** In the Opsware Command Center, you can generate CSV files containing information about manage servers and export it to Microsoft Excel. If the file contains non-ASCII characters, Microsoft Excel fails to open the file with the correct encoding. Since Microsoft Excel 2002 and 2003 does not support UTF-8 encoding, Unicode characters are not displayed correctly.

**Workaround:** You can use any one of the following two workarounds.

**Method 1**

Perform the followings steps to display non-ASCII characters correctly in Microsoft Excel:

1. Download and Save the CSV file.
2. Open the CSV file using Microsoft Windows Notepad. Windows Notepad displays non-ASCII characters correctly.
3. From the Edit menu, select Select All.
4. From the Edit menu, Select Copy
5. Open Microsoft Excel.
6. In a blank Excel worksheet, place the cursor on cell A: 1.
7. From the Excel Edit menu, select Paste. The contents from windows Notepad, is copied to Microsoft Excel.

8. In Microsoft Excel, from the Data menu select Text to Columns.

9. Change the delimiter from Tab to Comma. Click finish.

10. Save the Microsoft Excel worksheet.

Method 2

1. While importing CSV files which contain non-ASCII characters, use OpenOffice (open source software). OpenOffice supports non-ASCII characters.

2. Copy the contents of the CSV file to a blank Microsoft Excel worksheet to display non-ASCII characters correctly.

**Bug ID:** 29568

**Description:** A user belonging to the Administrators group can create a customer but does not have write access to resources associated with the customer.

**Subsystem:** OCC - Customers

**Platform:** Independent

**Symptom:** A user who belongs to the Administrators group creates a customer. In the Opsware Command Center, the user's Profile indicates that all customer accounts are readable and writeable. However, the user does not have access to resources (such as packages) associated with the customer. For example, in the OCC Client, the user cannot view the newly created customer in the Customer Assignment field of the Create Package window.

**Workaround:** Assign the user to a group that has read and write access to the customer.

**Bug ID:** 29681

**Description:** Agent caches old locale even after the locale is changed.

**Subsystem:** Opsware Command Center - DSE

**Platform:** Independent

**Symptom:** Change the locale of a managed server and run a DSE that echoes multi-byte characters that require the new locale.  On the Script Output tab these characters appear as question marks.
**Workaround:** Restart the Agent on the managed server where you've changed the locale and then run the DSE script again.

**Bug ID:** 30515
**Description:** A JAVAscript error occurs when you create a custom attribute for a server group with a "\" at the end of the custom attribute name.
**Subsystem:** OCC – Custom Attributes
**Platform:** Platform Independent
**Symptom:** If you create a custom attribute for a server group with a "\" at the end of the custom attribute name, a JAVAscript error occurs. As a result no subsequent operations like adding, deleting, or editing a custom attribute can be performed for that server group.
**Workaround:** When you create a custom attribute for a server group, do not use "\" at the end of the custom attribute name.
If case you create a custom attribute for a server group with "\" at the end of the custom attribute name, delete the server group and create a new one.

**Bug ID:** 30167
**Description:** The psrvr.properties file includes entries for pref.occ.support.href and pref.occ.support.text, which specify the support link at the bottom of the Opsware Command Center. Non-ASCII characters are entered for pref.occ.support.text are not displayed correctly by the Opsware Command Center.
**Subsystem:** Opsware Command Center
**Platform:** Independent
**Symptom:** In the link displayed by the Opsware Command Center, the non-ASCII characters appear as boxes. Also, the link does not work.

**Workaround:** If you edit the psrvr.properties file with a text editor, to insert non-ASCII characters, convert the characters to UTF-8 with the Java native2ascii tool.

**Bug ID:** 32248

**Description:** Java Script error occurs when you try to delete a large number of templates in the Opsware Command Center.

**Subsystem:** Opsware Command Center

**Platform:** Independent

**Symptom:** In the Opsware Command Center, when you try to delete a large number of templates, the following Java Script error occurs:

```
Invalid Pointer.
```

**Workaround:** None. Do not delete more a large number of templates at one time from the OCC.

**Bug ID:** 32707

**Description:** An error message is not displayed if you try to install an application on a server with incompatible OS version.

**Platform:** Platform Independent

**Subsystem:** Opsware Command Center - Wizards

**Symptom:** Using the Install Software Wizard, if you try to install an application on a server with incompatible OS version and skip the Preview step, the job is completed without displaying an error message.

The job also does not appear in the My Jobs page.

**Workaround:** None.

## Opsware Command Center Client

**Bug ID:** 25904

**Description:** Unable to launch a remote terminal for servers that are running Unix and Windows operating systems.

**Platform:** Platform Independent

**Subsystem:** OCC Client **-** Global Shell

**Symptom:** When you try to launch a remote terminal from the Servers list window in the OCC Client, you will see a telnet session that briefly displays `connecting to 127.0.0.2`… and then closes.

**Workaround:** This is a bug in WindowsXP SP2. You must install the hotfix that is available at http://support.microsoft.com/default.aspx?kbid=884020.

**Bug ID:** 26033

**Description:** The following (example) warning occurs when you create a snapshot using selection criteria that includes the Documents and Settings directory, and files in that directory:

```
Unable to checksum C:\Documents and
Settings\LocalService\NTUSER.DAT: [Errno 13] Permission
denied:
'C:\\Documents and Settings\\LocalService\\NTUSER.DAT'
```

**Platform:** Platform Independent

**Subsystem:** OCC Client – Audit & Compliance

**Symptom:** When you include the Documents and Settings directory (and files in that directory) in your file system selection criteria, the snapshot will be created with an `Unable to checksum C:\Documents and Settings`… warning.

**Workaround:** Server Compliance does not support the ability to read the contents of this file. Content for these types of files will not be recorded in a snapshot. Add exclusion rules in your selection criteria to filter out these types of files.

**Bug ID:** 26115

**Description:** Leaving required Value Set Editor element values will delete element line in configuration file when previewed or pushed.

**Subsystem:** OCC Client - Application Configuration

**Platform:** OS Independent

**Symptom:** If a required Value Set element is left blank, the application configuration will become invalid and if the application configuration is pushed, the element in the configuration file on the server might be deleted.

**Workaround:** Do not leave required Value Set Editor elements empty, or the required value will be removed from the configuration file when previewed or pushed. The exception to this is optional blocks, which do not have to have required values entered, unless another field in that block has a value entered.

**Bug ID:** 26858

**Description:** An `UnmarshalException` error occurs when the amount of data that is sent to the OCC Client causes the OCC Client to run out of memory.

**Platform:** Platform Independent

**Subsystem:** OCC Client **-** Audit & Compliance

**Symptom:** When you create a package that uses a snapshot (of HKEY_LOCAL_MACHINE and additional files) as the source, and you try to expand the Windows Registry in the Create Package (Details tab) window, Visual Packager displays the following error: `UnmarshalException.`

**Workaround:** Specify selection criteria that will collect fewer objects. For example, select only parts of the file system and not the entire file system of a target.

**Bug ID:** 27211

**Description:** Opening multiple OCC jobs from the OCC Client causes the job to open in the last active browser window.

**Platform:** Platform Independent

**Subsystem:** OCC Client

**Symptom:** When you open a job created in the Opsware Command Center (OCC) from the Opsware Command Center Client (OCC Client), the job is displayed in the last active browser window.

Workaround: None.

**Bug ID:** 27214

**Description:** Invoking OCC Client Help causes Online Help to open in last active browser window.

**Platform:** Platform Independent

**Subsystem:** OCC Client

**Symptom:** When you invoke Opsware Command Center Client Help, the Online Help is displayed in the last active browser.

Workaround: None.

**Bug ID:** 27276

**Description:** A `serverCompliance.FailedToExtractContents` error occurs when you try to create a snapshot or perform an audit using selection criteria that includes a file that has an encrypted attribute.

**Platform:** Platform Independent

**Subsystem:** OCC Client – Audit & Compliance

**Symptom:** When you try to create a snapshot or perform an audit that includes an encrypted file in the selection criteria, you will get a `serverCompliance.FailedToExtractContents` error when you try to browse the snapshot or audit results.

**Workaround:** Server Compliance does not support encrypted files. Content for these types of files will not be recorded in a snapshot or in audit results. Add exclusion rules in your selection criteria to filter out these types of files.

**Bug ID:** 27454

**Description:** In the audit results of a file and directory comparison, an inherited permission does not accurately display.

**Platform:** Platform Independent

**Subsystem:** OCC Client **-** Audit & compliance

**Symptom:** In the audit results of a file and directory comparison, if the permission is an inherited permission from an ancestor of the parent (that is a grandparent, great grandparent, and so on), it does not accurately display.

**Workaround:** Use the Remote Terminal in the OCC Client to display the permissions for the object in question.

**Bug ID:** 27586

**Description:** Renaming filenames limitation in Global Shell, OCC Client Server Browser/File System.

**Platform:** Platform Independent.

**Subsystem:** OCC Client - Global Shell, OCC Client Server Browser/File System

**Symptom:** Using the Global Shell or OCC Client Server Browser/File System to rename an existing filename on a Windows managed server will fail - even if you answer "Yes" to the prompt to overwrite dialog. This failure will occur even if your user has write permission to the file system and the destination file is writable.

**Workaround:** To copy "file1" to an existing file called "file2" in C:\TEMP.

1. Open the global shell.
2. Navigate to the directory containing the file you want to rename:
   ```
   cd /opsw/Servers/@/foo.server/files/Administrator/C/TEMP
   ```
3. Delete the target file:
   ```
   rm file2
   ```
4. Rename (move) the source file to the target:
   ```
   mv file1 file2
   ```

**ID:** 27693

**Description:** Pushing an application configuration to a server can timeout when the template runs as a post-install script that reboots the server.

**Platform:** Independent

**Subsystem:** OCC Client **-** Application Configuration Management

**Symptom:** Pushing an application configuration to a server can fail when it contains a post-install script (like the one below) that reboots the server:

```
@!filename-key=/arnold/hosts/post.bat@
@!filename-default=/c/tmp/post.bat@
echo "post.bat"
%SystemRoot%\system32\tsshutdn 0 /REBOOT /V
```

The push fails because the reboot exceeds the four minute timeout set for Application Configuration. The error is not reported back to the job dialog window. The job proceeds until it times out.

**Workaround:** In the post-install script, specify the server to reboot asynchronously, and the job will succeed.

**Bug ID:** 27733

**Description:** A `java.lang.outofMemory` error occurs when you try to browse a snapshot that contains too many Windows Registry keys.

**Platform:** Platform Independent

**Subsystem:** OCC Client – Audit & Compliance

**Symptom:** A `java.lang.outofMemory` error can occur for many different reasons, the most common reason is because the snapshot is too large. The Java Console log provides more detailed information about an error that occurs during snapshot parsing.

**Workaround:** Shut down the OCC Client, and restart it.

**Bug ID:** 27815

**Description:** The packaging server for the AIX4.3 operating system was incorrectly configured. The OCC Client erroneously configured a RedHat AS3 server as the packaging server.

**Platform:** Platform Independent

**Subsystem:** OCC Client **-** Visual Packager

**Symptom**: This should only happen if you reinstalled the Opsware SAS and did not reset the packaging server settings in the OCC Client.

**Workaround:** When you have a new Opsware installation, you must reset the packaging server settings in the OCC client.

**Bug ID:** 28001

**Description:** When you use the Copy To action from a Snapshot browser or Audit Result browser to copy a file and directory (with different users and user groups) from one Unix server to another Unix server, the same user name (uid) is displayed for both the source and target.

**Platform:** Platform Independent

**Subsystem:** OCC Client **-** Audit & Compliance

**Symptom:** If you use the Copy To action to copy the following source file:

```
 -rw-r--r-- 1 qatest qatest 46 Jun 9 21:29 first.txt
```

to a target file that is:

```
-rw-r--r-- 1 root other 24 Jun 9 17:52 first.txt
```

you will see the uid (instead of the group name) displayed as the following file:

```
-rw-r--r-- 1 101 qatest123 46 Jun 9 21:29 first.txt
```

When you run the `ls -n` command, you will see that the uid is the same for both the source and the target. In this example, `qatest123` has the same uid of `qatest`.

When you run the `ls -n` command on the source, you will see the following information:

```
-rw-r--r-- 1 101 100 46 Jun 9 21:29 first.txt
```

When you run the `ls -n` command on the target, you will see the following information:

```
-rw-r--r-- 1 101 100 46 Jun 9 21:29 first.txt
```

**Workaround:** Verify that both servers use the same user name (uid) and group name (gid) mapping.

**Bug ID:** 28054

**Description:** A deleted and recreated Opsware user is unable to browse the Server Explorer file system in the Opsware Command Center Client.

**Platform:** Platform Independent

**Subsystem:** OCC Client **-** Opsware Global File System

**Symptom:** When the Opsware administrator deletes an Opsware user and recreates the same Opsware user, the recreated user is unable to browse the Server Explorer file system in the Opsware Command Center Client.

**Workaround:** Restart the Opsware Global File System (OGFS) to disable access to the Server Explorer file system.

**Bug ID:** 28165

**Description:** OCC Client fails if you have JRE 1.4.1 installed.

**Platform:** Platform Independent

**Subsystem:** OCC Client

**Symptom:** When you launch OCC Client from a system which has JRE 1.4.1 installed, the following error occurs:

```
An error occurred while launching/running the application.
Title: OCC Client
Vendor: Opsware Inc.
Category: Download Error
Missing signed entry in resource:
http://occ.brownsox.qa.opsware.com/webstart/xercesImpl.jar
```

**Workaround:** Java JRE 1.4.2 must be installed on your system to run the OCC Client. You can download this version of Java from http://java.sun.com/j2se/1.4.2/download.html

**Bug ID:** 28774

**Description:** When the packaging server resides in an Opsware Satellite (behind a Software Repository Cache), the create package process fails.

**Platform:** Platform Independent

**Subsystem:** OCC Client – Visual Packager

**Symptom:** If you try to create a package when the packaging server resides in an Opsware Satellite (behind a Software Repository Cache), the following error occurs:

```
Error Encountered
SUMMARY:
Name: Upload To Software Repository Cache Prohibited
Description: Uploads to Opsware Software Repository Caches
are prohibited
Solution: Upload the package to an Opsware Software
Repository in an Opsware Core.
```

**Workaround:** The Visual Packager feature does not support uploads to the Software Repository Cache (which is an Opsware Satellite component that contains local copies of files). Therefore, if the packaging server resides in a Satellite, Visual Packager will not work. Do not configure a packaging server to be behind an Opsware Satellite with a Software Repository Cache configuration. Set up the packaging server in an Opsware core so that you will be able to upload packages to the Software Repository.

**Bug ID:** 28969

**Description:** When a snapshot or audit fails to upload to the Software Repository, the error message does not tell you to check the disk space on the Software Repository.

**Platform:** Platform Independent

**Subsystem:** OCC Client – Audit & Compliance

**Symptom:** The snapshot or audit progress status bar displays that the process is uploading the snapshot or audit to the Software Repository and then the job fails.

**Workaround:** When this error occurs, check the available disk space on the Software Repository.

**Bug ID:** 29067

**Subsystem:** OCC Client - Application Configuration, Jobs Window

**Platform:** Independent

**Description:** In the Audit Application Configurations job window, the Server Details area might report that all "Configurations are in compliance". However, the Servers area of the same job might show the out-of-sync icons.

**Workaround:** This is a known caching issue. The cache has not caught up with the latest update on the server. After a few minutes, open the window again and the correct icons will display.

**Bug ID:** 29136

**Description:** For Application Configurations that use JScript or VBScript pre- or post-install and post-error scripts, the push operation will succeed although the scripts fail.

**Subsystem:** OCC Client - Application Configuration

**Symptom:** When pushing an application configuration that contains a JScript or VBScript pre- or post-install and post-error scripts, the push succeeds even though the scripts fail. In these cases, the push ignores the scripts altogether. The application configuration does not catch the failure of the scripts and allows the push to complete without errors.

**Workaround:** The author of these types of scripts must make sure the scripts are free of errors to detect possible failures, and have the script forcibly return a non-zero exit status by invoking WScript.Quit(<status>).

**Bug ID:** 29192/29237

**Description:** Error when you open a terminal window for a Windows or Unix server.

Subsystem: OCC Client – Remote Terminal, Global Shell

**Platform:** Independent

**Symptom:** In the OCC Client you can use the Remote Terminal feature to open a terminal window for a Unix or Windows server and the Global Shell feature to open a terminal window for Opsware Global File System (OGFS). If the Remote Terminal session or the Global shell session for server times out or is disconnected, the following error displays:

```
    An internal error has occurred.  See the console log for
    details.
```

**Workaround:** Restart the OCC Client and then open a new terminal window for a Windows or Unix server.

**Bug ID:** 29335

**Description:** Error is given when trying to view contents of a file, stating "unsupported charset"

**Platform:** Platform Independent

**Subsystem:** OCC Client

**Symptom:** When viewing a file contents that is in multibyte characters, and JRE was installed before the special fonts were installed on the server, the contents of the file are garbled and an error is given.

**Workaround:** This error is caused when the JRE is installed BEFORE the multibyte fonts are loaded on the local system. To solve this error, you will need to uninstall JRE, and then relaunch the OCC Client.

Instructions:

1) Close the OCC Client.

2) Open "Add/Remove Programs"

3) Remove all "Java 2 Runtime Environment, SE v1.4.2_XX" and "Java 2
SDK, SE v1.4.2_XX" programs.

4) Close the Control Panel

5) Access OCC Client again using the Opsware Command Center and go to the home page

6) Click the Launch OCC Client link.

7) You will be prompted to install JRE if you use Internet Explorer to access OCC; follow instructions to install the 1.4.2 JRE.

8) When finished, the OCC Client login dialog should appear.

To reinstall Asian language fonts, follow these instructions:

1) Open the Control Panel

2) Open "Regional and Language Options"

3) Click/select the "Languages" tab

4) Make sure the "Install files for East Asian Languages" checkbox is checked

5) Click the Apply button; dialogs will display and the fonts will install. Wait until installation is finished.

6) Click OK to close the "Regional and Language Options" dialog.

7) Relaunch the OCC Client.

**Bug ID:** 29374

**Description:** When a Windows registry key and a value have the same name and exist in the level in the registry hierarchy, only the registry key is displayed in the Global Shell terminal and in the Server Explorer registry browser.

**Subsystem:** OCC Client – Global Shell

**Platform:** Independent

**Symptom:** Only the Windows registry key is displayed in the Global Shell terminal and in the Server Explorer registry when the registry key and value have the same name and exist in the level in the registry hierarchy.

**Workaround:** None.

**Bug ID:** 29382

**Description:** Import Values into Application Configuration incorrectly logged as a "preview"

**Platform:** Platform Independent

**Subsystem:** OCC Client- OGFS

**Symptom:** If you import a value set from a configuration file or application configuration into an application configuration using the Import Values button, this action will incorrectly be logged in the Hub as an application configuration Preview.

**Workaround:** None.

**Bug ID:** 29501

**Description:** Changing the encoding with the swenc command might cause problems for background processes.

**Subsystem:** OCC Client – Global Shell

**Platform:** Linux

**Symptom:** In a Global Shell session, change the encoding with the swenc command. Background processes that are running in the Global Shell session might fail.

**Workaround:** Wait until background processes have completed before changing the encoding with swenc.

**Bug ID:** 29521

**Description:** No information is logged in the audit trail log after you close the Global Shell window by clicking the X button.

**Subsystem:** OCC Client – Global Shell

**Platform:** Independent

**Symptom:** There is no information in the audit trail log after you close the Global Shell window by clicking the X button in the upper right corner of the window.

**Workaround:** End your Global Shell session and Remote Terminal session by exiting the shell (ctrl-d or exit in bash, similar in other shells) rather than closing the window by clicking the X button. If you do not do this, the audit message that corresponds to the end of the session will still get logged, but not until after you log off the OCC Client.

**Bug ID:** 29872

**Description:** Visual Packager supports only ASCII characters in the application node path name.

**Subsystem:** OCC Client - Visual Packager

**Platform:** Platform Independent

**Symptom:** If you include non-ASCII characters in the application node Name in the Specify Application window, Visual Packager creates the new node in the Software Tree (with packages attached) and each non-ASCII character displays as a question mark (?).

**Workaround:** None.

**Bug ID:** 29980

**Description:** In CML sequence aggregation, namespace sequences append when either sequence-append or sequence-prepend is specified instead of prepending when prepend is specified.

**Platform:** Platform Independent

**Subsystem:** Application Configuration

**Symptom:** In some cases, even though sequence-prepend is specified for a namespace sequence, the sequence will use sequence-append. The CML contained in this tag definition would be affected by this bug:

If the CML contained this tag definition:

```
@sequenceA;unordered-namespace-set@
ITEM: @.item1@ @item2@
```

This sequence would append and prepend as specified:

```
@sequenceB;unordered-string-set;;;field-delimiter-is-eol@
ITEM: @.@
```

**Workaround:** Try to simplify namespace sequences into string sequences; in the above example, you would replace sequenceA with sequenceB.

**Bug ID:** 30029

**Description:** Cursor remains an hour glass after opening a scheduled job

**Platform:** Platform Independent

**Subsystem:** OCC Client - My Jobs

**Symptom:** In the My Jobs window, double clicking a scheduled job opens up the Schedule Job dialog window. However, the mouse pointer remains an hour glass.

**Workaround:** Move the mouse around a few times and the cursor reverts back to an arrow.

**Bug ID:** 30109

**Description:** Actions cannot be performed on services with names containing non-ASCII characters.

**Subsystem:** OCC Client - Server Explorer

**Platform:** Linux

**Symptom:** In the OCC Client, the Services window of the Server Explorer enables you to change run levels and perform actions such as start and stop. However, if the service name contains non-ASCII characters, you cannot use the Services window to change the run levels or perform the actions.

**Workaround:** Use only ASCII characters in service names.

**Bug ID:** 30265

**Description:** Data-manipulation script in application configuration can only be executed on individual servers.

**Platform:** Platform Independent

**Subsystem:** OCC Client **-** Application Configuration

**Symptom:** If you have a data-manipulation script inside an application configuration, you will only be able to run this script on individual servers, not on an entire server group from the Server Groups Browser.

**Workaround:** If you would like to run the data-manipulation script on a server group from inside the Server Groups Browser, you will need to run it on each individual server.

**Bug ID:** 30271

**Description:** Shift_JIS file names within a ZIP package are not displayed correctly.

**Subsystem:** OCC Client - Visual Packager

**Platform:** Windows

**Symptom:** With the Visual Packager of the OCC Client, upload a ZIP package that contains files whose names contain Shift_JIS characters. If you view the contents of the uploaded package in the Opsware Command Center, the Shift_JIS characters of the file names are not displayed correctly. (However, the package metadata, which is always UTF-8 on Windows, is displayed correctly.)

**Workaround:** Use only ASCII characters in these file names.

**Bug ID:** 30275

**Description:** An Application Configuration script fails to run if the script name has non-ASCII characters.

**Subsystem:** OCC Client - Application Configuration

**Platform:** Independent

**Symptom:** When you try to run the script, an error such as the following might appear:

```
Script execution failed: Code: '1', script name: ...
server id: ... stdout: ... stderr: ... cannot open
```

**Workaround:** Use only ASCII characters in the file names of Application Configuration scripts.

**Bug ID:** 30354

**Description:** When an Opsware user is deleted, the home directory is not deleted. If a user with the same user name is subsequently created, the new user inherits the existing home directory (and all contents).

**Subsystem:** OCC Client – Global Shell

**Platform:** Independent

**Symptom:** If an Opsware user is deleted and a new Opsware user is created with the same user name, the new user can view files that the previous user had in their home directory.

**Workaround:** Do not reuse user names. If you do reuse user names, delete the Global Shell home and tmp directories when you delete the owning user of those directories.

**Bug ID:** 30369

**Description:** Files with size 0 are not listed correctly in the OCC Client Server Explorer's file browser.

**Platform:** Platform Independent

**Subsystem:** OCC Client

**Symptom:** Any file with a size of zero (0) will have its properties listed incorrectly in the OCC Client's Server Explorer file browser. The file will show "Unknown" as the file type, and show an old date as the last modified date.

**Workaround:** None.

**Bug ID:** 30429

**Description:** If you try to create a package that includes a patch that needs to be uploaded to the Software Repository, where the Customer Assignment for the new package is not set to Customer Independent, the upload will fail.

**Subsystem:** OCC Client - Visual Packager

**Platform:** Independent

**Symptom:** When you try to create a package that includes a patch that needs to be uploaded to the Software Repository and the Customer Assignment for the new package is not set to Customer Independent, the patch will not be uploaded and the package will not be created.

**Workaround:** Change the Customer Assignment to Customer Independent to upload the patch to the Software Repository and create the new package. Patches can only be owned by Customer Independent. Only patches with the Customer Assignment of Customer Independent can be uploaded to the Software Repository.

**Bug ID:** 30495

**Description:** OCC Client not launch directly, from outside of the Opsware Command Center.

**Platform:** Windows 2003

**Subsystem:** OCC Client

**Symptom:** If you attempt to launch the OCC Client application on a Windows 2003 server from outside of the Opsware Command Center (for example, from your desktop), it will not launch.

**Workaround:** Adjusting your browser's security settings will solve this issue. Note, however, that making these changes will revert your browser's security to Windows 2000 levels.

1. From the control panel, choose Add/Remove Programs 2. Click Add/Remove Windows Components 3. Uncheck "Internet Explorer Enhanced Security Configuration"

4. Click Next as many times as necessary, and then Finish.

5. Restart your browser.

**Bug ID:** 30514

**Description:** User must belong to Administrators group to browse metabase.

**Subsystem:** OCC Client - Global Shell

**Platform:** Windows

**Symptom:** In a Global Shell session, a non-admin user has permission to view the `/opsw/@/<server>/metabase` subdirectory of OGFS. However, the user cannot browse metabase, and the session displays the message `"Protocol error."`

In the agent.err file, the following lines appear:

```
<timestamp> [10997] ERR  Error from Agent for unique <int>:
. . .
File ".\base\ops\shell\ogfs_wshandler.py", line 402, in run
```

```
   File ".\base\ops\shell\metabase.py", line 72, in
   metabase_getattr
```

**Workaround:** Login as a member of the Administrators group (admin).

**Bug ID:** 30557

**Description:** The Opsware user "nobody" is unable to launch the Global Shell.

**Subsystem:** OCC Client – Global Shell

**Platform:** Independent

**Symptom:** Create an Opsware user "nobody" and grant it self shell permissions. Log in to the OCC Client as "nobody" and try to launch the Global Shell. The telnet client briefly displays and then disappears. Try to log in as "nobody" directly on the Hub (using /opt/OPSWogfs/bin/ogsh). This also fails and no error message is displayed.

**Workaround:** Do not create an Opsware user called “nobody”.

**Bug ID:** 30559

**Description:** An "RFS specific error" can occur in the OGFS when you try to access the file system of a managed server, where the specified login account is disabled on the managed server. For example, the "ls /opsw/Server/@/m221.qa/files/arnold/" command fails if the login account "arnold" on server "m221.qa" is disabled.

**Subsystem:** OCC Client – Global Shell

**Platform:** Independent

**Symptom:** When you enter "ls /opsw/Server/@/m221.qa/files/arnold” on the managed server "m221.qa”, where the login account “arnold” is disabled, Opsware Global Shell displays an “RFS specific error”.

**Workaround:** Enable the login account on the managed server or revoke permissions to access the managed server using that account.

**Bug ID:** 30597

**Description:** When sequence-prepend is specified, outer scope sequence values are used even though Block Inheritance is specified.

**Platform:** Platform Independent

**Subsystem:** OCC Client - Application Configuration

**Symptom:** When Block-inheritance is specified on a sequence that is set to sequence-prepend, it is incorrectly blocking the inner scope values instead of the outer scope values. Thus, it is possible to end up with values from the outer scope, instead of the inner scope in the merged sequence.

For example:

```
CML file
=========
@!filename-key="/test/file"@
@!filename-default="/tmp/file"@
@!namespace=/test/preserveValuesWithExplicitNull/@
@!sequence-prepend@
set1=@set1;unordered-string-set@

Server Scope Values
===================
set1/1=a
set1/2=b
set1/3=c
Server Instance Scope Values
============================
set1/1=Block Inheritance
set1/2=1
set1/3=2
Preview Output
==============
   set1=a b c
```

**Workaround:** Use sequence-append.

**Bug ID:** 30664

**Description:** There is no progress indicator displayed when you import the MBSA 2.0 patch database using the OCC Client.

**Subsystem:** OCC Client – Patch Management for Windows

**Platform:** Windows

**Symptom:** After you click Import in the Import from Vendor window or in the Import Patch Database window, the window disappears and there is no UI display that indicates the progress of the operation.

Workaround: None.

**Bug ID:** 31127

**Description:** The Microsoft Support page displays when you try to view the vendor's documentation for some Windows NT4 patches.

**Subsystem:** OCC Client - Patch Management for Windows

**Platform:** Windows NT4.0

**Symptom:** When viewing the vendor's documentation for some Windows NT4 patches, the Microsoft support page (http://support.microsoft.com/) is displayed, instead of a Security Bulletin or Knowledge Base Article. When no vendor documentation URL is supplied in the Microsoft patch database, Opsware substitutes this URL.

**Workaround:** None.

**Bug ID:** 31325

**Description:** You must use the Ctrl key to add to the list of Microsoft products in the Edit Patch Products window.

**Subsystem:** OCC Client – Patch Management for Windows

**Platform:** Windows

**Symptom:** When you select additional products in the Edit Patch Products window and then click Select, only the products you just selected will be included in the list. The products that previously existed in the list are no longer selected.

**Workaround:** In the Edit Patch Products window, press and hold down the Ctrl key and select the products you want to add, and then click Select to add them to the existing list. This will assure that the newly added products and the previously selected products are included in the list.

**Bug ID:** 31455

**Description:** Even though Patch Management for Windows is fully supported by an Opsware Agent that is version 4.5 or later, you can still attach a patch policy to a server or server group when you are using an Agent that precedes version 4.5.

**Subsystem:** OCC Client – Patch Management for Windows

**Platform:** Windows

**Symptom:** You are using an Agent that is older than Opsware SAS 4.5 and can attach a patch policy to a server or server group.

**Workaround:** Upgrade the Agent to version 4.5 or later to fully support Patch Management for Windows.

**Bug ID:** 31456

**Description:** Patch install and patch uninstall actions should be disabled when the target server is using an Opsware Agent that precedes version 4.5.

**Subsystem:** OCC Client - Patch Management for Windows

**Platform:** Windows

**Symptom:** Even though you can install a patch on or uninstall a patch from a server that has an Agent that precedes Opsware SAS 4.5, Patch Management for Windows is fully supported only by an Opsware Agent that is version 4.5 or later.

**Workaround:** Do not install a patch on or uninstall a patch from a server that is running an Agent that precedes version 4.5. Upgrade the Agent to version 4.5 or later to fully support Patch Management for Windows.

**Bug ID:** 31553

**Description:** In the OCC Client, the service status might not be updated correctly when the user acts on a service.

**Subsystem:** OCC Client

**Platform:** Platform Independent

**Symptom:** If the user stops, starts, or restarts a service before the initial loading of the service list has completed, the status might not reflect the user's action on the service.

**Workaround:** Before acting on a service, wait for the progress bar to show that the loading of the service list has completed.

**Bug ID:** 31704

**Description:** F1 Help Opening in Multiple Browser Windows in Internet Explorer

Platform: Windows

**Subsystem:** Online Help in OCC Client

**Symptom:** When you click F1 in a window in the OCC Client and are using Internet Explorer as your default browser, each time you click F1 the help system will open in a new instance of Internet Explorer.

**Workaround:** To prevent a new IE window for each invocation of context-sensitive help, perform the following steps:

1. In IE, select Tools -> Internet Options.
2. Select the Advanced tab.
3. Select "Reuse Windows for launching shortcuts."
4. Click OK.

**Bug ID:** 31715

**Description:** Cache refresh problems in some OCC Client windows.

**Platform:** Independent

**Subsystem:** OCC Client

**Symptom:** Some OCC Client windows will not automatically show updates made in other windows. For example, if you open a Server Explorer and make changes to an application configuration such as adding a new configuration template, this new configuration template will not appear in the main application window unless you press F5 to refresh the main application window.

**Workaround:** Press F5 to see any changes made when you have multiple windows open in the OCC Client.

**Bug ID:** 31736

**Description:** Selecting objects in the OCC Client rapidly using up or down arrow keys can cause slow display in the Preview pane.

**Platform:** Independent

**Subsystem:** OCC Client

**Symptom:** If you select an object inside the OCC Client, for example, a server from Servers | All Managed Servers, and then select a Server in the Content pane and use your up and down arrow keys to select servers, the Preview pane may not display the server information as quickly as you select servers. This depends on how quickly you move from server to server.

The reason for the slow down is that each new selected item will change the contents of the preview pane. The speed of the loading depends on the complexity of the UI and the size of the data object(s) being retrieved from the cache or server.

**Workaround:** If you do not see information in the Preview pane when you are quickly selecting an object using the up or down arrow keys, wait a few moments for the information to display. Or, you can minimize the Preview pane (the down arrow button in the right side of the header) so that the data will not load as the next item is selected.

**Bug ID:** 31828

**Description:** A Non-Compliant error displays when the reconcile processes will not install a patch that is superseded by a patch that is already installed. Since you can attach multiple patch policies to a single server, if a superseded patch is in one policy and the superseding patch is in another policy, it is possible for that server to never be Compliant.

**Subsystem:** OCC Client – Patch Management for Windows

**Platform:** Windows

**Symptom:** Patch A supersedes patch B. Policy PA includes patch A and policy PB includes patch B. Both policies are attached to a managed server. If patch A is already installed on that server, the reconcile process will not install patch B because patch A supersedes patch B. The patch compliance information will display patch B as Non-Compliant because it is not installed.

**Workaround:** Install patch B separately, by using the Install Patch task window. The Reconcile Patches task window will not install a superseded patch if a superseding patch is already installed.

**Bug ID**: 31833

**Description**: An error occurs when you download HTML pages instead of patch binaries from the vendor. Some download URLs provided by Microsoft point to HTML pages and not to patch binaries. The OCC Client and the populate-opsware-update-library script check to ensure that files that are downloaded are not HTML pages.

**Subsystem**: OCC Client – Patch Management for Windows

**Platform**: Windows

**Symptom**: If you downloaded HTML pages instead of the patch binaries from Microsoft, an error occurs.

**Workaround**: In the Import from Vendor window in the OCC Client, enter a valid URL to override the default URL.

**Bug ID:** 31960

**Description:** Post-error scripts will not be executed during a push if any failure occurs up to and including the pre-install scripts.

**Platform:** Independent

**Subsystem:** OCC Client-Application Configuration

**Symptom:** If during an Application Configuration push any failure occurs up and including to the pre-install script, then post-error scripts will not be executed.

**Workaround:** None

**Bug ID:** 31962

**Description:** Packaging server information is no longer available when you upgrade a core from Opsware SAS 5.3 to Opsware SAS 5.5.

**Subsystem:** OCC Client – Visual Packager

**Platform:** Independent

**Symptom:** To create packages using the Visual Packager feature, you will need to set a packaging server for each type of operating system for the packages you plan to create.

After you perform a Rolling Mesh upgrade to upgrade the multimaster mesh from Opsware SAS 5.3 to Opsware SAS 5.5, the information about the packaging server is no longer available from the OCC Client.

**Workaround:**. None. After the upgrade, reset the preferences for the packaging server.

**Bug ID:** 32005

**Description:** The date format used for the Start Time on the Schedule Compliance Scan window is different than the Short Date Format used in User Preferences. The Start Time for a patch compliance scan is based on 24 hours and specifies the hour, minute, second, and AM or PM. The Short Date Format is based on 12 hours and specifies the day, month, and year.

**Subsystem:** OCC Client – Patch Management for Windows

**Platform:** Windows

**Symptom:** When you compare the Start Time on the Schedule Compliance Scan window with the Short Date Format in User Preferences, you will see two different date formats used.

**Workaround:** None

**Bug ID:** 32008

**Description:** Microsoft often releases several versions of a patch that have the same QNumber. If you have these types of patches in a policy, the reconcile patches operation will display an error indicating that one of these patches has not been downloaded.

**Subsystem:** OCC Client – Patch Management for Windows

**Platform:** Windows

**Symptom:** You added hotfixes to a patch policy by their QNumber. Microsoft released several versions of these hotfixes for the same QNumber, where one version is a patch for Windows 2000 Service Pack 3 servers and another version is a patch for Windows 2000 Service Pack 4 servers. Therefore, when you added these patches to the policy, you added both versions of the hotfix. When you try to install the patches by using the reconcile patches operation, an error displays indicating that one of these patches has not been downloaded.

**Workaround:** When you add patches to policies, make sure that all versions of the same QNumber are imported. Use the populate-opsware-update-library script frequently to make sure that your Software Repository is up to date with the latest patches.

**Bug ID:** 32026

**Description:** Patch policies may not display if certain user permissions were changed and the OCC Client has cached previous permissions.

**Subsystem:** OCC Client – Patch Management for Windows

**Platform:** Windows

**Symptom:** You cannot view patch policies because the Allow Install or Allow Uninstall Patch permissions were changed (from No to Yes) or the Manage Patch Policy permission was changed from None, and either:

1) The OCC Client was not restarted.

Or

2) The local user cache is not deleted and the OCC Client was restarted.
(When the Allow Install Patch permission is set to Yes, then the Manage Patch and Manage Patch Policy permissions are automatically set to Read.)

**Workaround:**

1) Close the OCC Client.

2) Clear the local user cache.

3) Restart the OCC Client so that all permission changes are applied.

**Bug ID:** 32112

**Description:** You cannot install the following Exchange and DirectShow patches as part of a patch policy because their GUIDs are not unique. The Exchange patches are Q870540, Q894549, Q894689, and Q906780. These patches are special cases where each QNumber has multiple versions, where each version applies to a different country. For example, there are five versions of Q870540 (English, French, German, Italian, and Japanese). Since Patch Management currently supports only English locale, be sure to select the English version of Q870540 when you install it. The DirectShow patch that does not have a unique identifier is Q904706.

**Platform:** Windows

**Subsystem:** OCC Client – Patch Management for Windows

**Symptom:** If you add these patches to a policy and then try to install them, they will not be installed.

**Workaround:** Use the Install Patch task window to install these Exchange and DirectShow patches separately (independent of a policy). Do not use the Reconcile Patches task window to install these patches.

**Bug ID:** 32117

**Description:** Use the directional arrows to enter a valid date in the “Run Task at” text box in the Reconcile Patches task window, in the Install Patch task window, and in the Uninstall Patch task window.

**Subsystem:** OCC Client – Patch Management for Windows

**Platform:** Windows

**Symptom:** You are unable to type in some of the date segments in the “Run Task at” text box; however, when you use the directional arrows, you are able to enter all date information. When you enter some date segments, you will see that the other segments are automatically adjusted. You cannot enter a year that exceeds 10 years from now.

**Workaround:** None.

**Bug ID:** 32154

**Description:** An out of memory error occurred when trying to import the Windows 2003 Service Pack 1 from the vendor.

**Subsystem:** OCC Client – Patch Management for Windows

**Platform:** Windows

**Symptom:** In the Import from Vendor window, a java.lang.OutOfMemoryError displayed when you tried to import the Windows 2003 Service Pack 1 from the vendor.

**Workaround:** To import patches that are larger than 20MB, use the populate-opsware-update-library script.

**Bug ID:** 32213

**Description:** You cannot schedule a patch reconcile, a patch install, or a patch uninstall job to run more than 10 years from now.

**Subsystem:** OCC Client – Patch Management for Windows

**Platform:** Windows

**Symptom:** When you use the directional arrows to enter the year in the “Run Task at” text box in the Scheduling step in the Reconcile Patches task window, in the Install

Patch task window, or in the Uninstall Patch task window, you cannot enter a year that exceeds 10 years from now.

**Workaround:** None.

**Bug ID:** 32277

**Description:** The checkmark in the Installed column in the patches pane for a selected server does not immediately display after the patch installation.

**Subsystem:** OCC Client – Patch Management for Windows

**Platform:** Windows

**Symptom:** After you successfully install a patch, the checkmark in the Installed column in the patches pane will not immediately display.

**Workaround:** Refresh the patches window display to see the checkmark in the Installed column.

**Bug ID:** 32376

**Description:** You cannot copy a patch policy exception to a server that does not exactly match the operating system version of the patch.

**Subsystem:** OCC Client – Patch Management for Windows

**Platform:** Windows

**Symptom:** When you try to copy a patch policy exception to a server or server group that is not using the same operating system version of the patch, the copy operation will fail.

**Workaround:** None.

**Bug ID:** 32415

**Description:** Email notifications are not sent when the install, uninstall, or reconcile processes fail due to pre-install or pre-uninstall scripts that failed to run.

**Subsystem:** OCC Client – Patch Management for Windows

**Platform:** Windows

**Symptom:** You tried to install a patch where the pre-install or pre-uninstall script failed. No email notification was sent.

**Workaround:** None.

**Bug ID:** 32467

**Description:** You cannot use the OCC Client to uninstall a patch that was installed with the OCC application node.

**Subsystem:** OCC Client – Patch Management for Windows

**Platform:** Windows

**Symptom:** You created an application node and added a patch to it. In the OCC, you installed the application node on a managed server. In the OCC, you removed the application node from the server. In the OCC Client, you tried to uninstall it with the Uninstall Patch task window and received an error explaining that "This patch cannot be uninstalled because it is referenced by another part of the model."

**Workaround:** Use the OCC Client for all Windows patching.

**Bug ID:** 32473

**Description:** You cannot remove a patch that has a status of Deprecated from a patch policy.

**Subsystem:** OCC Client – Patch Management for Windows

**Platform:** Windows

**Symptom:** Select a patch that is already in a policy and change the status of the patch from Available to Deprecated. Open the policy, select the deprecated patch, and then try to remove it from the policy. The Remove Patch from Policy window does not display the deprecated patch.

**Workaround:** Change the patch status from Deprecated to Available and then remove it from the policy. Change the patch status back to Deprecated.

**Bug ID:** 32520

**Description:** A pre/post install, a pre/post uninstall, and a pre/post download script will fail if it exceeds the one minute timeout.

**Subsystem:** OCC Client – Patch Management for Windows

**Platform:** Windows

**Symptom:** You specified a pre/post install, a pre/post uninstall, or a pre/post download script for a patch reconcile, a patch install, or a patch uninstall and it failed because it exceeded the one minute timeout.

**Workaround:** None.

**Bug ID:** 32546

**Description:** You cannot import Windows NT4.0 patches that have an ftp URL by using the Import from Vendor window.

**Platform:** Windows

**Subsystem:** OCC Client – Patch Management for Windows

**Symptom:** When you try to import a Windows NT4.0 patch that has an ftp URL, the process suspends.

**Workaround:** Import Windows NT4.0 patches that have ftp URLs by using the populate-opsware-update-library script.

**Bug ID:** 32588

**Description:** A patch or patch policy is temporarily not displayed in the list when you click Cancel or the X (in the title bar) in the Delete Patches or Delete Patch Policies confirmation dialog.

**Subsystem:** OCC Client – Patch Management for Windows

Platform: Windows

**Symptom:** You selected a patch or a patch policy and launched the Delete Patch or Delete Patch Policy action. You clicked Cancel or the X (in the title bar) to cancel the delete operation. Even though you canceled the delete, the patch or patch policy that you selected is no longer displayed in the list.

**Workaround:** From the Navigation pane, select a different Windows operating system in the Software Library. Then select the Windows operating system where you cancelled the delete to refresh the list of patches or patch policies. You will see the patch or patch policy that you canceled the delete operation for in the refreshed list.

**Bug ID:** 32599

**Description:** In the Patches and All Patches views, a patch is displayed as grayed out when Patch Management cannot determine whether the version of the patch that is installed is the same as the version of the patch that is in the Software Repository. This occurs when the GUID identifier is not provided or is the same for both versions of the patch.

**Subsystem:** OCC Client – Patch Management for Windows

**Platform:** Windows

**Symptom:** A patch install appears successful; however, after verification, Opsware determined that the patch was not actually installed. When you view All Patches, you see two patches displayed: one is grayed out and shown as installed-not-by-opsware and one is not installed.

**Workaround:** None.

**Bug ID:** 32622

**Description:** In the Job Progress window, the Patch Install status may display “Completed” even when the patch is still being installed.

**Platform:** Windows

**Subsystem:** OCC Client – Patch Management for Windows

**Symptom:** When you click Start Job in the Install Patch task window or in the Reconcile Patches task window, the Install Status in the Job Progress window displays “Completed” even when the patch is still being installed (as indicated by “Installing” in the Status column).

**Workaround:** In cases where the Install Status displays “Complete” and patches in the Status column display “Installing” or “Pending”, refer to the Status column for the correct status.

**Bug ID:** 32625

**Description:** If you have already imported a Microsoft Malicious Software Removal tool, such as Q890830, into your Opsware core prior to upgrading to Opsware SAS 5.5, care should be taken when using this package.

**Platform:** Windows

**Subsystem:** OCC Client – Patch Management for Windows

**Symptom:** You tried to install Q890830 with the Install Patch task window and the job failed.

**Workaround:** The Malicious Software Removal Tool is not officially supported; however, if you are upgrading from a previous version of Opsware SAS and have already imported the package, care should be taken when using this package with the Patch Management for Windows feature. Since there are different versions of this package, all with the same QNumber, do not add this package to a patch policy. (Microsoft typically releases a new version of this package each month.) If you use the Install Patch task window to install this package, be sure to specify the correct command-line arguments to ensure a silent install and that all server reboots are suppressed.

**Bug ID:** 31617

**Description:** The MBSA 2.0 import is not honoring the selected list of Microsoft products that you want to track patches for.

**Platform:** Windows

**Subsystem:** OCC Client – Patch Management for Windows

**Symptom:** When you set Windows 2003 as the only product to import from MBSA 2.0, all Windows 2003 patches and about ten Windows 2000 patches are imported.

**Workaround:** None.

**Bug ID:** 32572

**Description:** Unable to create packages for multiple Snapshots or Audit Results.

**Platform:** Platform Independent

**Subsystem:** OCC Client – Server Compliance

**Symptom:** From the OCC Client you are able to select the Create Package option from the menu when you select multiple Snapshots or Audit Results.

But the Create Package operation is carried out for the first selected snapshot or audit result.

**Workaround:** None. You can create a package for only one Snapshot or Audit Result at a time.

**Bug ID:** 32658

**Description:** Removing the only object from a Server Object category (folder) does not remove the Server Object category (folder) from the selection criteria.

**Platform:** Platform Independent

**Subsystem:** OCC Client – Server Compliance

**Symptom:** When a Server Object category (folder) contains a single object and if you remove the object, then the Server Object category (folder) is not removed from the selection criteria. As a result if you run a job on the Server Object category (folder), the job will fail.

**Workaround:** None. After removing the last object in a Server Object category (folder), remove the empty Sever Object category (folder) if it still exists from the selection criteria before running a job.

**Bug ID:** 32701

**Description:** When a patch in a server group has an always install exception and when that same patch is in another server group has a never install exception, the wrong patch exception icon (always install) might be displayed in the Exception column in the Server Browser.

**Platform:** Windows

**Subsystem:** OCC Client – Patch Management for Windows

**Symptom:** Your server belongs to server group1 and server group2. In server group1, the exception type for a patch is always install. In server group 2, the exception type for the same patch is never install. In the server browser, the Exception column displays an always install icon, which is incorrect. The Exception column is supposed to display the never install icon.

**Workaround:** None. Even though the incorrect exception icon (always install) might be displayed, Opsware SAS correctly determines whether to install the patch in a patch reconcile operation and when calculating patch compliance. When a server belongs to more than one server group, a never install exception takes precedence over an always install exception.

**Bug ID:** 32706

**Description:** Operations in Patch Management for Windows should not be performed on server groups called Public Groups or Private Groups. This release does not support patching operations on these two server groups.

**Platform:** Windows

**Subsystem:** OCC Client – Patch Management for Windows

**Symptom:** In the OCC Client, if you attempt to run any patch management operation, such as attaching patch policies and reconciling patches on server groups called Public Groups or Private Groups, the following behavior is observed:

- Install and uninstall operations will act on all servers that are in any of the subordinate groups, recursively.
- Reconcile patch operations may result in installing patches in a patch policy that is not attached to those servers.

**Workaround:** Do not model information on these Public Groups or Private Groups, such as attaching patch policies. In addition, do not attempt to perform operations on these groups, such as reconciling patches.

**Bug ID:** 32732

**Description:** An error is displayed when you create snapshots with invalid metabase paths.

**Platform:** Independent

**Subsystem:** OCC Client – Server Compliance

**Symptom:** When you create a snapshot using invalid metabase paths, the Job is completed with an error. Also in the snapshot browser only summary information is displayed for that snapshot.

This occurs when the snapshot contains invalid metabase paths and can occur in the following scenarios:

- When you have multiple servers in a selection criteria and you choose a metabase path that is only present on one
- When you select metabase path and later delete it.

**Workaround:** None. Use only valid matabase paths while creating snapshots.

**Bug ID:** 32734

**Description:** Perform Audit may fail with xml.SAXPParseException.

**Platform:** Independent

**Subsystem:** OCC Client – Server Compliance

**Symptom:** Sometimes when you perform an Audit from a snapshot, it might fail with xml.SAXPParseException. This occurs when the snapshot contains nonexistent COM objects and can occur in the following scenarios:

- When you have multiple servers in a selection criteria and you choose a COM object that is only present on one
- When you select a Com object and later delete it.

**Workaround:** None. Use valid COM objects to create snapshots.

## Packages

**Bug ID:** 27021

**Description:** Installation of a latest version of a package does not remove the old version of the package on Windows 2003.

**Platform:** Windows

**Subsystem:** Packages

**Symptom:** When you install the latest version of a package in a Windows server, the older version of the package is not uninstalled automatically.

**Workaround:** None. Even though the older version of the package is not uninstalled, the latest version is used by the Windows server.

## Patch Management

**Bug ID:** 22960

**Description:** The browser stops responding when you upload a patch from the Microsoft Patch Database in the Opsware Command Center.

**Platform:** Windows

**Subsystem:** Patches

**Symptom:** When you upload a patch from the Microsoft Patch Database using the Patch Preference tab in the Opsware Command Center, the browser appears to stop responding. Even though the browser stops responding, the patch is uploaded successfully.

**Workaround:** None.

**Bug ID:** 28871

**Description:** Opsware SAS 5.2 does not support MBSA version 2.0 for patch management.

**Platform:** Windows

**Subsystem:** Patch Management

**Symptom:** During the installation of Opsware SAS, you are required to upload the mbsacli.exe patch utility, which is shipped with the Microsoft Base Security Analyzer (MBSA version 1.2.1). Although MBSA version 2.0 is available from Microsoft, Opsware SAS 5.2 does not support MBSA version 2.0 for patch management.

**Workaround:** None. Do not upload MBSA version 2.0, since Opsware does not support MBSA version 2.0 for patch management.

## Satellite

**Bug ID:** 27982

**Description:** `wordbot.unableToCacheFile` error in a Satellite with multiple Software Repository Caches.

**Platform:** Platform Independent

**Subsystem:** Software Repository Cache

**Symptom:** If you have a Satellite that contains multiple Software Repository Caches, and the Satellite is configured for manual updates, you may get the error wordbot.unableToCache file when performing operations that retrieve files from the Cache (for example, when installing software on a server in the affected Satellite). This error occurs when not all of the Software Repository Caches have a copy of every file.

**Workaround**: When applying manual updates in a Satellite with multiple Software Repository Caches, apply the update to each Software Repository Cache in the Satellite.

## Software Provisioning

**Bug ID:** 26956

**Description:** A template which is Customer Independent should not be assigned to a customer.

**Platform:** Platform Independent

**Subsystem:** Templates

**Symptom:** In the Opsware Command Center, when you create a template you can select the Operating System version and the Customer for that template. You can also have the server that you apply the template to automatically assign to the customer associated with the template.

When you create a template that is Customer Independent, select the No option in the Assign Customer field.

**Workaround:** None.

## Web Services Data Access Engine

**Bug ID:** 28568

**Description:** Error occurs in the Web Services Data Access Engine log file when you access the Manage Sever page.

**Platform:** Platform Independent

**Subsystem:** Web Services Data Access Engine

**Symptom:** In the Opsware Command Center when you access the Manage Sever page for the first time, a benign exception occurs in the Web Services Data Access Engine log file.

**Workaround:** None.

## Miscellaneous

**Bug ID:** 28809

**Description:** Patch uninstallation fails with errors.

**Subsystem:** Reconcile

**Platform:** Solaris

**Symptom:** In Solaris 10, when you uninstall any patch, the uninstallation fails with the following error:

```
Backout of another patch is in progress try after some
time.
```

This error can occur because the server you are attempting to uninstall a patch from does not have the Solaris 10 patch 119254-06 installed on it.

**Workaround:** Install patch 119254-06 for Solaris 10. Without patch 119254-06, uninstalling patches on Solaris 10 servers will experience intermittent failures and display an error on the managed server.

# Known Problems, Restrictions, and Workarounds in Opsware SAS 5.5.1

This section describes the workarounds to known problems in Opsware SAS 5.5.1.

## OS Provisioning

**Bug ID:** 32945

**Description:** OS Re-provisioning fails with Red Hat Linux 3 ES/AS/WS IA64 on HP RX1600 Itanium server.

**Subsystem:** OS Provisioning

**Platform:** LINUX

**Symptom:** When you try to re-provision a Red Hat Linux 3 ES/AS/WS IA64 on HP RX1600 Itanium server, the operation fails with a build script error.

**Workaround:** To re-provision a Red Hat Linux 3 ES IA64 on HP RX1600 Itanium server, you must first deactivate the server. After deactivating the server, provision the OS on the server.

See “Support for OS Provisioning for Red Hat Linux 3 AS/ES/WS on Itanium” in the Opsware SAS 5.5.1 Release Notes for more information.

See "OS Provisioning Process" in Opsware SAS 5 User's Guide for information on the OS Provisioning Process.

## Opsware Command Center Client

**Bug ID:** 32863

**Description:** Even though one version of a patch is already installed on a server, it is possible that the vendor will recommend that another version of the same patch should be installed. In this case, Patch Management indicates only that the patch is recommended. Patch Management does not indicate that the patch is both (already) installed *and* recommended.

**Platform:** Windows

**Subsystem:** OCC Client – Patch Management for Windows

**Symptom:** A version of a patch is already installed on a server and there is no black check mark in the Installed column in the All Managed Servers preview pane. After you install a different version of the patch (because the patch was recommended by the vendor), Patch Management reports that two versions of the patch are now installed.

**Workaround**: None.

**Bug ID:** 32907

**Description:** The uninstall patch process failed with an exit code -3, which means that the Agent was unable to find the uninstaller for the selected patch.

**Platform:** Windows

**Subsystem:** OCC Client – Patch Management for Windows

**Symptom:** When you tried to uninstall a patch that was installed with Patch Management and the Agent could not find the uninstaller for that patch, the uninstall process failed. (A black check mark in the Installed column in the All Managed Servers preview pane indicates that the patch was installed by Opsware.)

**Workaround**: Use the Windows Add or Remove Programs tool to uninstall a patch from a server.

**Bug ID:** 32912

**Description:** The email notification for an install patch, uninstall patch, or reconcile patches job indicates only whether a patch was installed or uninstalled. Email notification does not report on whether pre/post install scripts or pre/post uninstall scripts successfully ran. For example, an email notification that indicates a patch install as “Status: Completed” will correspond to a Job Progress summary that indicates “Completed With Errors”. In this case, all patches in the job were installed or uninstalled successfully, but there may have been an error when running a job script.

Platform: Windows

**Subsystem:** OCC Client – Patch Management for Windows

**Symptom:** The Job Progress summary in the Install Patch task window, Uninstall Patch task window, or Reconcile Patches task window shows the Install Status or Uninstall Status as “Completed With Errors” and the corresponding email notification shows “Status: Completed”, which indicates that the patch was successfully installed.

**Workaround:** To view detailed information about the status of these types of jobs, such as which patches were installed and whether a script successfully ran, open the job in the Job Logs window and then select a row in the table in the Job Progress window.

**Bug ID:** 32935

**Description:** Global Shell audit directory has read-any access.

**Subsystem:** OCC Client - Global Shell

**Platform:** Independent

**Symptom:** The Global Shell audit directory can be read by any Unix user with a login to the core server. It can also be read from within a Global Shell session if the user have file system permissions to the core server.

**Workaround:** Enter the following command:

```
chmod 700 /var/opt/OPSWmnt/audit/streams/<server>
```

**Bug ID:** 32944

**Description:** Possible to bypass Global Shell auditing and launch GlobalShell permission.

**Subsystem:** OCC Client - Global Shell

**Platform**: Independent

**Symptom:** A user with a Unix login to the hub server can bypass the Global Shell user interface and access the OGFS directly.

**Workaround:** Do not allow users to have Unix logins to the hub server.

**Bug ID:** 32951

**Description:** When you perform reconcile patches on a server group that contains only servers that are running a Windows NT4.0, Windows 2000 RTM (no Service Pack), Windows 2000 Service Pack 1, or Windows 2000 Service Pack 2 operating system, no patches are installed and a permissions error displays.

**Platform:** Windows

**Subsystem:** OCC Client – Patch Management for Windows

**Symptom:** No patches are installed and a permissions error displays when you perform reconcile patches on a server group that contains only servers that are running a Windows NT4.0, Windows 2000 RTM (no Service Pack), Windows 2000 Service Pack 1, or Windows 2000 Service Pack 2 operating system.

**Workaround:** The reconcile patches process requires that at least one of the servers in the server group is running Opsware Agent 5.5 and a Windows 2000 Service Pack 3 (or higher) operating system or a Windows 2003 operating system that uses MBSA2.0. You cannot use the reconcile patches process if all servers in the server group are running a Windows NT4.0 operating system, a Windows 2000 RTM (no service pack), Service Pack 1, or Service Pack 2.

# What’s New in Opsware SAS 5.5.2

## New Operating System Support

Opsware SAS 5.5.2 supports the Windows 2003 64 bit operating system for Opsware Agents.

Opsware SAS 5.5.2 provides full support for this operating system, including the ability to manage servers running Windows 2003 64 bit, the ability to install Windows 2003 64 bit on bare metal servers, and the ability to run DCI reports for Windows 2003 64-bit servers.

## RIS vs. Unattended Setup for Windows 2003 64-bit OS Provisioning

In Opsware SAS 5.5.2, the implementation for Windows 2003 64-bit OS provisioning emulates a RIS installation. However, Opsware SAS might install the Windows 2003 64-bit OS slightly differently that Window Unattended Installation because of the way that parameters are interpreted in the unattend.txt file.

To achieve RIS emulation, Opsware SAS 5.5.2 minimizes these differences by automatically adding the necessary parameters to the unattend.txt file during OS installation.

## OS Provisioning Requirements for Windows 2003 64-bit

Before you use the OS Provisioning feature to install Windows 2003 64-bit on a bare metal server, you must meet the following requirements:

- When installing Windows 2003 with SP1 slipstreamed in, the Windows Firewall is installed and activated by default.

You *must* disable the Windows Firewall by adding the following parameters to the unattend.txt file that you supply for the OS Definition in the Opsware Command Center:

```
[WindowsFirewall]
Profiles = WindowsFirewall.TurnOffFirewall

[WindowsFirewall.TurnOffFirewall]
Mode = 0
```

- If you are running a server with an EMS console (such as console redirection to a serial port), the Windows 2003 installer will halt an unattended installation and wait for console input.

  To install the OS on a server with an EMS console, add the following parameter to the unattend.txt file:

  ```
  [Unattended]
  EMSSkipUnattendProcessing = 1
  ```

- If you have an EMS console and your unattend.txt file includes the following parameter and value, you cannot use a blank Administrator password:

  ```
  [GuiUnattended]
  AdminPassword=*
  ```

  To allow the OS installation to proceed with a blank Administrator password, add the following parameter to the unattend.txt file:

  ```
  EMSBlankPassword = Yes
  ```

- Instead of a single directory called i386 in the root of the media, the directory structure for the Windows 2003 64-bit media has two main directories:

  ```
  amd64
  i386
  ```

  You must copy both these directories onto the Opsware SAS Media Server running in your Opsware SAS core.

Because of the change to the OS media directory structure in this release, the MRL for Windows 2003 64-bit no longer terminates in the i386 directory; the MRL terminates one directory earlier.

Opsware SAS 5.5.1 and earlier releases:

```
smb://media/share/win2003/i386
```

Opsware SAS 5.5.2:

```
smb://media/share/win2003.x64
```

***NOTE*** *If you specify the wrong MRL convention when using import_media, Opsware SAS 5.5.2 displays an error that your media is invalid.*

- The Windows 2003 64-bit media contains long filenames that do not conform to the DOS 8.3 character convention; therefore, you cannot use the DOS-based pre-boot environment to copy the files directly from the network share to the server that you are installing the OS on.

To work around this situation, you must tar the following directories in the media directory on the Opsware SAS Media Server:

```
i386
amd64
```

Create two tarfiles in the media root directory:

`i386.tar` → containing the i386 directory contents

`amd64.tar` → containing the amd64.tar directory contents

To create these tar files, perform the following steps.

***NOTE You must create the tar files before running import_media or it will display an error message directing you to create the tar files.***

1. Change directories to the root directory of the Opsware SAS Media Server; for example:

```
cd /media/windows/win2003.x64
```

2. Run the following commands to create the tar files:

```
tar cf i386.tar i386
tar cf amd64.tar amd64
chmod a+r i386.tar amd64.tar
```

When creating the tar files for these directories, make sure the files are readable by all.

## Documentation for Opsware SAS 5.5.2

This release comes with the following documentation:

- *Opsware SAS 5.5.2 Release Notes*
- *Planning Deployments for Opsware SAS 5*
- *Opsware SAS 5 Deployment and  Installation Guide*
- *Opsware SAS 5  Configuration Guide*
- *Opsware SAS 5  Administration Guide*
- *Opsware SAS 5  User's Guide*
- *Opsware Data Center Intelligence 1.8 Administrator's Guide*
- *Opsware SAS DCML Exchange Tool 2.5 Reference Guide*
- *Opsware SAS Web Services API 2.2 Guide*
- *Opsware SAS Intelligent Software Module (ISM) Development Kit 2.0 Guide*
- *OCLI 2.0 Reference Guide*
- *CML Tutorial for Opsware SAS 5*

The Opsware SAS documentation is available online at https://download.opsware.com/kb/category.jspa?categoryID=20

Ask your Opsware administrator for the user name and password to access the site.

# Supported Installations for 5.5.2

The Opsware SAS 5.5.2 release supports the following installations:

- New installations of a standalone core
- New installations of a multimaster core
- New installations of a Satellite
- Upgrade from Opsware SAS 5.5.1 to Opsware SAS 5.5.2.

## Upgrading to Opsware SAS 5.5.2

In Opsware SAS 5.5.2, you can upgrade your Opsware installation to this release.

Opsware SAS 5.5.2 supports the following upgrade paths:

- Upgrading a Standalone Core from 5.5.1 to 5.5.2
- Upgrading a Multimaster Mesh from 5.5.1 to 5.5.2
- Upgrading an Opsware Satellite from 5.5.1 to 5.5.2

For information about upgrading to Opsware SAS 5.5.2, see the *Opsware SAS 5.5 Upgrade Guide*, or contact your Opsware Support Representative:

# What's Fixed in Opsware SAS 5.5.2

The following bugs are fixed in Opsware SAS 5.5.2.

## Patch Management

**Bug ID:** 127619

**Description:** When uploading a self-extracting executable Hotfix that did not contain ieupdate.exe, updated.exe, or hotfix.exe, Opsware SAS stored the value for __OPSW_hotfix_date as 0 in the Hotfix meta-information. When the reboot_on_install attribute for the Hotfix was set to 1, the 0 value for __OPSW_hotfix_date caused the server to immediately reboot when the Hotfix was installed.

**Subsystem:** Patch Management

Platform: Windows

**Resolution:** Fixed. The data stored for __OPSW_hotfix_date is now accurately stored as non-zero for Hotfixes that do not contain update.exe, ieupdate.exe or hotfix.exe.

**Bug ID:** 132546

**Description:** When importing a patch that has an FTP URL, the Opsware SAS client hung.

**Subsystem:** Patch Management

**Platform:** Windows NT 4.0

**Resolution:** Fixed. When a patch has an FTP URL, the Import button in The SAS Client dialog box is disabled. If you are importing multiple patches and any of them have an FTP URL, the Import button is disabled in the dialog box.

**Bug ID:** 132898

**Description:** When uploading a PTF, Opsware SAS processed the APAR listings encoded within the PTF and generated virtual APAR packages. If the PTF had incorrect APAR listings, using the Opsware SAS DCML Exchange Tool (DET) to import the PTF into another Opsware SAS core caused the DET import to fail.

**Subsystem:** Patch Management

Platform: AIX

**Resolution:** Fixed. Importing a PTF into another SAS core by using DET works correctly when the PTF contains inconsistent APAR listings.

**Bug ID:** 133114

**Description:** When installing a patch with the OCC Client, the results window displays a null value if the server name or patch name are not stored in the OCC Client cache.

**Subsystem:** Patch Management

Platform: Windows

**Resolution:** Fixed. The OCC Client retrieves the correct server or patch name even if it is not loaded in the cache yet.

**Bug ID:** 134589

**Description:** The timeout value in the Opsware Command Engine script opsware.patch_compliance was set to 3 minutes. If a job timed out, the OCC Client did not indicate that the job timed out and the server alternated displaying status messages of “scan required” and “scanning.”

**Subsystem:** Patch Management

Platform: Windows

**Resolution:** Fixed. The timeout value in the opsware.patch_compliance script is 900 seconds.

## Opsware SAS Web Services 2.2 API

**Bug ID:** 133031

**Description:** Using the createUser method in the Opsware SAS Web Services 2.2 API via the Perl binding created a SAS user account that had incomplete user data and it altered the data for the Opsware admin account.

**Subsystem:** Opsware User and Groups Administration

**Platform:** Independent

**Resolution:** Fixed. In the previous release, Opsware SAS used an incorrect set of APIs for setting user attributes. In Opsware SAS 5.5.2, creating SAS users by using the SAS WS API createUser method correctly creates the SAS user account. Additionally, it sets the user’s full name to a concatenation of the first name, a space, and the last name because the Opsware Command Center (web) UI will not display users that are missing a last name and the createUser method cannot receive user input for the full name of the new user.

## OS Provisioning

**Bug ID:** 133770

**Description:** Booting a new Windows server (for example, by booting the server into DOS), could result in the server not appearing in the Server Pool in the Opsware Command Center.

**Subsystem:** OS Provisioning in the Opsware Command Center

Platform: Windows

**Resolution:** Fixed. An exception on the Server Pool page was causing the server not to be displayed in the Server Pool list even though the server successfully booted into the Server Pool.

## OCC Client UI

**Bug ID:** 133251

**Description:** The chunk sizes used by the OCC Client were not optimized for performance.

**Subsystem:** OCC Client UI

**Platform:** Independent

**Resolution:** Fixed. The load chunk size for the server cache and the patch cache were changed. When Opsware SAS contains data for a large number of servers and patches, the initial cache load is optimized for client/server performance.

**Bug ID:** 133323

**Description:** When the OCC Client encountered an exception when reloading cache data, it deleted all cache files and reloaded the cache data.

**Subsystem:** OCC Client UI

**Platform:** Independent

**Resolution:** Fixed. The OCC Client uses an individual timestamp for each cache file to prevent reloading cache files that successfully loaded. The next time the cache automatically refreshes, only the cache files that failed to load will be reloaded in full.

**Bug ID:** 133694

**Description:** Expanding the server group nodes while the server group cache was loading created a synchronization error and the OCC Client UI could stop responding. (Simultaneous operations were attempting to access the shared data cache.)

**Subsystem:** OCC Client UI

**Platform:** Independent

**Resolution:** Fixed.

**Bug ID:** 127590

**Description:** After installing an Opsware Agent on a server running Windows NT 4.0 Terminal Server Edition, the server's C drive is not accessible through the OGFS.

**Subsystem:** Server Explorer

**Platform:** Windows

**Resolution:** Fixed.

## Opsware Agent Discovery and Deployment (ODAD)

**Bug ID:** 134402

**Description:** When using the ODAD in the OCC Client to install an Opsware Agent on a server, the Opsware Agent running on the Global File System Server component in the Opsware core logged the parameters you entered for the ODAD in ACSII text in the cogbot.err file. These parameters included the root password for the server that the Opsware Agent was being installed on.

**Subsystem:** Opsware Agent Discovery and Deployment

**Platform:** Independent

**Resolution:** Fixed. Passwords used as parameters for ODAD are not written to the cogbot.err file on the server running the Global File System Server component. Passwords are written to the cogbot.log file with the following text:

```
"---hidden---"
```

## ISM Development Kit (IDK)

**Bug ID:** 134108

**Description:** When unpacking the latest DCI .ism file by using the - -unpack comment, the IDK returns the following error message:

error: "ISM  'CIPackage_en-1.8' does not exist in this directory"

**Subsystem:** IDK – DCI .ism file

**Platform:** Windows

**Resolution:** Fixed

## DCML Exchange Tool (DET)

**Bug ID:** 134855

**Description:** The previous release of DET did not export a checksum for packages. In Opsware SAS 5.5, the DET writes a checksum for all packages. This functional difference caused DET to download all packages, greatly increasing the duration of the export operation.

Subsystem: DET

**Platform:** Independent

**Resolution:** Fixed. When DET calculates a digest for a package, it skips the checksum and the package appears unchanged and is not downloaded. If the package did in fact change, the change is reflected in the modification date and version of the object.

## Miscellaneous

**Bug ID:** 132955

**Description:** When clicking the link for another user's job in the SAS Client UI, Opsware SAS opened the Opsware Command Center (web) UI and displayed the Home page. It did not display the page for the job selected.

Subsystem: Jobs

**Platform:** Independent

**Resolution:** When clicking the link for another SAS user's job, the Job page appears if you have the View All Jobs permission in Opsware SAS. When clicking the link for another SAS user's scheduled job, the Job page appears if you have the Edit All Jobs permission. If you have only the View All Jobs permission, Opsware SAS displays a read-only view of the Job page for scheduled jobs.

**Bug ID:** 132963

**Description:** Opsware SAS did not use the correct OpenSSL libraries for m2crypto.

**Subsystem:** Opsware SAS core

**Platform:** Red Hat Linux AS 3

**Resolution:** Fixed. Opsware SAS does not use the system libraries. Opsware SAS uses libraries developed by Opsware Inc. to compile the m2crypto included in the Opsware SAS distribution.

# Known Problems, Restrictions, and Workarounds in Opsware SAS 5.5.2

This section describes the workarounds to known problems in Opsware SAS 5.5.2.

**Bug ID:** 134379

**Description:** User directory gets created with a corrupted name.

**Subsystem:** Server Management

**Platform:** Windows

**Symptom:**

- Create a user on the server. Note that a profile for the user is not created yet in the "Document and Settings" directory.
- Do not log into the server as the user.
- Use Opsware SAS to perform an action on the server; for example, run an Opsware SAS DSE script as this user.
- Log into the server and go to the "Document and Settings" directory. The directory name for the user profile was created with corrupted characters.

If the directory already existed (for example, the user had logged onto the server by using the console or remote desktop), the directory name is not changed.

**Workaround:** When you create a user on a Windows server, log into the server with that user by using a remote desktop or at the console before performing Opsware SAS actions (such as, file system browsing, running a DSE script, or registry browsing) that result in the server login ID being used on the server.

**Bug ID:** 134832

**Description:** The OCC Client exhibits poor performance when you click All Managed Servers.

**Subsystem:** Server Explorer in the OCC Client UI

**Platform:** Independent

**Symptom:** When a user clicks All Managed Servers immediately after starting the OCC Client, with their cache already populated, it takes a long time for the full server list to appear. For example, it can take 20 minutes for a list of 14,000 servers to appear.

**Workaround:** To see the entire server list immediately, wait 1-2 minutes after launching the OCC Client before clicking All Managed Servers.

**Bug ID:** 134103

**Description:** Selecting a patch to view its vendor documentation closes the OCC Client.

**Platform:** Windows

**Subsystem:** OCC Client - Windows Patch Management

**Symptom:** In the OCC Client, selecting a patch to view the vendor documentation closes the OCC Client. This behavior is observed when the OCC Client is launched by using JRE v 1.4.2_11. The bug in JRE v 1.4.2_11 is documented as #6385867 on "bugs.sun.com"

**Workaround:** Use JRE v 1.4.2_9 or JRE v 1.4.2_10. Do not use JRE v 1.4.2_11 to launch the OCC Client.

**Bug ID:** 134464

**Description:** In the Opsware Command Center (web) UI, scheduled jobs can be run even if you have no permissions to the Job's server.

**Platform:** Independent

**Subsystem:** OCC Web - My Jobs

**Symptom:** In the Opsware Command Center (web) UI, you can schedule a job on a managed server if you have "Write" permissions to that server. Once the job is

scheduled, other users with "Edit All Jobs" permissions and no permissions to the Job's server can run, cancel, or save that Job. Opsware SAS does not re-verify permissions when users run a scheduled Job.
**Workaround:** None.

**Bug ID:** 134415

**Description:** To launch the OCC Client, Opsware SAS supports version 1.4.2_10 or earlier of the JRE for JNLP file.

**Platform:** Independent

**Subsystem:** Opsware SAS OCC Client

**Symptom:** A bug was introduced by Sun in JRE 1.4.2_11 in which accessing the vendor documentation of the patch feature will immediately halt the application. This issue might be resolved in a future patch release of the JRE from Sun; however, 1.4.2_11 and 1.4.2_12 should not be used to run the OCC Client. Use JRE version 1.4.2_10 or earlier.

**Workaround:** The following requirements are needed for running the OCC Client:

3. Download and install 1.4.2_10 from http://java.sun.com/produces/archive.
4. Enable _10 in the Java Web Start control panel.
5. Disable _11 and _12 in the in the Java Web Start control panel.

**Bug ID:** 135453

**Description:** All Tibco versions up to version 7.5.1 contain a security vulnerability.

**Platform:** Independent

**Subsystem:** Model Repository Multimaster Component

**Symptom:** All Tibco versions up to version 7.5.1 contain a security vulnerability. The impact of this vulnerability can include remote execution of arbitrary code, information disclosure, and denial of service.

**Workaround:** None. For more information about this vulnerability, see http://www.tibco.com/resources/mk/rendezvous_security_advisory.txt.

# What’s New in Opsware SAS 5.5.3

## New Operating System Support

Opsware SAS 5.5.3 supports new versions of Solaris 10 Sparc and Solaris 10 x86. This release supports OS provisioning of Solaris 10 Sparc U2 and Solaris 10 x86 U2.

## Performance Optimizations

The following operations have been optimized to improve performance:

- OCC Client startup
- Patch compliance scan

## OCC Client Messages

The usability of the OCC Client has been improved with the following warning messages:

- Shutdown warning message.
- Warning message about changing the default cache update time interval (which is not recommended).
- Warning message not to reload the cache.

## ISM Upload via Satellite

Users in an Opsware Satellite data center can upload ISMs to a remote core.

## Documentation for Opsware SAS 5.5.3

This release comes with the following documentation:

- *Opsware SAS 5.5. Release Notes*
- *Planning Deployments for Opsware SAS 5*
- *Opsware SAS 5 Deployment and Installation Guide*
- *Opsware SAS 5 Configuration Guide*
- *Opsware SAS 5 Administration Guide*
- *Opsware SAS 5 User's Guide*
- *Opsware Data Center Intelligence 1.8 Administrator's Guide*
- *Opsware SAS DCML Exchange Tool 2.5 Reference Guide*
- *Opsware SAS Web Services API 2.2 Guide*
- *Opsware SAS Intelligent Software Module (ISM) Development Kit 2.0 Guide*
- *OCLI 2.0 Reference Guide*
- *CML Tutorial for Opsware SAS 5*

The Opsware SAS documentation is available online at

https://download.opsware.com/kb/category.jspa?categoryID=20

Ask your Opsware administrator for the user name and password to access the site.

# Supported Installations for 5.5.3

The Opsware SAS 5.5.3 release supports the following installations:

- New installations of a standalone core
- New installations of a multimaster core
- New installations of a Satellite
- Upgrade from Opsware SAS 5.5.1 or 5.5.2 to Opsware SAS 5.5.3.

## Upgrading to Opsware SAS 5.5.3

Opsware SAS 5.5.3 supports the following upgrade paths:

- Upgrading a Standalone Core from 5.5.1 or 5.5.2 to 5.5.3
- Upgrading a Multimaster Mesh from 5.5.1 or 5.5.2 to 5.5.3
- Upgrading an Opsware Satellite from 5.5.1 or 5.5.2 to 5.53

For information about upgrading to Opsware SAS 5.5.3, see the *Opsware SAS 5.5 Upgrade Guide*, or contact your Opsware Support Representative.

# What's Fixed in Opsware SAS 5.5.3

The following bugs are fixed in Opsware SAS 5.5.3.

**Bug ID:** 132862

**Description:** The Gateway crashes because it doesn't free error strings properly.

**Subsystem:** Opsware Gateway

**Platform:** Independent

**Resolution:** Fixed.

**Bug ID:** 133045

**Description:** Installation of some update filesets failed with a missing requisite fileset error even though the requisite fileset was also attached to the server.

**Platform**: AIX

**Subsystem**: Reconcile

**Resolution**: Fixed.

**Bug ID:** 135775

**Description:** The vault handles queried transactions incorrectly, pulling each transaction multiple times. As a result, the core is behind in handling transactions.

**Subsystem:** Model Repository Mulitmaster Component (vault)

**Platform:** Independent

**Resolution:** Fixed.

**Bug ID:** 138051

**Description:** In Configuration Tracking, you were unable you specify any filters with a date greater than December 31, 2006.

**Platform:** Independent

**Subsystem:** Configuration Tracking

**Resolution:** Fixed.

**Bug ID:** 138053

**Description:** When opening a Job progress or results for a shared script that had invalid parameters entered, the Job window is blank.

**Platform:** Independent

**Subsystem:** Distributed Scripts

**Resolution:** Fixed.

**Bug ID:** 139911

**Description:** The Data Access Engine hangs when DNS reverse lookups fail. As a result, reconciles would not begin, and the web UI for the spin and way would hang for 10 minutes before returning.

**Subsystem:** Data Access Engine (spin)

**Platform:** Independent

**Resolution:** Fixed. Log IPs instead of doing reverse lookups.

**Bug ID:** 139980

**Description:** During an Opsware SAS upgrade, mulitmaster conflicts resulted from the twist's data transformations that occured simulatneously in multiple data centers. Only the multimaster central twist should perform data transformations to avoid conflicts.

**Subsystem:** Web Services Data Access Engine (twist)

**Platform:** Independent

**Resolution:** Fixed.

**Bug ID:** 140010

**Description:** Devices in a Satellite that should be in a device group are not added to the group unless the rules for the group are changed.

**Subsystem:** Web Services Data Access Engine (twist)

**Platform:** Independent

**Resolution:** Fixed.

**Bug ID:** 140162

**Description:** On a managed server in a Satellite data center, ISMTool upload cannot bypass the wordcache in a Satellite and upload to the realword (Software Repository) in the core.

**Subsystem:** ISMTool

**Platform:** Independent

**Resolution:** Fixed. To bypass the wordcache, perform the following steps:

- In the core gateway properties file, include the following lines:

```
opswgw.EgressFilter=tcp:theword:1003:*:*
opswgw.EgressFilter=tcp:realword:1003:*:*
opswgw.EgressFilter=tcp:wordcache:1003:*:*
```

- Restart the core gateway.
- Configure DNS or /etc/hosts so that the server running the core gateway can resolve “realword” to the host running the word.
- On the managed server in the Satellite data center, set the environment variable ISMTOOLSR=realword. Then, run ismtool –upload.

**Bug ID:** 140513

**Description:** Under some circumstances, a version of the Opsware agent older than the most recent version will be deployed on Windows servers. This occurs during usage of the ODAD (ADT) feature of the OCC Client.

**Subsystem:** Agent Deployment, Upgrade Backend

**Platform:** Windows

**Resolution:** Fixed.

# Known Problems, Restrictions, and Workarounds in Opsware SAS 5.5.3

This section describes the workarounds to known problems in Opsware SAS 5.5.3.

**Bug ID:** 134379

**Description:** Garbled user profile folder name if Opsware SAS  accesses the managed server before the user logs in to the managed server.

**Subsystem:** Agent

**Platform:** All Windows

**Symptom:** If Windows managed server is accessed by Opsware SAS as a Windows user that has not been used to log into the managed server (with RDP or the console), Opsware SAS creates a garbled user profile.  For example, if you provision the OS on the Windows server with Opsware SAS, the Administrator folder (under C:\Documents and  Settings) is not accessible.

**Workaround：** If you create a new user, be sure to log in to the server with that user either with RDP or the console before using Opsware SAS actions that result in your server login being used on the server.  This includes file system browsing as your user, running a DSE as a specified user, registry browsing as your user, and so forth.

**Bug ID:** 135453

**Description:** Security vulnerability in all Tibco versions up to 7.5.1.

**Subsystem:** Model Repository Multimaster Component (vault)

**Platform:** Independent

**Symptom:** See the Tibco security advisory at the following URL:

`http://www.tibco.com/resources/mk/rendezvous_security_advisory.txt`

**Workaround:** See the Tibco security advisory at the preceding URL.

**Bug ID:** 135455

**Description:** Files in packages created by ISMTool are installed in hardcoded paths.

**Subsystem:** ISMTool

**Platform:** Windows 2003 x64

**Symptom:** For a package created by ISMTool or Visual Packager, when the package is installed on a managed Windows server, the files within the package are always installed under C:\Program Files.  This path is hardcoded in the buildism script.

**Workaround:** None

**Bug ID:** 138510

**Description:** The 'wordbot-clear' service is bound to all IP addresses instead of 127.0.0.1.

**Subsystem:** Software Repository (cleartext)

**Platform:** Independent

**Symptom:** This is a potential security issue, but does not affect the functionality of Opsware SAS. A security scan may report that privileged port 1006 is listening and responding to HTTP requests.

**Workaround:**  For a workaround, contact your Opsware Inc. support representative.

**Bug ID:** 140482

**Description:** Reconcile Software Wizard does not work with over 100 application nodes.

**Subsystem:** Opsware Command Center

**Platform:** Independent

**Symptom:** If you manually attach more than 100 application nodes to a server and you then launch the Reconcile Software Wizard, the wizard cannot display more than 100 nodes.  In the wizard, if you click on 2, 3, or Next to show the next page of nodes, the display shows up blank with "There are no items to show."

**Workaround:** Use Install Software to attach and reconcile your software.

# Documentation Errata

## Updates to the Opsware SAS 5 User's Guide

The followings topics in the Opsware SAS 5 User's Guide are updated with new information.

**Permissions Required for Working with Server Groups**

The table "Permissions Required for working with Server Groups" in the Opsware SAS User's guide is updated to include the following information:

In this table the Manage Servers permission and Model Public Server Groups permission have been updated.

| **Name of Permission** | **Where Selected** | **Enables You To** |
|---|---|---|
| Manage Servers | | Create and delete private groups, as well as edit their basic properties. |
| Model Public Server Groups | The Manage Servers Permissions section on the Other tab in Users and Groups | Add custom attributes, patches, applications to server groups. |

## Updates to the Opsware SAS 5 Administration Guide

The followings topic in the Opsware SAS 5 Administration Guide is updated with new information.

### Global Shell Audit Logs

The “Global Shell Audit Logs” section in the Opsware SAS Administration Guide is updated to include the following information:

The Global Shell Audit Logs section refers to the wrong default certificate:

```
/var/lc/crypto/cogbot/cogbot.srv
```

The correct default certificate is:

```
/var/lc/crypto/waybot/waybot.srv
```

## Updates to the Opsware SAS 5 Configuration Guide

The followings topic in the Opsware SAS 5 Configuration Guide is updated with new information.

### Uploading Windows Update Rollup Unit Type

The section “Uploading Windows Update Rollup Unit Type” is added to the chapter

“OCLI 1.0 for Package Management” in the Opsware SAS 5 Configuration Guide.

To upload Windows Update Rollup unit types using OCLI version 1.0, use

the following command:

```
oupload -O<os version>  -t<pkgtype> -C<customer> filename
```

where:

- the -t option for Update Rollups has to be "Windows Update Rollup"
- the -C option for all patch types has to be "Customer Independent"
- the filename being uploaded must already exist in the Model Repository and viewable using the OCC Client or OCC.

Example:

To upload Update Rollup, `Windows2000-KB891861-v2-x86-ENU.EXE` using OCLI, use the following command:

```
 oupload -O"Windows 2000" -t"Windows Update Rollup" -C"Customer
Independent" Windows2000-KB891861-v2-x86-ENU.EXE
```

# Contacting Technical Support

To contact Opsware Technical Support:

Phone: +1 877 677-9273 (1-877-Opsware)
E-Mail: support@opsware.com

To Contact Opsware Training:

E-mail: education@opsware.com for information.

Opsware Inc. offers several training courses for Opsware users and administrators.