MIRAPOINT

a CP company

System Software Upgrade Instructions

May 2013
Part Number: 010-00910

This Release Note supports Messaging Operating System (MOS) release 4.3.7 and higher releases until replaced by a newer edition.

The Mirapoint Software and Mirapoint documentation are Copyright © 1998-2012 Mirapoint Software, Inc. All Rights Reserved. You may not print, copy, reproduce, modify, distribute or display this work in hard copy, electronic, or any other form, in whole or in part, by any electronic, mechanical, or other means, without the prior written consent of Mirapoint Software, Inc., except that you are permitted to make one copy for archival purposes only in connection with the lawful use and operation of this software.

Mirapoint, RazorGate, and the Mirapoint logo are registered trademarks of Mirapoint Software, Inc. Mirapoint Message Server, Mirapoint Directory Server, Mirapoint Operations Console, RazorSafe, DirectPath, WebMail Direct, WebCal Direct, and GroupCal Direct are trademarks of Mirapoint Software, Inc.

Mirapoint integrates third party software programs within the Mirapoint Software, which are subject to their own license terms. If the user does not agree to abide by the applicable license terms for the integrated third party software programs as defined by the Mirapoint Software License Agreement, then you may not install or operate the Mirapoint Software.

Portions of this product are Copyright © 1982, 1986, 1989, 1991, 1993 the Regents of the University of California. All Rights Reserved.

Portions of this product are Copyright © Dell Inc. Used with permission.

Portions of this product are Copyright © 2010 Red Hat, Inc. All Rights Reserved. The “Red Hat” trademark and the “Shadowman” logo are registered trademarks of Red Hat, Inc. in the U.S. and other countries.

Portions of this product are Copyright © 1997, 1998 FreeBSD, Inc. All Rights Reserved.
Portions of this product are Copyright © 1996-1998 Carnegie Mellon University. All Rights Reserved.

Portions of this product are Copyright © 1997-1998 the Apache Group. All Rights Reserved.
Portions of this product are Copyright © 1987-2006 Larry Wall. All Rights Reserved. See http://www.perl.org.
Portions of this product are Copyright © 1990, 1993-1997 Sleepycat Software. All Rights Reserved.

This software is derived in part from the SSLava™ Toolkit, which is Copyright © 1996-1998 by Phaos Technology Corporation. All Rights Reserved.

Portions of this product are Copyright © 1998, 1999, 2000 Bruce Verderaime. All Rights Reserved.
Portions of this product are Copyright © 1999-2003 The OpenLDAP Foundation, Redwood City, California, USA. All Rights Reserved.
Portions of this product are Copyright © 2005-2010, The Dojo Foundation. All Rights Reserved.
Portions of this product are Copyright © 2010, Yahoo! Inc. All Rights Reserved.
Portions of this product are Copyright © 2010 VMware, Inc. All Rights Reserved.

OpenLDAP is a registered trademark of the OpenLDAP Foundation.

Macintosh is a trademark of Apple Computer, Inc.

Windows, Outlook, Exchange, and Active Directory are trademarks of Microsoft Corporation.

Java and Solaris are trademarks of Sun Microsystems, Inc.

Linux is a registered trademark of Linus Torvalds.

Zimbra and the Zimbra logo are trademarks of VMware, Inc.

All other trademarks are the property of their respective owners.

OTHER THAN ANY EXPRESS LIMITED WARRANTIES THAT MIRAPOINT PROVIDES TO YOU IN WRITING, MIRAPOINT AND MIRAPOINT'S LICENSORS PROVIDE THE SOFTWARE TO YOU “AS IS” AND EXPRESSLY DISCLAIM ALL WARRANTIES AND/OR CONDITIONS, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. IN NO EVENT SHALL MIRAPOINT'S LICENSORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY OR CONSEQUENTIAL DAMAGES, HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY (INCLUDING NEGLIGENCE OR OTHER TORT), ARISING IN ANY WAY OUT OF YOUR USE OF THE SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF DAMAGES. MIRAPOINT’S LIABILITY SHALL BE AS LIMITED IN THE LICENSE AGREEMENT.

Contents

Technical Support 5
Sending Diagnostic Data to Technical Support 6

Upgrading to the latest MOS release 7
Before You Upgrade 8
Product Notices 9
NIS Is Not Supported 9
Deprecated Commands and Applications 9
SNMP MIBs are Periodically Updated 9
Recommended Schedule for Image Backups 9
Upgrading with the Administration Suite 10
Upgrading with the Command-Line Interface (CLI) 11
Reinstalling If Problems Arise 12
Upgrading on Clustered Appliances 12
After You Upgrade 14
Update Appliance Licenses 14
Update Appliance Time (non-NTP Server Only) 14
Update the Antispam Engines 14
Check the Antivirus Protection 15
Reinstall Needed Patches 15
Back Up the Appliance 15
Upgrade Your Brand 16

Appendix 17
Evaluating Performance for MOS Upgrade 17
Identifying Your User Profile 17
Checking Your Appliance Load 19

Technical Support

If you experience problems with your appliance, contact the company from which you purchased your Mirapoint appliance.

If you purchased your appliance directly from Mirapoint, contact Mirapoint Technical Support by email, telephone, or via the Mirapoint Support website:

Email: support@mirapoint.com
(China) support@mirapoint.com.cn

Telephone:

- (USA and Canada) 1.800.353.8437
- (Italy) + 39 011 4513811 + 39 011 4513832
- (UK) 00 800 222 88800
- (China) 400 707 1086
- (Australia) 1 800 633 784
- (Elsewhere) +800 2228 8800.

Website: https://support.mirapoint.com/

When contacting Technical Support, be prepared with the following information about your appliance:

This information can be obtained by entering the 'model get info' command in current MOS

Table 1 Required Appliance Information for providing Technical Support

Information	MOS CLI command
Software release	`Version`
Host ID	`License Hostid`
Serial number	`Model Get Serial`
Hardware model	`Model Get Chassis`

Sending Diagnostic Data to Technical Support

To help diagnose problems, Technical Support may ask you to provide diagnostic data from your appliance. If requested, to send diagnostic data to Support:

1. Use a web browser to go to this URL:

   `http://MirapointSystem/diag`

   where *MirapointSystem* is the fully qualified domain name of your appliance.
2. Enter the username and password credentials of a user with administration privliges to log into the Multifunction Diagnostic sub-system.
3. Select the "Collect Diagnostic Data" link from the LHS menu, set the Diagnostic Level attribute to the correct value [1..7] that has been requested by the support staff. Leave the Transfer Method set to FTP upload (the default) unless you need to use a different method to send the diagnostic data to support.
4. Click Transfer Diagnostic Data to send the data to Mirapoint Technical Support.

Upgrading to the latest MOS release

This chapter describes how to upgrade to the latest MOS release on any compatible Mirapoint Message Server or RazorGate appliance. You can upgrade the version of MOS on any Mirapoint Message Server or RazorGate appliance running MOS release 4.1.9-GA or later.

Please see the following sections for information on check that must be performed when upgrading to the latest MOS release.

- Before You Upgrade on page 8
- Install a release, using either method:
  - Upgrading with the Administration Suite on page 10
  - Upgrading with the Command-Line Interface (CLI) on page 11
- Reinstalling If Problems Arise on page 12
- Upgrading on Clustered Appliances on page 12
- After You Upgrade on page 14

Once installed, a MOS release cannot be uninstalled.

By installing the MOS software, you agree to accept the terms of the License Agreement referenced at the start of this document.

Never reboot the appliance while an upgrade is in progress.

Mirapoint requires that all appliances on the same network run the same MOS release, including patches. For example, a RazorGate appliance must run the same MOS release as the Message Server for which it serves as a proxy.

When upgrading, even if the new release has different default settings for the appliance options, most options will remain unchanged after the upgrade. For example, for the Calendar service, on a new appliance "Email Mode" is the default. When upgrading to this release, the existing Calendar service mode is preserved rather than automatically switching to the default "Email Mode".

Before You Upgrade

Before you upgrade to a release, you need to do the following tasks as applicable to your appliance configuration:

1. Ensure the appliance is running a compatible and upgradeable release as listed on the support site.
2. Perform a backup before upgrading, using your normal appliance backup process.

   For RazorGate appliances that do not have JMM mailboxes, Mirapoint recommends using the CLI `Conf Export` command to save a copy of the appliance configuration.
3. If your appliance is licensed for Antispam, note which engine(s) you are using, such as `default` or `rpdengine`:
   - In the Administration Suite, use the Anti-Spam page.
   - In the CLI, use the `Uce Version` command.

   You must explicitly reapply these engines after upgrading, as part of the After You Upgrade on page 14.
4. If you are using LDAP autoreply and are upgrading from a release prior to MOS 4.1, update your Mirapoint schema file:
   a. To obtain the current schema, use the `Dir Getschema Mirapoint` command.
   b. Add the LDAP autoreply attributes that are new in MOS 4.4: `miWmprefShowMiralets, miWmprefShowMessageView`

   For more information on updating the schema, see the `Dir` command in the Mirapoint Administration Protocol Reference.
5. Note which Defect and Enhancement Patches (D* and E* Patches) are installed on the appliance. If any of these patches are not integrated into the new MOS release you are installing (Check the MOS release notes) and you still need the functionality they provide after upgrading, you will need to re-install them as part of your post-installation configuration tasks.

Product Notices

This section provides important considerations before you upgrade. Please check https://support.mirapoint.com/ for the latest field notices and product updates.

NIS Is Not Supported

NIS (Network Information Service) is not supported in MOS 4.x releases. Mirapoint recommends that customers migrating from a MOS 3.x release with NIS authentication convert their data to LDAP.

Deprecated Commands and Applications

- F-Secure Antivirus is deprecated, as of November 2011. Mirapoint recommends that F-Secure users transition to using Sophos Antivirus as a replacement Antivirus solution.
- Mirapoint Operations Console was deprecated in a previous MOS release. Mirapoint recommends that Operations Console users convert your operational procedures to use the CLI `Conf Import` and `Conf Export` commands to replace the primary Operations Console functions.
- XML is now a standard feature, so a license is no longer necessary. (48940)
- Uce SetOption MultiEngineBulkOnly subcommand has been deprecated and is replaced by Uce SetOption RescanLowerLimit and RescanUpperLimit subcommands. (50241)
- Commands and applications deprecated in a new release still function in the first future release, but are no longer available in subsequent MOS release. For example, commands and applications deprecated from MOS 4.3. in MOS 4.4 are still available in MOS 4.4, but are no longer guaranteed to be available in any later MOS releases, such as 4.5. This gives you time to transition away from using the deprecated commands and applications before they are removed from the future versions of MOS.

SNMP MIBs are Periodically Updated

If you use SNMP to monitor your system, Mirapoint recommends downloading the MIB files from the system after upgrading Mirapoint software to ensure that you are using the latest MIBs. MIBs can be upgraded by any release. Current MIBs are always available at:

http://your-Mirapoint-host/help/snmp-mibs/

Recommended Schedule for Image Backups

For administrators who perform a daily image backup of the system, Mirapoint recommends not starting this backup during the nightly log processing, which begins at midnight. To avoid excessive system load, wait until after 1:00 a.m. before starting the daily image backup.

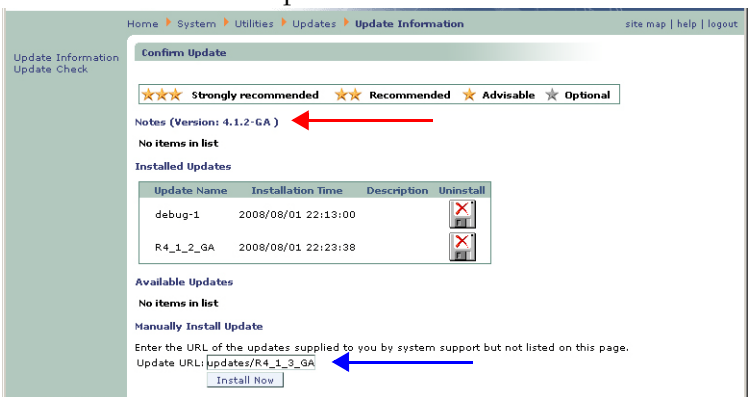
The Mirapoint Selective Restore feature's scheduled daily snapshots, if configured, start at midnight.

Upgrading with the Administration Suite

To upgrade to the latest MOS release using the Administration Suite:

1. Log in to the Administration Suite as administrator.
2. From the System > Utilities > License page, ensure you have the Upgrades Allowed license (f).

   If you do not have it, click Install Licenses. If that does not apply the license, contact your Mirapoint sales representative or Mirapoint Technical Support.
3. At the top of the System > Utilities > Updates > Update Information page, find the Version: number in parentheses.



4. Enter a link (for example `ftp://ftp.mirapoint.com/pub/updates/P4_4_2_FCS`) provided on the MOS release page of the support website.
5. Click Install Now.

   After the connection closes, the update completes on its own. The appliance reboots itself several minutes after the connection closes, depending on network speed, RAID arrays, and SAN configuration, if present. Reboot after installing the R-patch is longer than after the P-patch.

For important post-installation tasks, see After You Upgrade on page 14.

If the update fails for any reason (the appliance returns the message "`NO Unable to install update`"), log into the Administration Suite and view the System Log, which might indicate why the update failed. Possible reasons for a MOS upgrade to fail include:

* Your system support license ("Upgrades Allowed") expired.
* Not enough free disk space available on the appliance.
* You entered the name of the upgrade patch incorrectly. Everything except ftp://ftp.mirapoint.com is case-sensitive.

* You have a network connectivity problem. You might get better results by copying the patch .mpu5 files (for example; P4_4_3-GA.mpu5) to a local FTP server.
* Your current MOS release is too old to be upgraded to the intended version of MOS.

Upgrading with the Command-Line Interface (CLI)

To upgrade to the latest MOS release using the administration CLI:

1. Use a telnet client to connect to the administration command-line interface on port 23 on your Mirapoint appliance.
2. Log in as administrator.
3. Run the `Update Install:` command with a link (for example `ftp://ftp.mirapoint.com/pub/updates/P4_4_2_FCS)` provided on the MOS release page of the support website.

   After the connection closes, the update completes on its own. The appliance reboots itself several minutes after the connection closes, depending on network speed, RAID arrays, and SAN configuration, if present. Reboot after installing the R-patch is longer than after the P-patch.

P patches are generally for upgrades to minor release numbers, for example; 4.4.2-FCS to 4.4.3-GA. R patches are for release upgrades, for example; 4.2.5-GA to 4.4.3-GA.

To reduce maintenance downtime, you can download the update separately from needing to install it to a local FTP / HTTP server. This allows you download the update to a single location and re-use it to upgrade other appliances instead of downloading it each time for every appliance. For more information, see the Update command in the Mirapoint Administration Protocol Reference.

For important post-installation tasks, see After You Upgrade on page 14.

If the update fails for any reason (the appliance returns the message "`NO Unable to install update`"), log into the Administration Suite and view the System Log, which might indicate why the update failed. Possible reasons for a MOS upgrade to fail:
* Your system support license ("Upgrades Allowed") expired.
* Not enough free disk space available on the appliance.
* You entered the name of the upgrade patch incorrectly. Everything except ftp://ftp.mirapoint.com is case-sensitive.
* You have a network connectivity problem. You might get better results by copying the patch .mpu5 files to a local FTP server.
* Your current MOS release is too old to be upgraded to the intended version of MOS.

Reinstalling If Problems Arise

If you experience a failure which you believe might require a MOS reinstallation, contact Mirapoint Technical Support. Improper installation can cause data loss.

Upgrading on Clustered Appliances

Upgrading the MOS release on appliances in an N+1 failover cluster configuration is more complicated than the normal upgrade procedure. You must detach all appliances from the cluster, delete the cluster, upgrade the standby appliance, create a new cluster, and upgrade and attach each active appliance. Failure to follow this procedure can result in upgrade failure.

To install a MOS upgrade on clustered appliances:

1. Use a telnet client to connect to the administration command-line interface on port 23 to an active appliance, and log in as an administrator.
2. Detach the active appliance from the cluster:

   ```
   Cluster Detach
   ```
3. Repeat steps 1 and 2 until all active appliances are detached from the cluster.
4. Log in to the standby appliance as an adminsitrator.
5. From the standby appliance, delete the cluster:

   ```
   Cluster Delete
   ```

Though the cluster is gone, all active appliances continue to operate normally.

6. On the standby appliance, install the MOS upgrade:
   - To install using the Administration Suite, see Upgrading with the Administration Suite on page 10.
   - To install using the CLI, see Upgrading with the Command-Line Interface (CLI) on page 11.

   For important post-installation tasks, see After You Upgrade on page 14.
7. After the standby appliance is successfully upgraded, re-create the cluster:

   ```
   Cluster Add clustername
   ```
8. On an active appliance, install the MOS upgrade as performed in step 6, including post-installation tasks. (Perform the post-installation tasks on this node immediately after upgrade; do not wait until all active appliances are attached to the new cluster.)
9. Attach the appliance to the cluster:

   ```
   Cluster Attach clustername
   ```
10. On the standby appliance, associate the standby appliance with all of the active appliance in the cluster:

    ```
    Cluster Scan
    ```

11. Working on one active appliance at a time, repeat steps 8-10 on all active appliances.
12. After all active appliances have been upgraded and attached to the cluster, ensure all appliances have rebooted after their MOS upgrades and post-installation tasks completed.
13. Check the console output to confirm that all the nodes are found.

Ensure you complete an update list before upgrading.

After You Upgrade

After you upgrade to this release, you need to do the following tasks as applicable to your appliance configuration:

1. Update Appliance Licenses on page 14 for all appliances
2. Update Appliance Time (non-NTP Server Only) on page 14 for all appliances that are not using an NTP server
3. Update the Antispam Engines on page 14, for all appliances running Antispam
4. Check the Antivirus Protection on page 15, for all appliances running Antivirus
5. Reinstall Needed Patches on page 15, if you still need any D-patches, or E-patches (such as ConnectR or MCM), that are not integrated into this release
6. Back Up the Appliance on page 15, for all appliances except RazorGates without JMM mailboxes
7. Upgrade Your Brand on page 16, if you have a branded interface

Update Appliance Licenses

In case any licenses have changed or need to be reapplied after installing an updated MOS release, fetch the appliances licenses using either Install Licenses on the Administration Suite System > Utilities > License page or the CLI `License Fetch` command. Reapplying licenses does not require a restart of services on the appliance.

Update Appliance Time (non-NTP Server Only)

If you do not use an NTP server for the appliance you might need to update the time on the appliance. Later MOS releases synchronize time differently than in releases prior to MOS 4.2, so the upgrade could have reset the appliance time by up to several hours.

This is relevant only when upgrading from a MOS 4.1 release. It is not relevant when upgrading from MOS 4.2 or later releases.

Update the Antispam Engines

If you use one or more antispam engines, for each engine that you use, perform an explicit engine update using either the Administration Suite Anti-Spam > Updates page or the appropriate CLI command(s), such as:

- `Uce Update rpdengine`
- `Uce Update rpdasia`
- `Uce Update rpdeurope`
- `Uce Update rpdoutbound`
- `Uce Update default`
- `Uce Update premium`

Failure to execute the `Uce Update` command can cause mail flow disruptions.

For the first `Uce Update` command after a MOS upgrade, do not use `Uce Update *`. The wildcard does not have the expected effect because the appliance does not know after the upgrade which engines to update.

To verify the proper engines are installed after the update, use `Uce Version`.

Check the Antivirus Protection

If you use an antivirus solution, ensure that it is updated to the current version. If the appliance is configured for automatic antivirus updates, as Mirapoint recommends, this task might be extraneous.

To check the antivirus solution version on the appliance:

```
Antivirus GetVersion [sophos|rapid]
```

Reinstall Needed Patches

Install any patches that you still need on your appliance:

- If you use ConnectR or Mirapoint Connector for Mac (MCM), you must reinstall the patches that supply those downloads.
- You might need to reinstall some D-patches or E-patches, if you still need them and they are not integrated in this new MOS release.

Make sure you install patches for the new MOS release; patches for the old MOS release might not be compatible. For more information about a particular patch, contact Mirapoint Technical Support.

Back Up the Appliance

Mirapoint recommends that you immediately perform a full backup at this time. For RazorGate appliances without JMM mailboxes, Mirapoint recommends using the CLI `Conf Export` command to save a copy of the appliance configuration.

Before any action that might require an appliance reboot (such as adding disks, installing a software update, or halting the system), verify that neither a backup nor restore is in progress because rebooting stops it.

To check the status of a backup:

- For Mirapoint backup, run the CLI `Backup Status` commands.
- For NDMP backup, check the backup server (DMA).

Restoring A Backup

Format changes between major MOS releases might prohibit the restore of certain classes of user data from pre-upgrade backups, such as WebCal data, WebMail/WebCal preferences, Address Book data, user dictionaries, and message filters.

- Full restores—Can be done only to an appliance running the same MOS release and patches as when the backup was made. The mailstore (as reported by the `Storage Space` command) must also be the same size as, or larger than, the source appliance's mailstore.
- Selective restores—Can be done to an appliance running the same or a newer MOS release.

To check the status of a restore:

- For Mirapoint restore, run the CLI `Restore Status` commands.
- For NDMP restore, run the `Ndmp Merge Status` command.

Upgrade Your Brand

Because of the new interface for WebMail/WebCal Corporate Edition (CE) in this version of MOS, you must redo your branding for CE. Your current Standard Edition WebMail/WebCal and Junk Mail Manager brands remain intact once you upgrade to the latest MOS release and are re-used without changes.

If you had branded WebMail/WebCal Corporate Edition (CE) before upgrading to the latest MOS release, launching CE after the upgrade displays the CE - Version 1 interface. Seeing the old CE interface does not mean that the upgrade has failed; you must rebrand CE to see the new CE - Version 2 interface. Publishing the latest MOS CE branding overwrites the old CE interface branding, thus enabling the new CE interface with the new branding.

To brand Corporate Edition (version 2) to the latest MOS:

1. Download the MOS sysbrand.zip file for CE.
2. Unzip and modify the MOS files.
3. Publish the modified MOS CE brand files.

For complete details on branding Corporate Edition in MOS, see the Mirapoint Branding Guide.

Never publish a brand based on a different MOS release. It can lead to functionality loss, broken links, and incorrectly displayed pages. For example, do not publish a MOS 4.2.4 brand onto a MOS 4.3.7 appliance.

Appendix

This appendix applies to users who are upgrading from Corporate Edition Webmail -Version 1 to Version 2.

Evaluating Performance for MOS Upgrade

The extensive improvements in Corporate Edition Webmail - Version 2 requires additional server resources beyond what Corporate Edition Webmail - Version 1 required. If you offer Version 2 to your users, before upgrading your Message Server to MOS 4.4 you must evaluate the potential performance impacts on your appliance. If your answer is “no” to any of the following questions, you will not need to evaluate your server and can continue to upgrade to the latest MOS release.

- Are you running Corporate Edition WebMail?

  Check your license list for “Corporate Edition,” using either the CLI `license list` command, or in the Administration Suite under System > Utilities > License. If it is not licensed, there is no performance impact when upgrading.

- Are your users predominately Webmail users (at least 40% of your total peak user connection rate, or greater)?

  If your users are mostly POP and IMAP users, or an even distribution of POP, IMAP, and Standard Edition WebMail, there is no performance impact when upgrading MOS. To confirm your user connection type peak user rate distribution, see Identifying Your User Profile on page 17.

- Is your appliance heavily loaded?

  If your appliance is already heavily loaded on its current release, the load will only increase with this version of MOS. To evaluate this, see Checking Your Appliance Load on page 19.

- Are there any factors that would cause disk I/O to be slow?

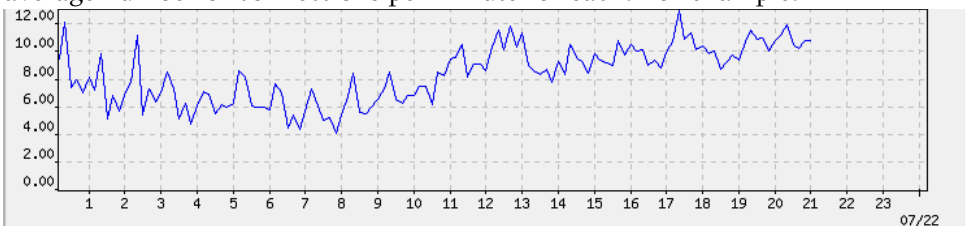
  Message Server performance can be significantly impacted by the performance of a supporting system, particularly parts of a SAN. When discussing an MOS upgrade, Mirapoint might require performance information from these supporting systems. If you do not have this information, please contact the appropriate vendor.

Identifying Your User Profile

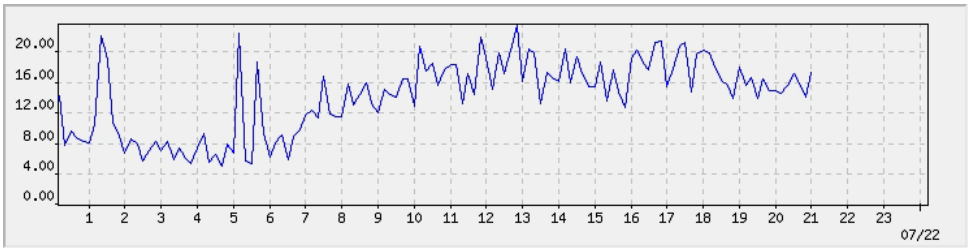
The main performance concern for upgrading to MOS is if most of your users are Corporate Edition users. To get a profile of your user community:

1. In the Administration Suite, go to Home > Performance Graphs > POP/IMAP.

2. In the bottom two graphs (POP Connections and IMAP Connections per Minute, respectively), look at busy periods and note what appears to be the average number of connections per minute for each. For example:

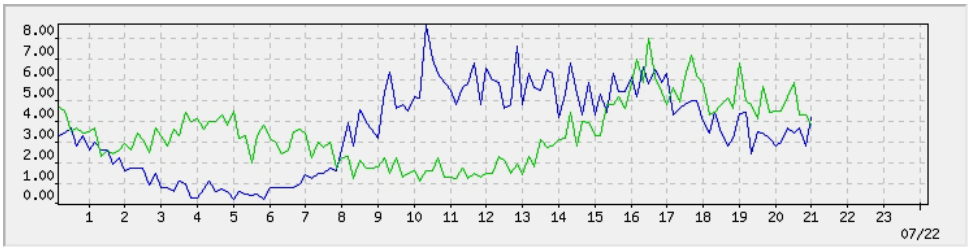


This graph could read that the appliance averages 10 POP logins per minute.



This graph could read that the appliance averages 18 IMAP logins per minute.

3. Go to Home > Performance Graphs > WebMail.
4. In the bottom graph (WebMail Logins and Logouts per Minute), look at busy periods, and note what appears to be the average number of logins (the blue line) per minute. For example:



This graph could read that the appliance averages 6 WebMail logins per minute.

5. Tally the total of POP, IMAP, and WebMail connections, and then compare their percentage value of total user connections:
   - POP = 10/34 = 29%
   - IMAP = 18/34 = 53%
   - WebMail = 6/34 = 18%

   The following table provides and example of webmail percentages to evaluate in context of the number of webmail connections.

WebMail Usage	Evaluation
< 40%	Low. Low risk of performance impact in upgrading to MOS 4.4 or later.
40-60%	Medium. Consider other factors before upgrading.

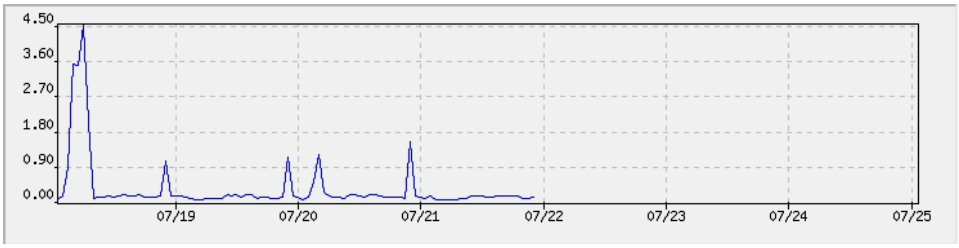
WebMail Usage	Evaluation
60% +	High. Consider other factors before upgrading.

While other factors can affect performance, such as the number of messages sent by each user, this evaluation considers such factors as consistent across all users.

Checking Your Appliance Load

If your appliance has a medium or high percentage of WebMail Corporate Edition users, you must evaluate how it handles the current load.

1. In the Administration Suite, go to Home > Performance Graphs > CPU.
2. In a week view of the System Load, note what appears to be the average load for the week. (The appliance can handle intermittent spikes; the average is the relevant statistic.)



This graph shows a single spike of moderate usage, but the load average is less than 1.

The table describes the Load Average numbers and their impact on the upgrade.

Load Average	Rating	Upgrade to MOS 4.4 or later.
< 2	Moderate	Should not cause performance issues.
2-4	Moderate to high	Probably will not impact performance, but if load is often at the high end, discuss upgrade impact with Mirapoint.
5-8	High	Probably will have high CPU usage during busy periods, and corresponding performance issues. Further information is required to determine upgrade impact.
9 +	Very high	Likely already experiencing performance issues. Contact Mirapoint before upgrading to MOS 4.4 or later.

If further advice about upgrading is needed, contact Mirapoint Technical Support as described in Technical Support on page 5.

Mirapoint recommends that you have Customer Care enabled. This sends a brief report to Mirapoint every Monday at 00:00 with information about the health of the appliance. To enable Customer Care, use the CLI `Conf Enable Customercare` command.