Deployment Guide

for version 3.11

October 31, 2016

Contents

1. Introduction 4
1.1 Getting Started 5
1.1.1 P1000 Pico 6
1.1.2 V1000 Virtual 7
1.1.3 M1000 MiniRack 8
1.1.4 E1000 Enterprise 9
1.1.5 E2000 Enterprise 10
2. Using the Mirth Appliance Control Panel 11
2.1 System Menu 13
2.1.1 Dashboard 14
2.1.2 Backups 16
2.1.3 Restore 18
2.1.4 Software Updates 20
2.1.5 Certificates 22
2.1.6 Auditing 26
2.1.7 Network 30
2.1.8 Alerts 34
2.1.9 VPN Server 35
2.1.10 Date & Time 36
2.1.11 Mail 37
2.1.12 Users 39
2.2 Folders Menu 45
2.2.1 Browse 46
2.2.2 Network Folders 48
2.3 Services Menu 50
2.3.1 Services Control 51
2.3.2 Auto Backup 52
2.3.3 Auto Update 54
2.3.4 Clustering 56
2.3.5 Console 59
2.3.6 Directory 61
2.3.7 Glassfish 63
2.3.8 Load Balancing 67
2.3.9 Postgres 70
2.3.9.1 Replication 73
2.3.9.2 Auto Failover 81
2.3.9.3 Manual Failback 84
2.3.10 Printing 85
2.3.11 SFTP 87
2.3.12 SNMP 91
2.3.13 SSL Tunnels 92
2.3.14 VPN Connections 94
2.4 Applications Menu 98
2.4.1 Applications Control 99
2.4.2 Select Default Application 106
2.4.3 Configure Referrer Whitelists 108
2.4.4 Mirth Connect > Clustering 109

2.4.4.1 Mirth Connect Clustering Wizard 111
2.4.4.2 Manual Setup for Mirth Connect Clustering 126
2.5 Help Menu 130
2.5.1 Documentation 131
2.5.2 Downloads 132
2.5.3 Contact Support 133
2.5.4 SupportNet 134
2.5.5 Context Help 136
3. Monitoring 137
4. Deployment Considerations 138
5. Factory Reset (hardware models only) 146

Introduction

Mirth® Appliances provide a ready-to-run healthcare messaging platform that is stable, secure, and scalable. With full commercial support and a simple management control panel, there is no easier way to run Mirth Connect with confidence in your organization. Mirth Appliances provide incredible value to any organization requiring heath information technology messaging capabilities.

Since Mirth Connect is based on open-source technology, there are no server license fees or per-message charges. The cost of a Mirth Appliance is very attractive when compared with alternatives such as piecing together a solution using various unsupported open-source products, purchasing and implementing a commercial software solution, or developing a custom application in-house.

> ⚠ You of course need to place the Mirth Appliance behind proper firewalling. It is always advisable to place a firewall in front of anything connected to the internet, including Mirth Appliances.
>
> See the Deployment Considerations section of this guide for more information about Mirth Appliances and firewalls.

Mirth Connect is an open source cross-platform HL7 interface engine that enables bi-directional sending of HL7 messages between systems and applications over multiple transports. By utilizing an enterprise service bus framework and a channel-based architecture, Mirth Connect allows messages to be filtered, transformed, and routed based on user-defined rules. Creating HL7 interfaces for existing systems becomes easy using the web-based interface and channel creation wizard, which associates applications with Mirth Connect engine components.

HL7 has established itself as the lingua franca of healthcare information exchange. In order to integrate your existing services with HL7 systems you must implement an adapter layer to transform messages between your domain and the HL7 world. Mirth Connect makes this easy by providing the framework for connecting disparate systems with protocol adapters and message transformation tools.

Mirth Connect uses a channel-based architecture to connect your systems with other HL7 systems. Channels consist of inbound and outbound endpoints, filters, and transformers. Multiple filters and a chain of transformers can be associated with a channel. The Mirth Connect interface allows for reuse of filters and transformers on multiple channels.

Getting Started

Mirth Appliances are designed for rapid deployment and ease of use. Simply mount or position the hardware, connect the power and network cables, and turn the unit on. Initial network configuration is performed via Dynamic Host Configuration Protocol (DHCP).

> ⚠ ***Note**: You can set the IP address by connecting directly to the Mirth Appliance with a monitor and keyboard (Console interface) or via the Control Panel (Web interface). See Console (Services > Console) or Network (System > Network).*

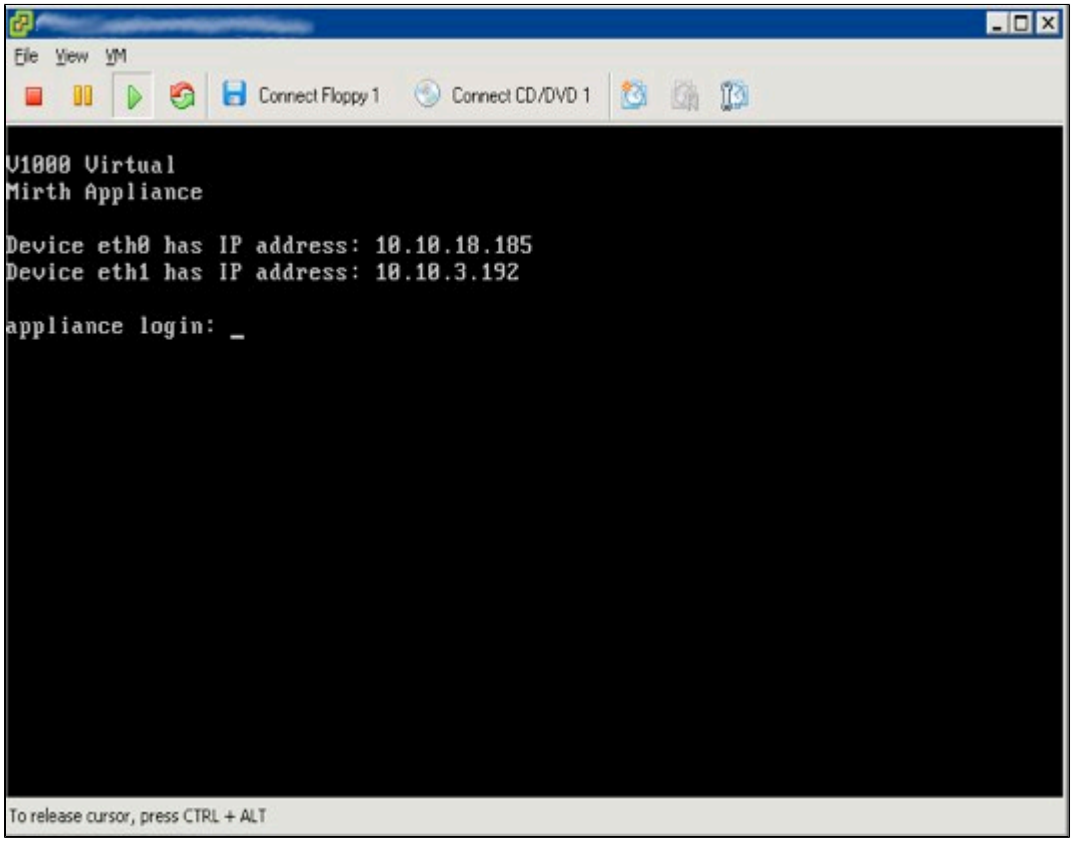
Connect a keyboard and monitor to the Mirth Appliance to get the device's IP address. Using the IP address, connect to the Appliance's embedded web application to monitor or configure the Appliance.

The following subsections have specific instructions for the various Mirth Appliance models.

P1000 Pico

Step	Action
1	Set on any flat surface. Install rubber feet pads (included). P1000 Appliances may be stacked.
2	Connect one or more network cables.
3	Connect a monitor and keyboard.
4	Connect the power supply.
5	Wait a few minutes for the Appliance to fully boot. Once the Appliance is fully booted, you will see the prompt appliance login. If using DHCP, note the IP address for eth0 displayed on the screen and skip to the last step.
6	If not using DHCP, login to the console interface with the default login/password, which is console/console. Once logged in, you will see the Mirth Appliance Console menu. Navigate down to the Change IP Address menu and follow the prompts.
7	You can now exit out of the console interface and manage the Appliance through the http interface at http://W.X.Y.Z/ , where W.X.Y.Z is the IP address of the Appliance. The default login/password for the web interface is admin/admin.

V1000 Virtual



Virtual Appliance in VMWare Player

Step	Action
1	You must have some version of VMware virtualization software already installed, such as VMware Player, Fusion, Server, etc.
2	If you have received a DVD from Mirth with the virtual Appliance image file, this file will be in the base directory. If delivered electronically, the image file will be in the “outgoing” directory of the sftp server.
3	Import the virtual machine image into the VM virtualization application you have running. Consult the documentation on your VMware product for importing and converting the Virtual Appliance image.
4	Wait a few minutes for the Virtual Appliance to fully boot. Once the Virtual Appliance is fully booted, you will see the prompt appliance login. If using DHCP, note the IP address for eth0 displayed on the screen and skip to the last step.
5	If not using DHCP, login to the console interface with the default login/password, which is console/console. Once logged in, you will see the Mirth Appliance Console menu. Navigate down to the Change IP Address menu and follow the prompts.
6	You can now exit out of the console interface and manage the Appliance through the http interface at http://W.X.Y.Z/ , where W.X.Y.Z is the IP address of the Virtual Appliance. The default login/password for the web interface is admin/admin.

M1000 MiniRack

Step	Action
1	Install in a 19” rack or cabinet using the included rack rails and mounting hardware. Adaptors are included to accommodate different styles of mounting holes.
2	Connect the power cord to the power supply on the back of the unit.
3	Connect one or more network cables.
4	Connect a monitor and keyboard.
5	Wait a few minutes for the Appliance to fully boot. Once the Appliance is fully booted, you will see the prompt *appliance login*. If using DHCP, note the IP address for eth0 displayed on the screen and skip to the last step.
6	If not using DHCP, login to the console interface with the default login/password, which is console/console. Once logged in, you will see the Mirth Appliance Console menu. Navigate down to the Change IP Address menu and follow the prompts.
7	You can now exit out of the console interface and manage the Appliance through the http interface at http://W.X.Y.Z/, where W.X.Y.Z is the IP address of the Appliance. The default login/password for the web interface is admin / admin.

E1000 Enterprise

Step	Action
1	Install in a 19” rack or cabinet using the included rack rails and mounting hardware. Adaptors are included to accommodate different styles of mounting holes.
2	Connect one or more power cords to the power supplies on the back of the Appliance.
3	Connect one or more network cables.
4	Connect a monitor and keyboard.
5	Wait a few minutes for the Appliance to fully boot. Once the Appliance is fully booted, you will see the prompt appliance login. If using DHCP, note the IP address for eth0 displayed on the screen and skip to the last step.
6	If not using DHCP, login to the console interface with the default login/password, which is console/console. Once logged in, you will see the Mirth Appliance Console menu. Navigate down to the Change IP Address menu and follow the prompts.
7	You can now exit out of the console interface and manage the Appliance through the http interface at http://W.X.Y.Z/, where W.X.Y.Z is the IP address of the Appliance. The default login/password for the web interface is admin/admin.

E2000 Enterprise

Step	Action
1	Install in a 19” rack or cabinet using the included rack rails and mounting hardware. Adaptors are included to accommodate different styles of mounting holes.
2	Connect one or more power cords to the power supplies on the back of the Appliance.
3	Connect one or more network cables.
4	Connect a monitor and keyboard.
5	Wait a few minutes for the Appliance to fully boot. Once the Appliance is fully booted, you will see the prompt appliance login. If using DHCP, note the IP address for eth0 displayed on the screen and skip to the last step.
6	If not using DHCP, login to the console interface with the default login/password, which is console/console. Once logged in, you will see the Mirth Appliance Console menu. Navigate down to the Change IP Address menu and follow the prompts.
7	You can now exit out of the console interface and manage the Appliance through the http interface at http://W.X.Y.Z/, where W.X.Y.Z is the IP address of the Appliance. The default login/password for the web interface is admin/admin.

Using the Mirth Appliance Control Panel

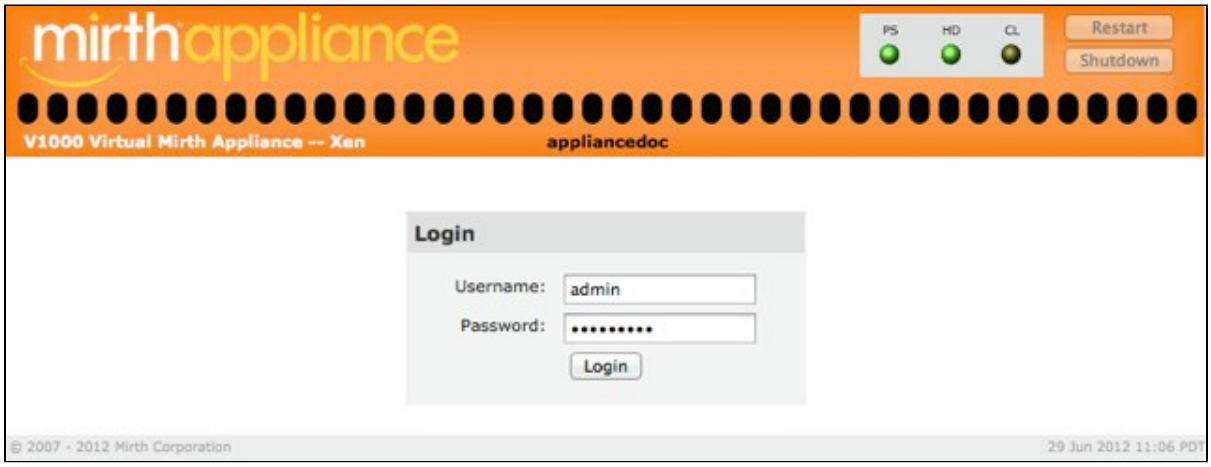
The Control Panel is a Web UI that allows the user to view and set the details of the Mirth Appliance's configuration and monitor and control its operation.

Conventions used in this guide

- References to the various items on the user interface pages are displayed in **bold** text. This includes page names, section names, field names, button names, and so on.
- Items that are not part of the page itself, such as values entered in text fields or selected from drop-down lists, are displayed in *italics*.
- In all cases the capitalization of these items matches what is on the screen.

The first step in using the Control Panel is to log in.

Logging In

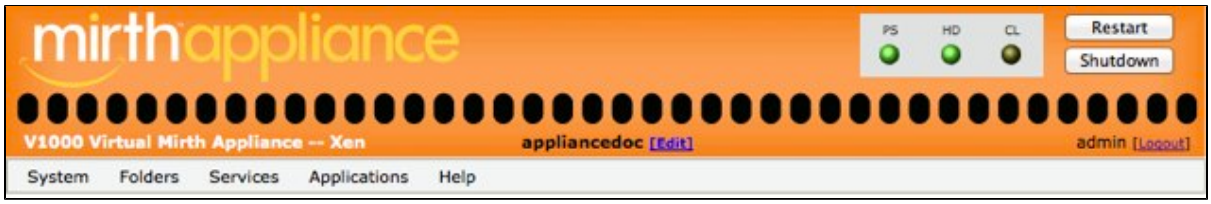


Mirth Appliance Control Panel Login Page

The default login credentials are username: admin, password: admin. Enter the username and password and click the Login button.

Note: *The default credentials should be deleted or changed as soon as possible to ensure security. See Users (Applications > Manage Control Panel > Users).*

Once a user is logged into the Appliance the Control Panel displays the following drop down menus: **System**, **Folders**, **Services**, **Applications**, and **Help**. Clicking on the name of the menu automatically selects the first drop down menu item. For example, the drop down items in the **System** menu are **Dashboard**, **Backups**, **Restore**, **Update**, **Certificates**, **Network**, **VPN Connections**, **Date & Time**, **Mail**, and **Users**. Clicking on the **System** menu goes directly to the **Dashboard** (the first item in the **System** menu).



Control Panel page header

Besides the menu bar, the Control Panel also displays three indicators: **PS**, **HD**, and **CL (or LB)**, and two buttons: **Restart** and **Shutdown**.

The indicators display the current status for the Power Supply, Hard Disk, and Clustering (or Load Balancing), respectively.

The color indicates their current status: green indicates functioning normally, yellow indicates a warning state, and red indicates a failure. A dark indicator means that the item cannot be monitored, such as CL (Clustering) when Clustering is not enabled. (See *Monitoring* in the Appliance's Help Overview.)

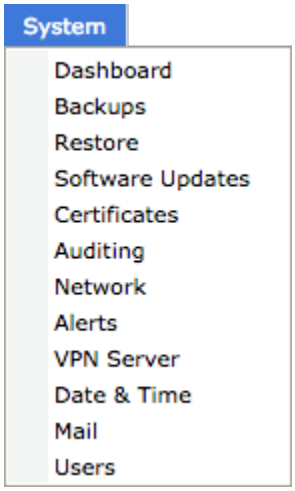
The **Restart** and **Shutdown** buttons allow you to restart or shutdown the Mirth Appliance. Clicking either of these buttons will display a confirmation dialog. If you confirm the action, the Appliance will execute it.

> ⚠ ***Note:*** *The* ***Shutdown*** *button is the preferred method for shutting down a Mirth Appliance.*

The **Restart** button will perform a reboot operation. The unit will shutdown and immediately power up again.

The **Shutdown** button will perform a system shutdown and leave the unit in a power-off state. To restart the Appliance after a shutdown, you must press the power button on the front panel.

System Menu

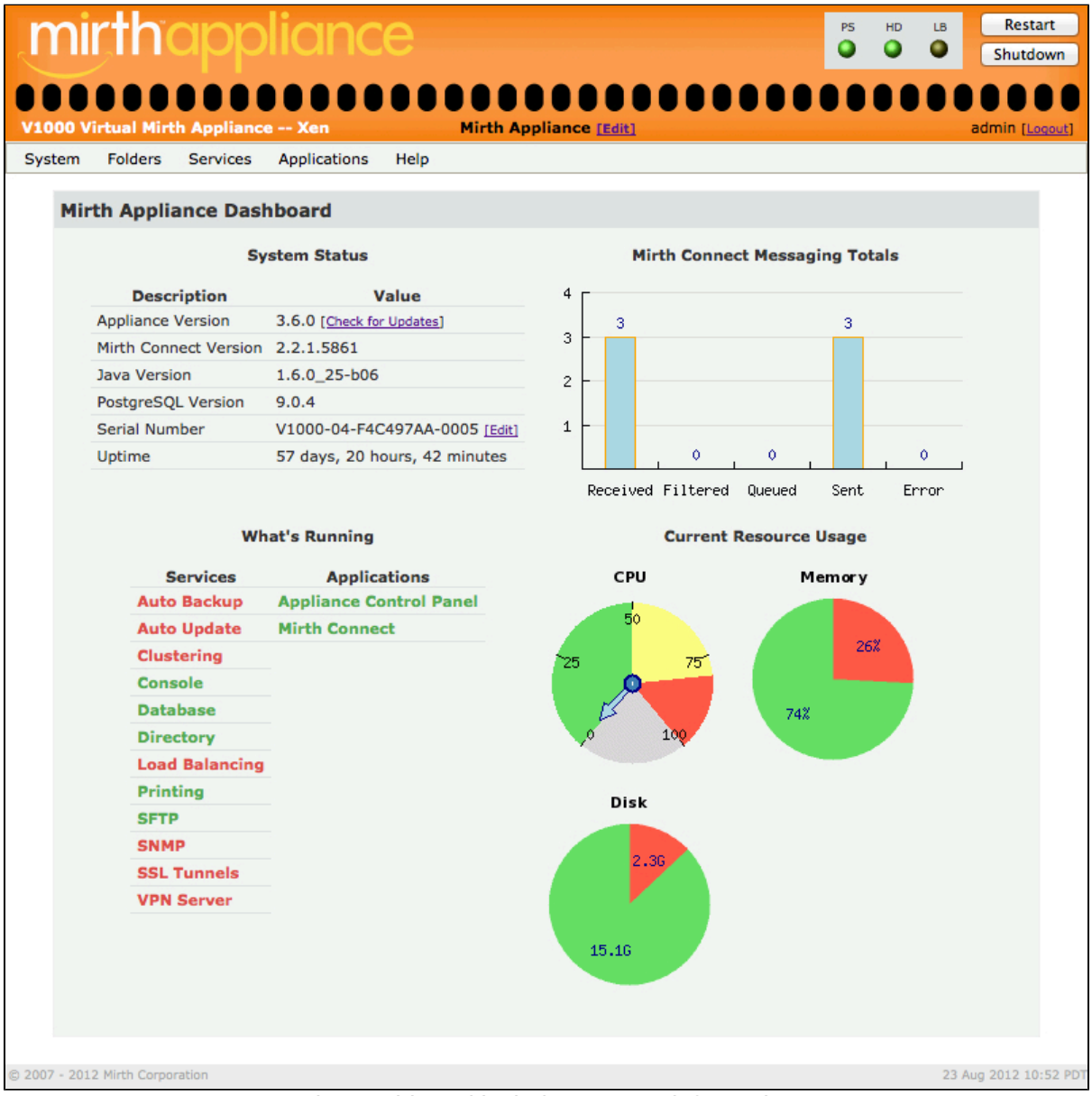


Mirth Appliance system administration is performed via the Control Panel web application. All functions are easy to perform and do not require any special operating system or command line knowledge.

Dashboard

After logging in to the Appliance, the initial screen is the **Mirth Appliance Dashboard**. You can navigate to this screen at any time by clicking the **System** menu or moving the cursor over the **System** menu and clicking on **Dashboard**.

The **Mirth Appliance Dashboard** page displays information about your Appliance and its current state. This information is important for monitoring how the system is operating. Some of this information is also necessary when contacting support.



The Dashboard includes System information

The **Dashboard** displays four areas of information: **System Status**, **Mirth Connect Messaging Totals**, **What's Running**, and **Current Resource Usage**.

- **System Status** displays version information for the Control Panel and for components and applications installed on the Mirth Appliance. These include the Appliance Version (the version of the Control Panel application) and a link for checking for updates to the Control Panel, the Java version, the PostgreSQL version, the Appliance's serial number, and the Appliance's uptime.

  The Appliance Version is the version of the Control Panel user interface. The **Check for Updates** link is a shortcut to the **Software Updates** feature (in the **System** menu).

  Individual versions are displayed for key software components such as Java and PostgreSQL, since it is often necessary to know the specific version of these components to ensure compatibility of channels, custom libraries, and custom databases.

  Uptime displays how long the Appliance has been running. This number will be reset each time the Appliance is powered on.

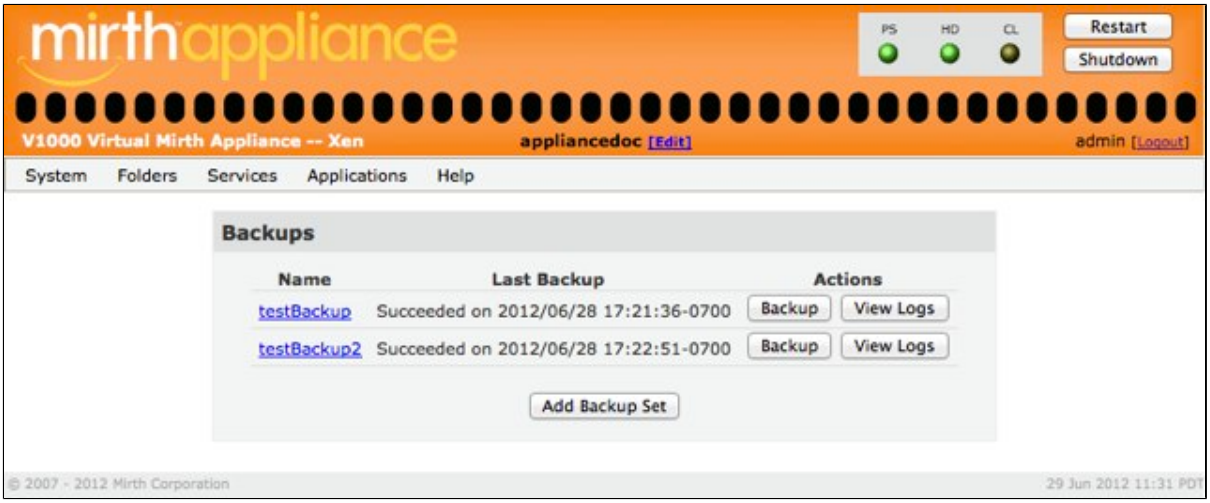
- **Mirth Messaging Totals** displays counts of the number of Mirth Connect messages received and how they have been processed: Received, Filtered, Queued, Sent, and Error.

- **What's Running** displays the services and applications currently installed and running on the Appliance. Items are displayed in green if they are currently enabled. Items are displayed in red if they are currently disabled. You choose what to enable or disable on the Services page.

- **Current Resource Usage** displays the Appliance's CPU load (as a percentage), hard disk usage (amount used/amount free), and memory (amount used /amount free). Each is graphed with counts.

> ⚠ ***Note:*** *Your Appliance's Serial Number, listed under* ***System Status****, is required when contacting Mirth support.*

Backups



Backups

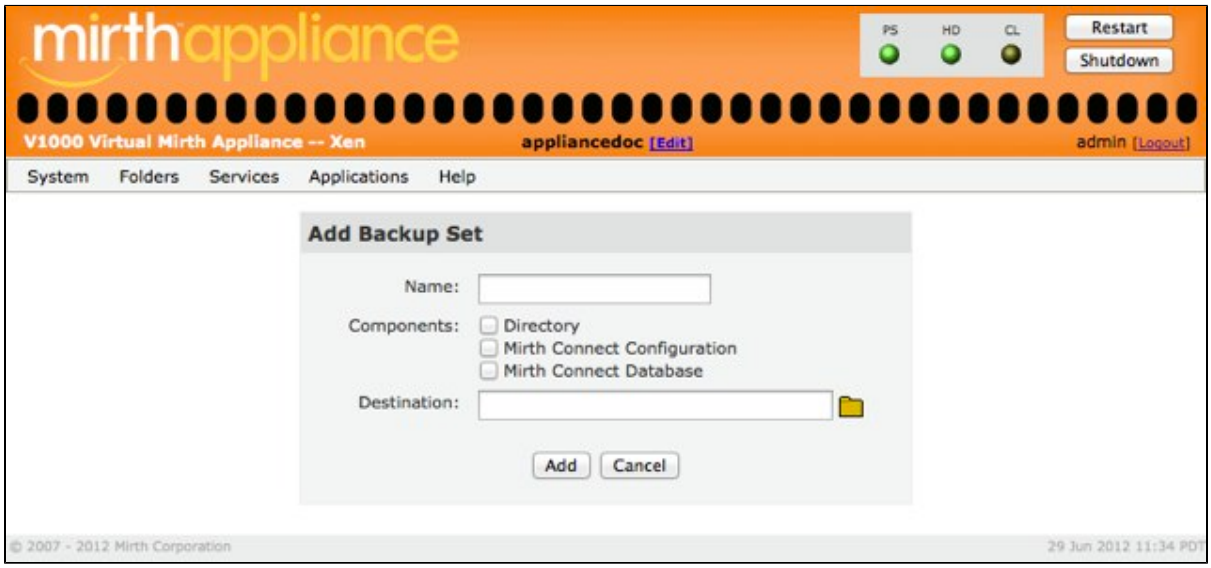
The **Backups** page allows you to create “backup sets” where you determine which data components are to be backed up and where the backup set will be saved. This page also allows you to manually run a backup for a backup set, to see the status from the last backup for each backup set, and to check the logs for a backup set.

Backup Sets

Backup Sets are collections of components with a given destination for the backup data.

To create a backup set, click the **Add Backup Set** button to go to the **Add Backup Set** page.

Give the backup set a name and select the components to include in the backup. Click the **Browse** link to select a destination folder.



Adding a Backup Set

> ***Note:*** *See Network Folders for instructions on creating network folders, to allow you to backup your data on network-accessible storage.*

Click the **Add** button to create the backup set.

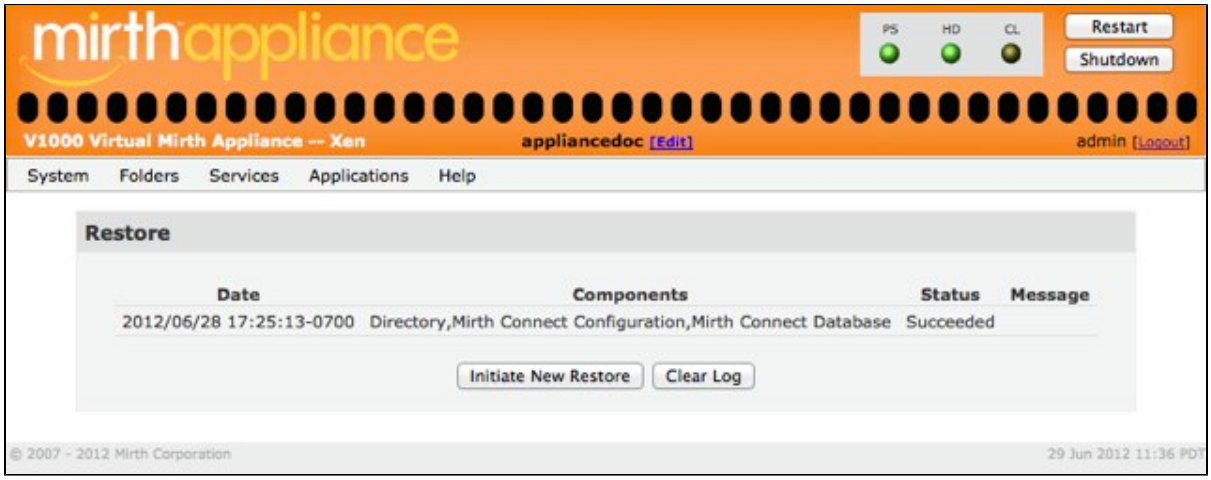
After you have created one (or more) backup sets, you can manually backup the backup set by clicking the **Backup** button to the right of the backup set name, or you can use the Auto Backup service to schedule regular backups (see **Auto Backup** under **Services**).

If you are using a network folder as the backup destination, the network storage location shows up as a folder name under the 'network' folder on the **/folders** page.

Backing up Mirth Connect allows you to quickly share Mirth Connect settings (transformers, filters, etc.) between Appliances. Create a network folder; backup Mirth Connect to the network folder; restore the backup data on another Appliance.

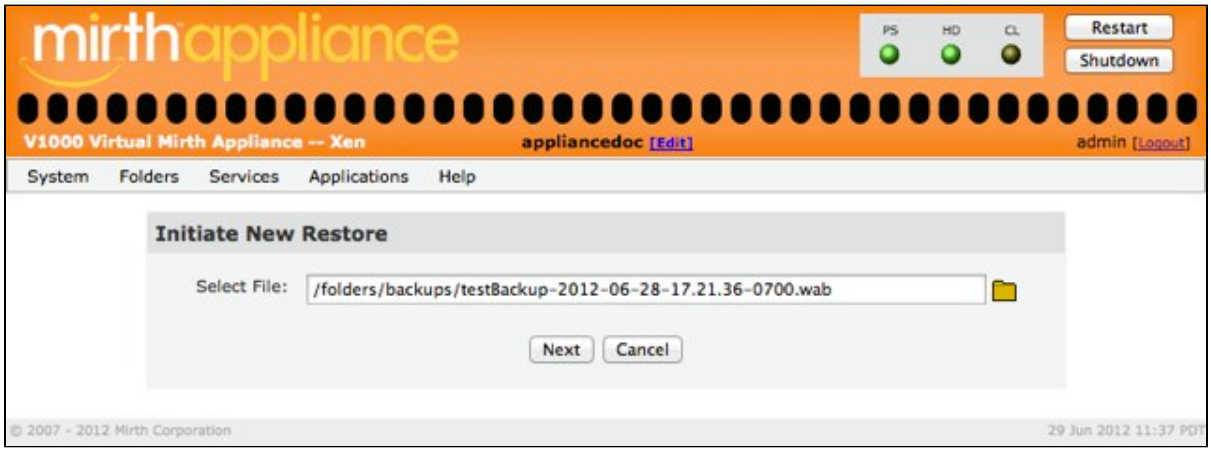
Restore

The **Restore** page allows you to select a backup to restore on the Appliance. When you restore a backup, you can select any or all of the components in the backup file's backup set to restore.



Restore

To begin the restore process, click the **Initiate New Restore** button.

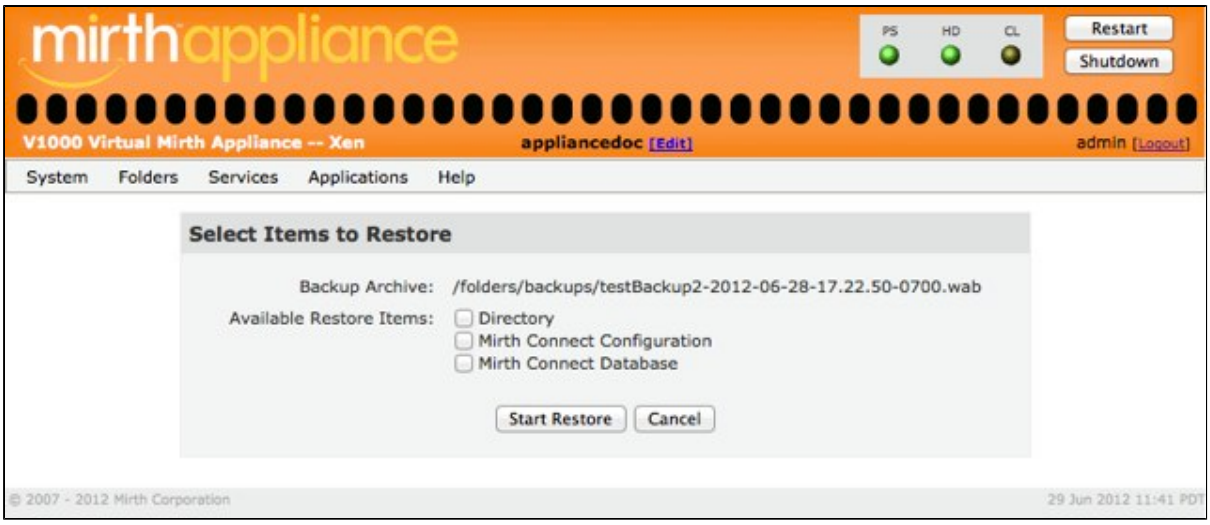


Initiating a Restore

Click the **Browse** link to browse the Appliance folders for a Backup set file. The Appliance opens a file browser to allow you to select a backup file from the Appliance folders (including network folders).

Select the backup file to restore (click on the file name). The Appliance will display the path and file name, allowing you to confirm your selection. To proceed, click **Next** (to select a different file, click the **Browse** link). To cancel the operation, click **Cancel**.

After clicking **Next**, the Appliance will allow you to select which components from the backup set to restore.



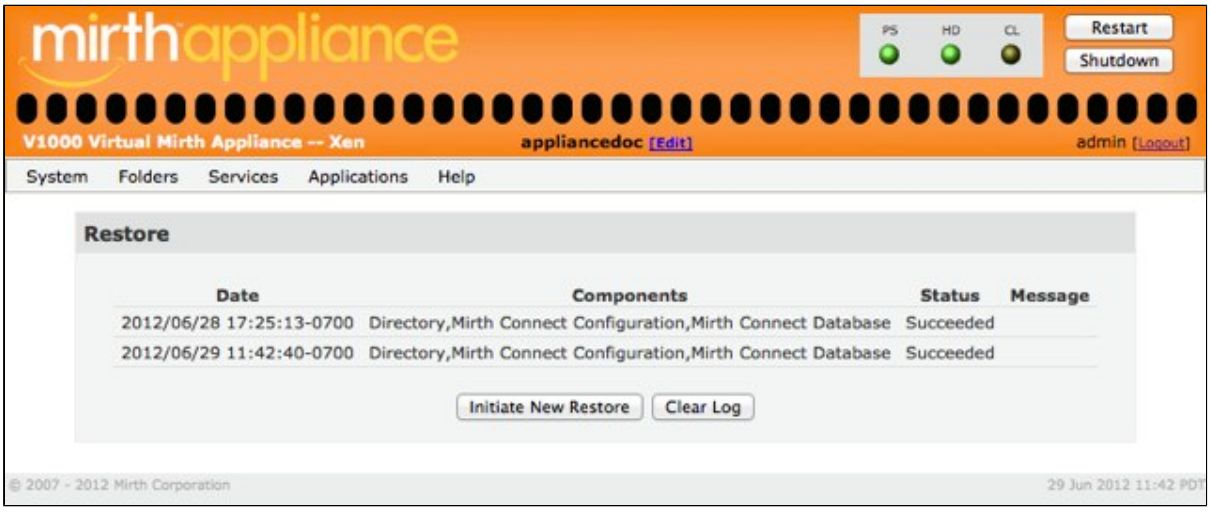
Select Items to Restore

You may select any or all of the available restore items.

> ⚠ If you are using Mirth Connect Clustering and Postgres Replication, in order to restore the **Mirth Connect Database** you first need to take the following steps:
>
> 1. Stop Mirth Connect on any node involved in a Mirth Connect Cluster and currently pointed to the database to be restored.
> 2. Stop all Postgres replication nodes currently streaming off the node that the restore will be occurring on.

Click **Start Restore** to execute the restore, or click **Cancel** to cancel.

The Appliance shows the progress of the restore process. When the process completes, the Appliance returns to the **Restore** page, adding a log entry for the most recent restore process.



Restore Page After Processing Restore

Software Updates

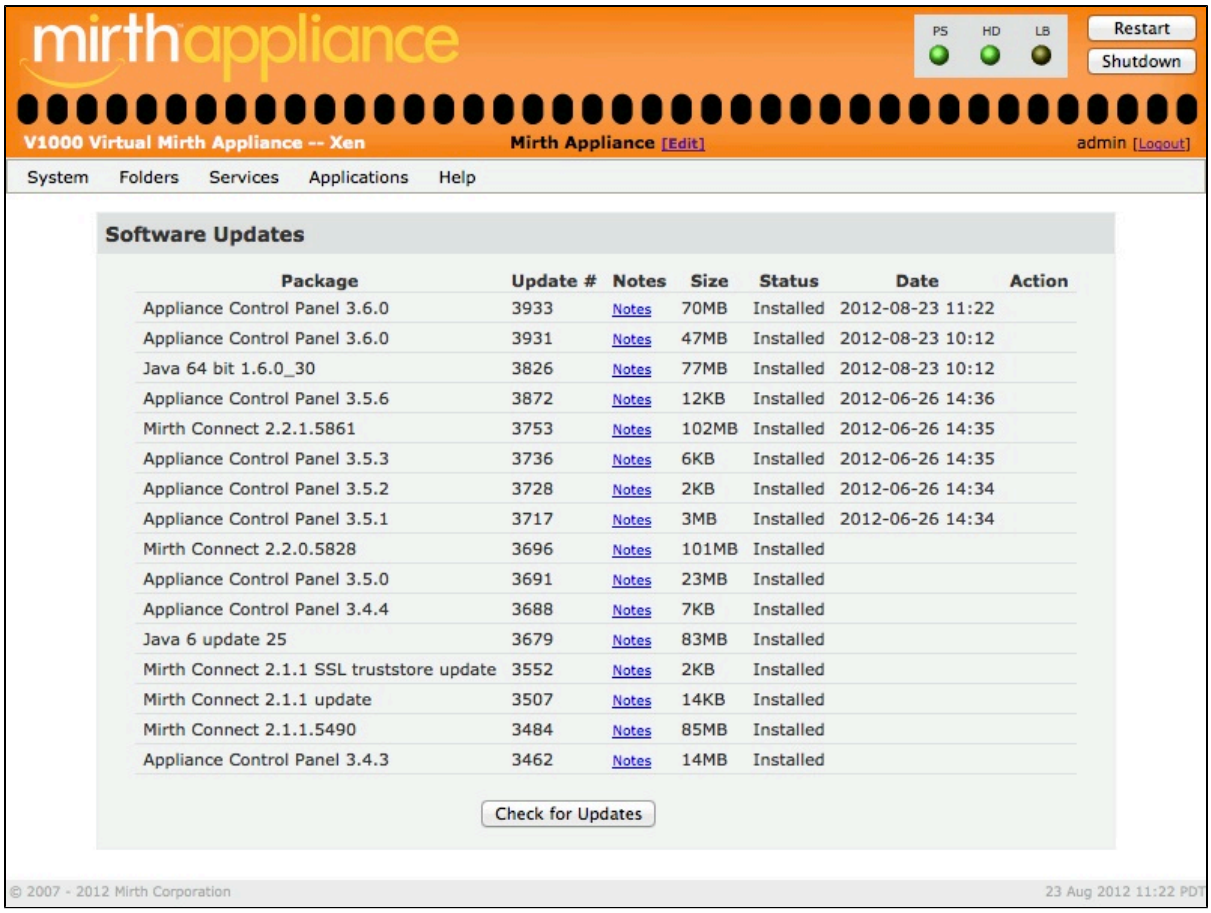
The Mirth Appliance is designed for easy updates to its internal software. Updates to Mirth applications, new features, bug fixes and security patches are all delivered online and controlled from the Appliance.

You can manually check for updates either by clicking the **Check for Updates** link on the Dashboard, or by selecting **Software Updates** from the **System** menu to go to the **Software Updates** page, and then clicking the **Check for Updates** button.

Updating the appliance is accomplished in several phases. First, the appliance will query the update server for available updates. While this process is running, the page will update with progress as each step is completed, and a status message will provide the number of available updates when the query is finished.

Check for Updates Page

Next, click **Okay** to proceed to the **Software Updates** page:



Software Update History

The **Software Updates** page displays a history of update activity on the Appliance. Each update in the history table shows the package name, release information, size, status, and the next action to take. The release information includes a version number and a link to the update's release notes.

The **Status** column lets you know if the update is available, downloading, ready to install, installed, or obsolete. The **Action** column contains a button if there is an action associated with the current state of the update. This allows you to control when updates are downloaded and installed. You can even suspend a large download and resume it later.

To check for updates, simply click the **Check for Updates** button and the Appliance will attempt to contact the update server over the Internet and see what updates are available for your system.

> ⚠ ***Note:*** *After you install an update, additional updates may become available. You should continue to check for updates until the Control Panel tells you there are no updates available.*

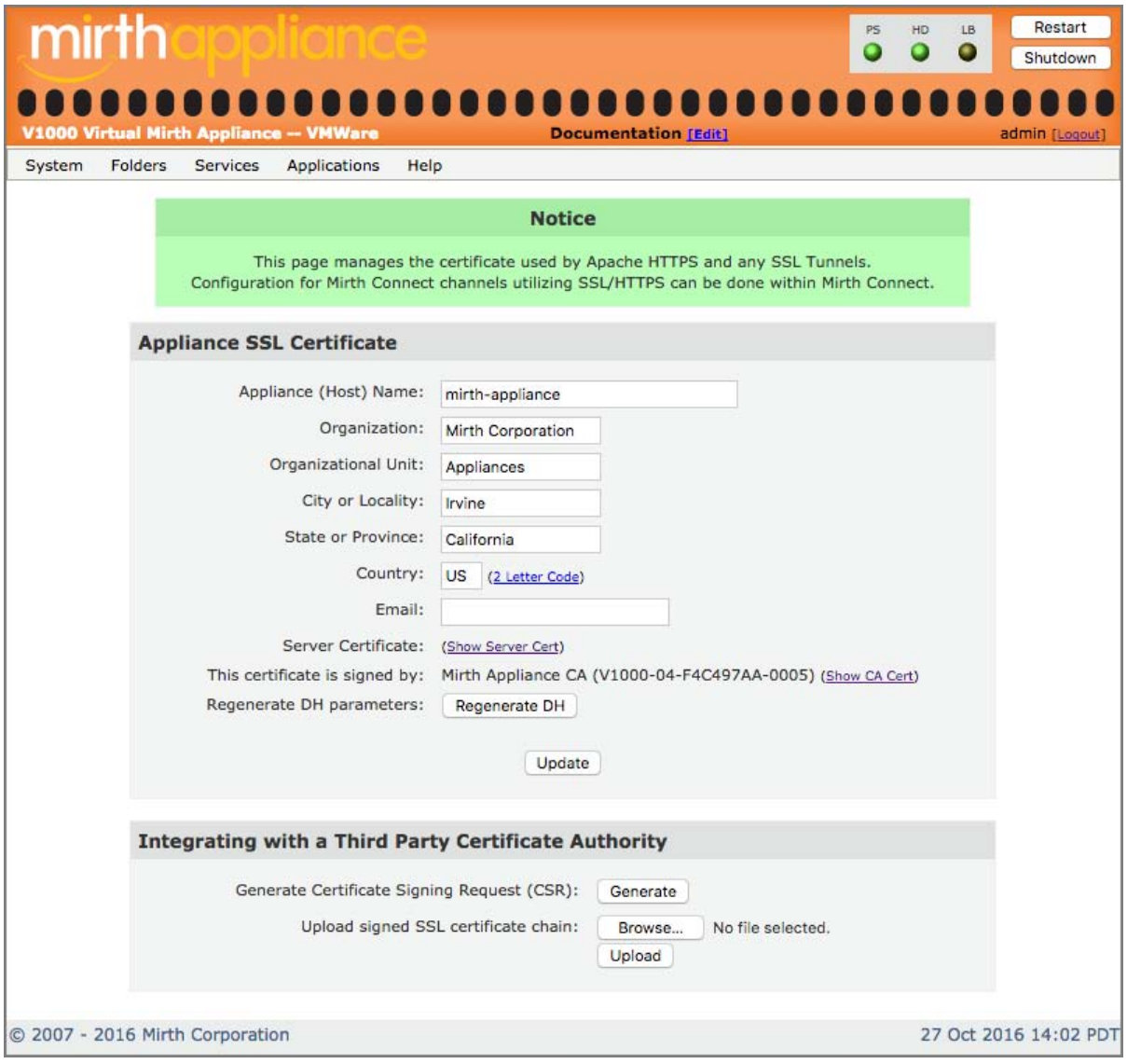
If an update is available, you will see a new entry at the top of the table and the past entries will be bumped down. Use the action buttons to complete the download and installation of the software.

When an update is installing you will see progress messages. When the installation is complete you will be redirected to the **Dashboard** page.

Certificates

Mirth Appliances ship with a local certificate authority and a default certificate installed. Although this will work out of the box, the remote side of the SSL connection may receive a message that the certificate doesn't match the site name, or that the certificate authority is untrusted. If this occurs, you can click the **Certificates** menu item in the **Systems** menu to modify the advanced certificate settings.

The **Appliance SSL Certificate** page with let you work with the local certificate authority, or prepare a certificate to be signed by a third-party authority.

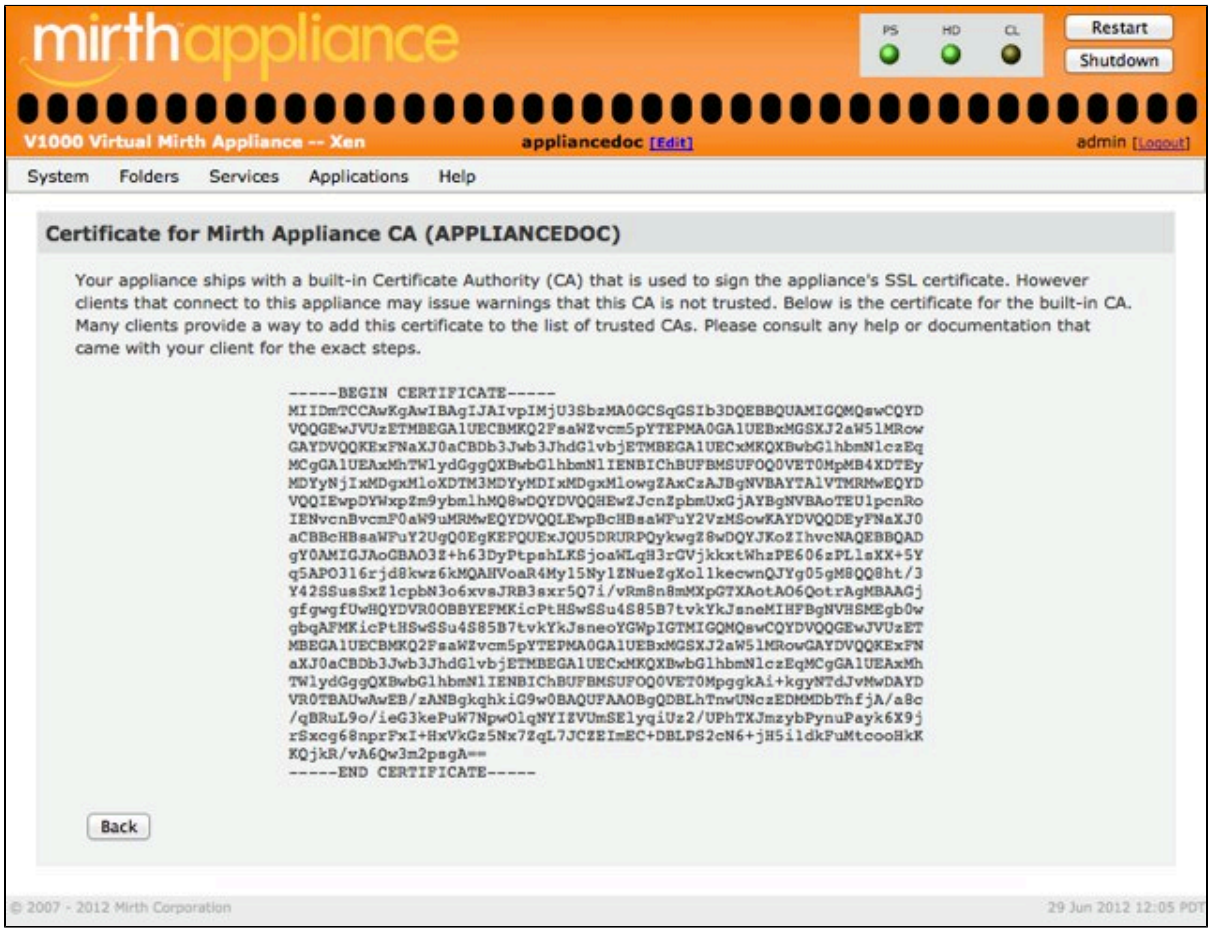


Mirth Appliance SSL Certificate Management

Using the Local Certificate Authority

To resolve an issue with a mismatched certificate name, update the new values for the Certificate on the **Appliance SSL Certificate** page. You can specify a new **Appliance (Host) Name**, **Organization, Organizational Unit**, **City or Locality**, **State or Province**, **Country, and Email**. The most important field is **Appliance (Host) Name** as this is the name that must match the DNS name referenced by the remote side of the SSL connection. Clicking the **Update** button after any change is made will cause the built in Certificate Authority to re-sign the local certificate. This process will replace the existing SSL certificate.

If the remote side of the SSL connection complains about not trusting the Appliance certificate authority, you can send them a copy of your CA certificate. They should be able to load this certificate into their software to tell it that you are a trusted source. To display this certificate, click the **Show_Cert** link on the **Appliance SSL Certificate** page, on the line that reads “This certificate is signed by: …”. You will be able to copy the certificate for distribution.

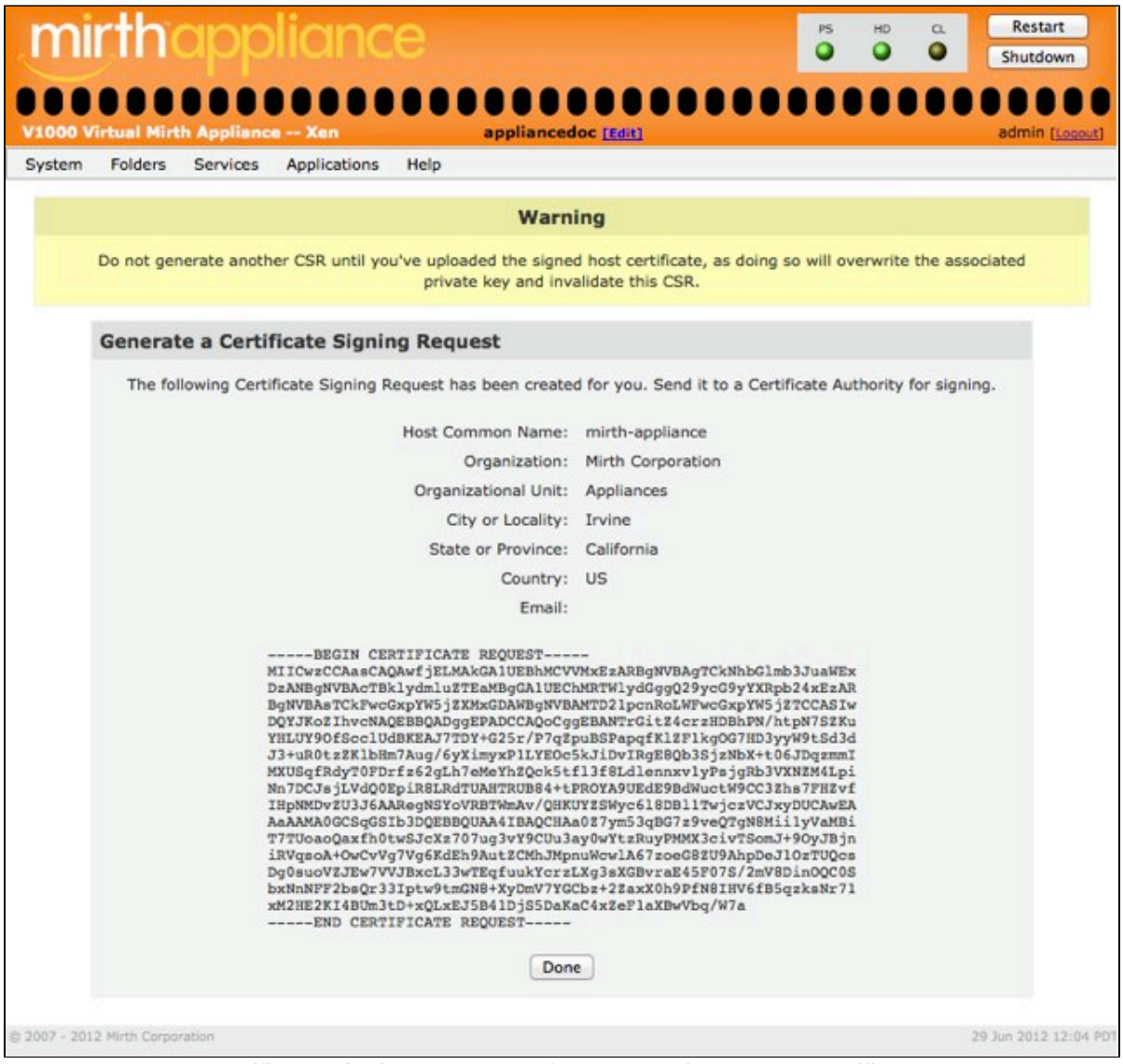


Displaying the Appliance's Certificate

Using a Third-party Certificate Authority

If it is necessary to use an SSL certificate from a well-known source such as VeriSign or GeoTrust, you can generate a certificate signing request. Enter the information that you would like to use in the designated fields of the **Appliance SSL Certificate** form, and click the **Generate** button. This will display a CSR that you can copy and use for your certificate order.

Pay close attention to the required fields and format guidelines as specified by your certificate authority of choice.



Certificate Signing Request, after Generating a New Certificate

> ⚠ ***Note:*** *Once you have created a CSR, do not repeat the process or generate another local certificate. Doing so will render the new third-party certificate invalid.*

When you receive the new signed SSL certificate from the third-party Certificate Authority, you will need to prepare a chain file and return here to the **Appliance SSL Certificate** page to upload it to the Appliance.

The file you will need to upload should include your signed certificate followed by any intermediate and root certificates, arranged in order from lowest-ranking to highest. To create this file, you can open a text editor (such as wordpad) and paste the entire body of each certificate into the file in the following order:

1. Your signed Certificate
2. The Intermediate Certificate (if any)
3. The Root Certificate

Make sure to include the beginning and end tags on each certificate. The result should look like this:

```
-----BEGIN CERTIFICATE-----
(Your signed certificate)
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
(The Intermediate certificate (if any))
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
(The Root certificate)
-----END CERTIFICATE-----
```

Save the combined file as *chain.pem*. Click the **Browse** button to select the file from your computer, and click the **Upload** button to apply the new certificate chain. This will replace the current SSL certificate, and the **Appliance SSL Certificate** page will display the new certificate information.

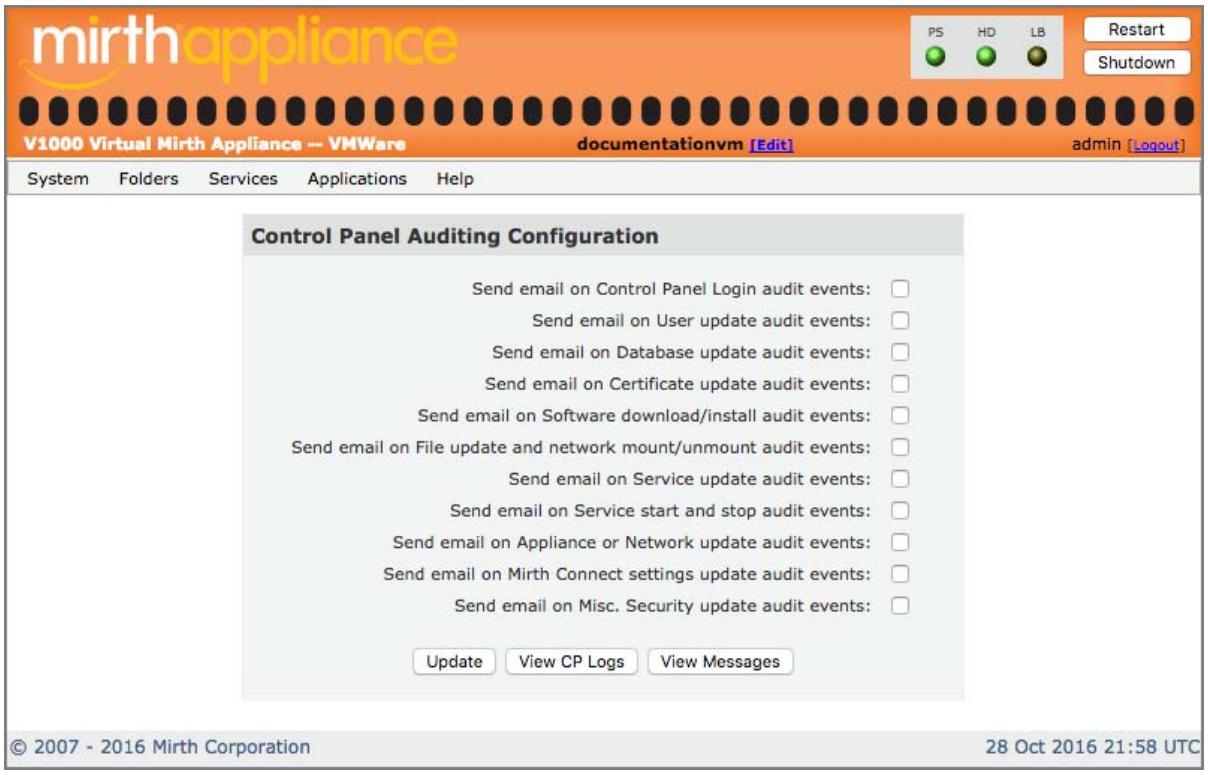
Remember that each Appliance requires a unique SSL host certificate. Attempts to upload a certificate from another host will fail, even if all of the information matches. Currently, the certificate settings do not affect the closed system of certificates used by the VPN servers.

Auditing

The Mirth Appliance Control Panel keeps an audit log of events such as logins, updates, downloads, installs, and the starting or stopping of services or applications. In addition to the entries in the log, email notices of these events can be sent to the notification addresses specified on the **Mail Configuration** screen.

There is also a log of error messages from the system, which includes the alert messages related to free disk space levels that can be set on the **Disk Free Space Alerts Configuration** page.

To go to the **Control Panel Auditing Configuration** window where you can access the audit log, the error/alert message log, and the auditing configuration settings, click the **Auditing** menu item in the **Systems** menu.



Configuring the audit-event-related emails

The configuration items on this page are checkboxes where you can indicate which types of audit events should have email notifications sent to the notification addresses specified on the **Mail Configuration** screen:

- **Send email on Control Panel Login audit events:**
  Email whenever someone attempts to log into the Control Panel.
- **Send email on User update audit events:**
  Email whenever someone adds or deletes users, updates user information, enables external LDAP authorization, or enables lockout and password restrictions.
- **Send email on Database update audit events:**
  Email whenever someone adds or deletes databases, enables or disables RO users, updates database information, or modifies Postgres settings.

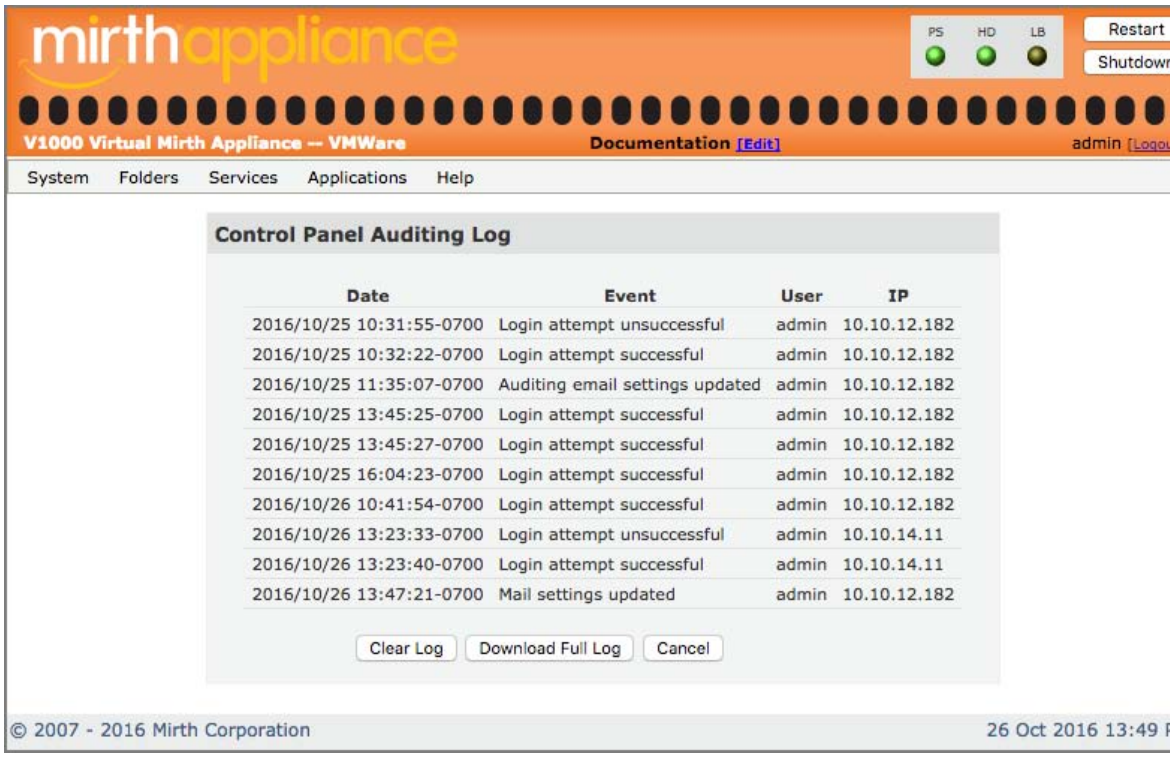
- **Send email on Certificate update audit events:**
  Email whenever someone generates a new CSR or uploads a new certificate or certificate chain.
- **Send email on Software download/install audit events:**
  Email whenever someone downloads or installs a software update.
- **Send email on File update and network mount/unmount audit events:**
  Email whenever someone uploads, downloads, or deletes a file, adds or deletes a folder, mounts a network folder or unmounts a network folder.
- **Send email on Service update audit events:**
  Email whenever someone add or deletes an SSL Tunnel, adds or deletes a VPN Connection, adds or deletes SFTP accounts, initiates a backup or a restore, or adds an IP to administer Glassfish.
- **Send email on Service start and stop audit events:**
  Email whenever someone starts or stops an application or service.
- **Send email on Appliance or Network update audit events:**
  Email whenever someone updates Network settings, Mail settings, Date and Time settings, or the serial number.
- **Send email on Mirth Connect settings update audit events:**
  Email whenever someone updates Mirth Connect settings.
- **Send email on Misc. Security update audit events:**
  Email whenever someone enables or disables console access, updates the console password, the SNMP settings, or initiates a shut down or restart of the Appliance.

When you check or uncheck one or more of these checkboxes, you then need to click the **Update** button to save the current settings.

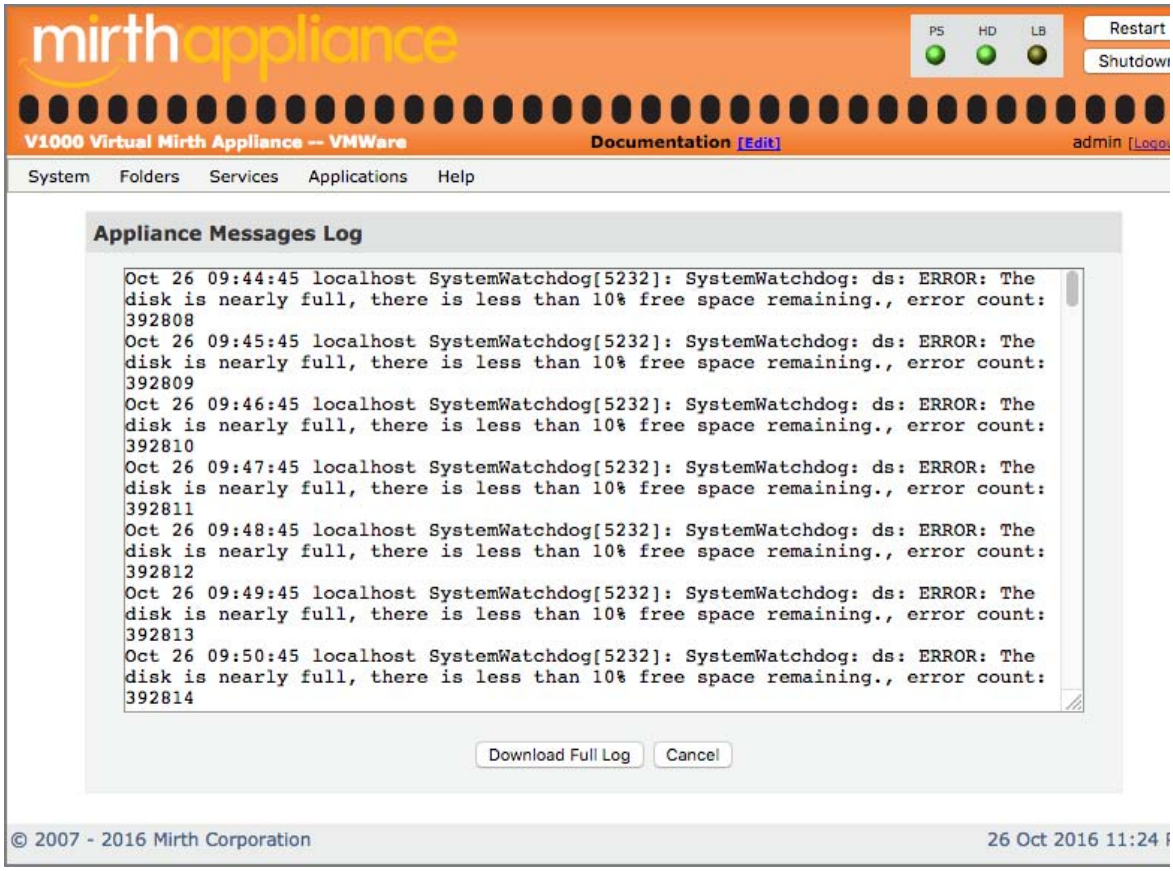
Viewing the logs

Next to the **Update** button are two buttons that allow you to view the logs:

- **View CP Logs** – click this button to view the **Control Panel Auditing Log**. On this page you can click the **Clear Log** button to delete the current entries in the log, or you can click the **Download Full Log** button to open a dialog to allow you to simply save the log in a file, or to save it and then open the saved file with a specified application. Clicking the **Cancel** button will take you back to the **Control Panel Auditing Configuration** window.

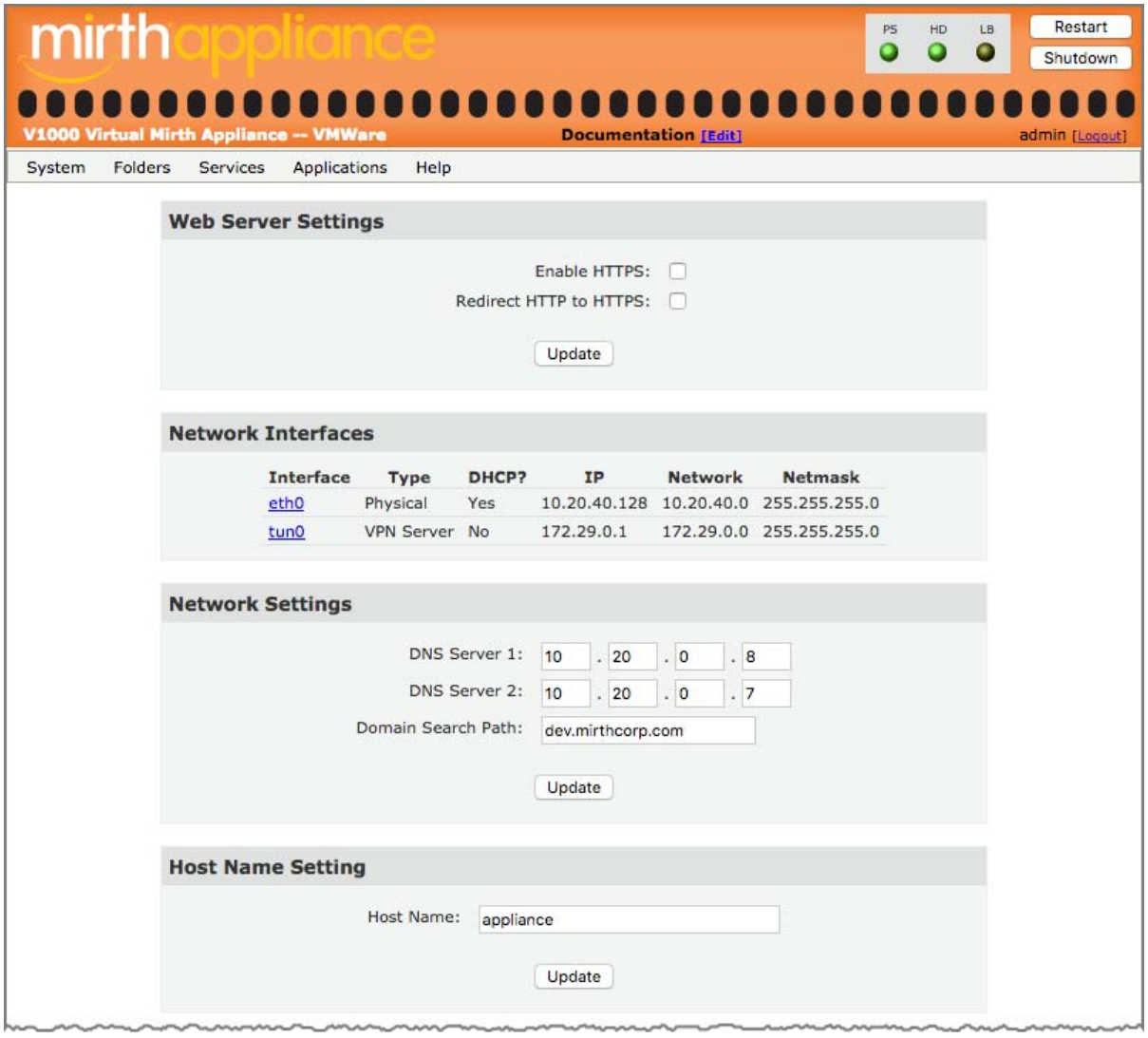


- **View Messages** – click this button to view the **Appliance Messages Log**. On this page you can click the the **Download Full Log** button to open a dialog to allow you to simply save the log in a file, or to save it and then open the saved file with a specified application. Clicking the **Cancel** button will take you back to the **Control Panel Auditing Configuration** window.

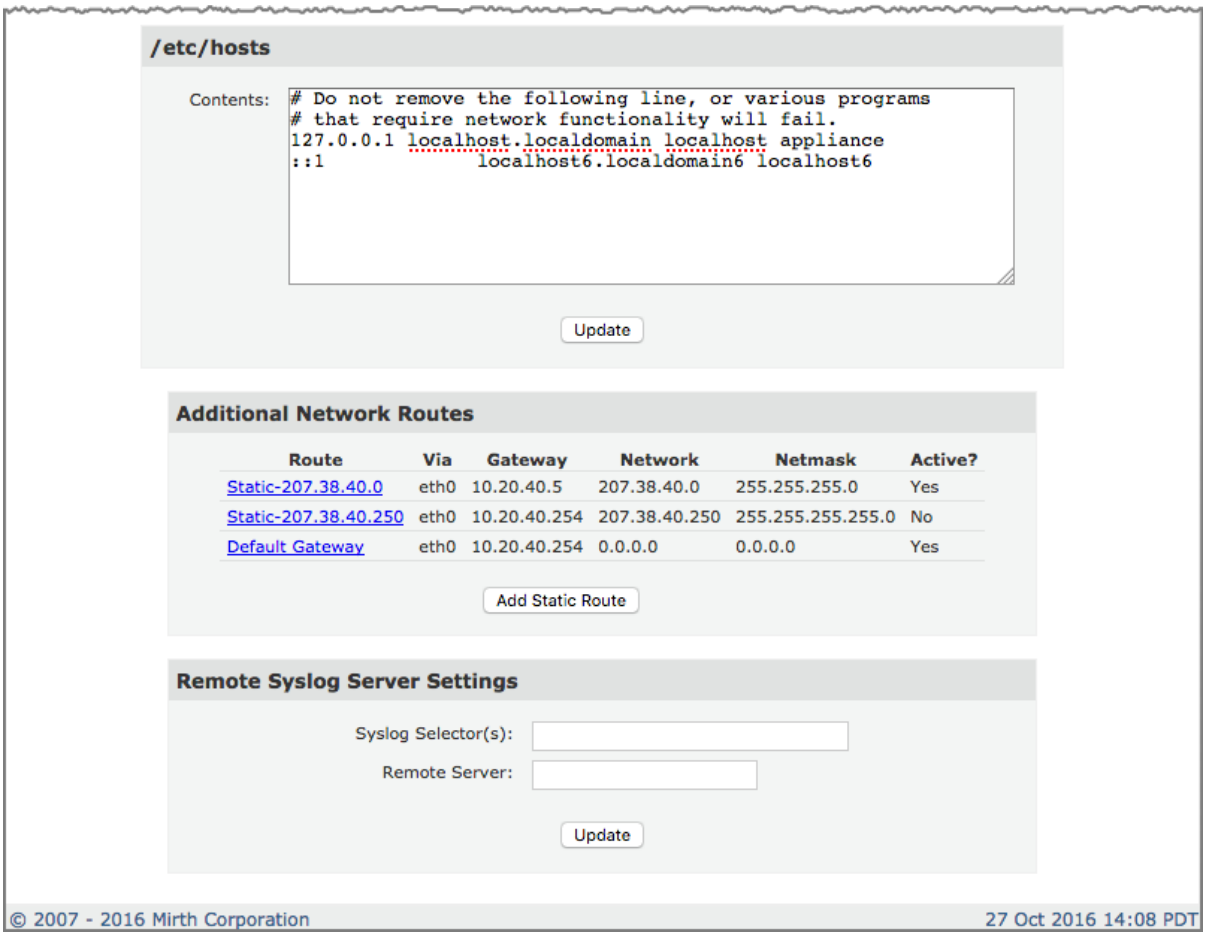


Network

Clicking the **Network** menu item in the **System** menu will access the network configuration settings. The top section presents HTTPS settings for the web server. The second section displays a view of the network interfaces. The third section presents current network settings. At the bottom are additional network routes.



Top section of page

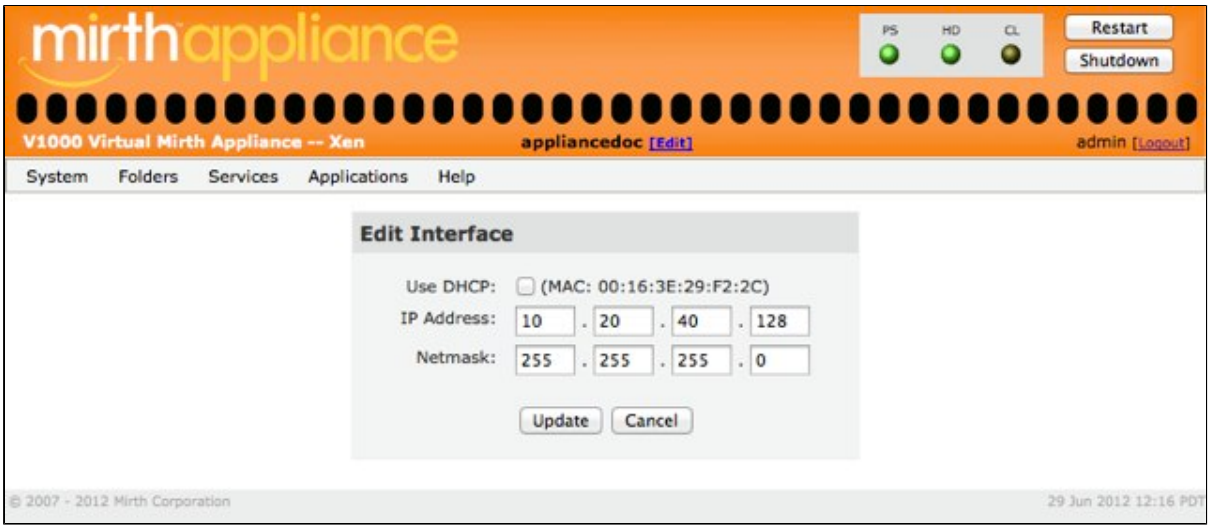


Bottom section of page

The Network Configuration page lets you adjust network and related settings.

By default network interfaces are configured using DHCP. To manually set the **IP Address** and **Netmask** values you must click the interface hyperlink.

Clicking on a **Physical** interface link will take you to the **Edit Interface** page where IP address and DHCP information is kept for that interface. Clicking on a **VPN Server** interface link will take you to the **VPN Server** services page.



Edit Interface page

> ***Note:*** *Using DHCP on either interface will overwrite manually set values for* ***Default Gateway****,* ***DNS Servers****, and* ***Domain Search Path*** *if your DHCP server provides these optional parameters.*

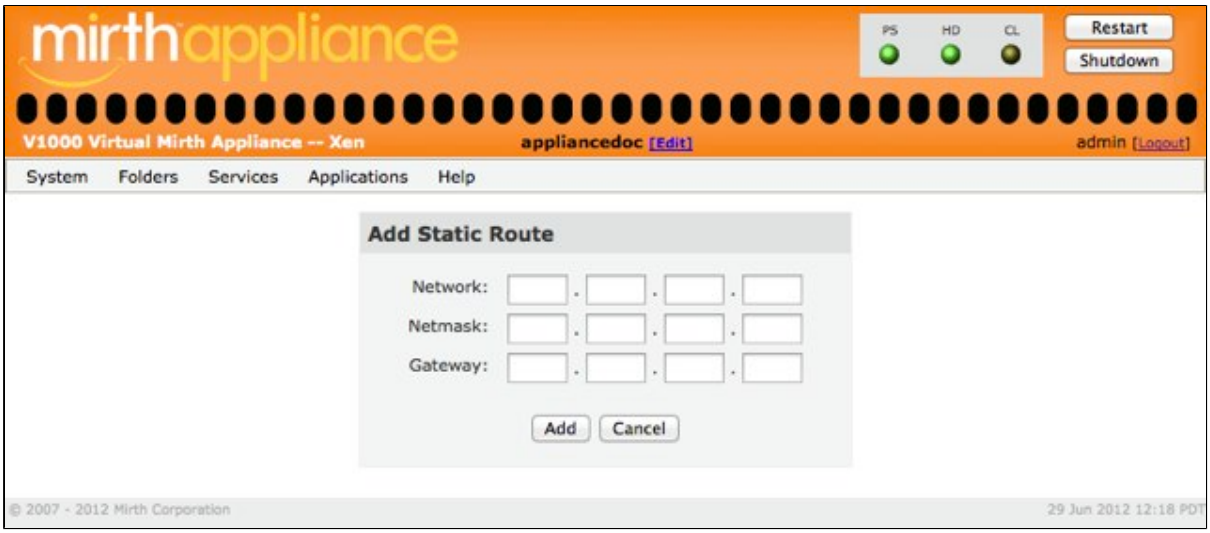
Network Settings section

The **DNS Server** addresses tell the Appliance where to look for translating domain names to IP addresses. These settings are required when using host names in channels and SSL tunnels, and also for all e-mail delivery.
The **Domain Search Path** is the default domain that is appended to hostnames when forming a fully qualified domain name. This will usually be the local domain for your internal network.

Additional Network Routes section

The **Default Gateway** represents the path used to connect to other networks. It is usually a router or firewall address, and it must always be directly accessible from at least one of the Appliance network interfaces.

To add or manage static routes click the **Add Static Route** button. You will be able to set the network, netmask, and gateway IPs.

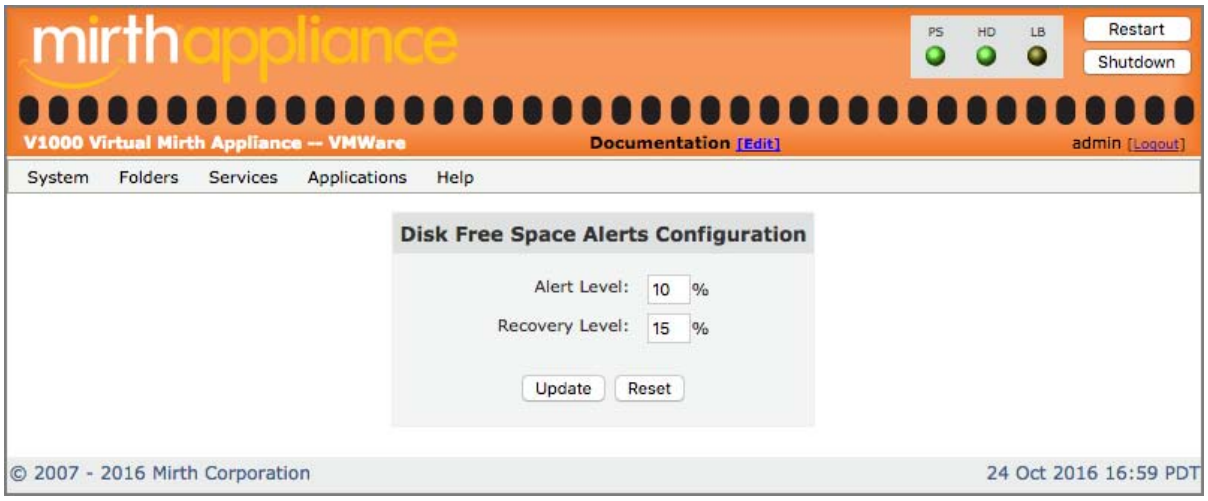


Static Routes

Alerts

Having some free disk space on your Appliance is important, so an alert is sent if the free space falls below a certain level. After this happens, another alert message will be sent when disk space is freed up so the amount of free space has risen back above another certain level.

In order to configure the designated levels at which these alerts will be sent, click the **Alerts** menu item in the **System** menu to access the **Disk Free Space Alerts Configuration** page.



There are two items that can be set on this page:

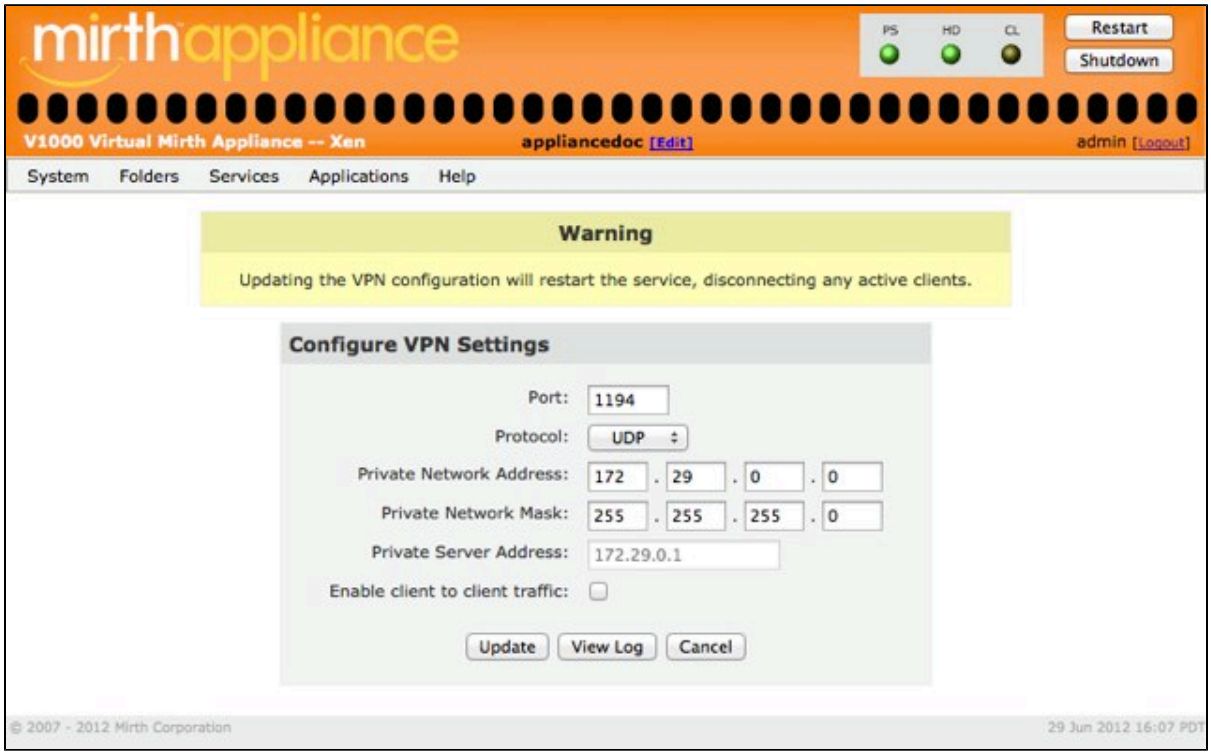
- **Alert Level** – When the free disk space goes below this level, the Appliance will send you an alert via email. Be sure you have an email recipient set under **System > Mail**, **Notification Email Address**. The default is 10%.
- **Recovery Level** – After going under the Alert Level, when the free disk space returns to a value above this Recovery Level, the Appliance will send you a notification via email. The default is 15%.

After making a change to either or both of these values, click the **Update** button to save the new values.

If you type in some new values but then change your mind, or realize that you have made a typo, you can click the **Reset** button to return the two values to the last values that were saved using the **Update** button.

VPN Server

The Mirth Appliance has the ability to terminate VPN connections for various uses. You can use a VPN tunnel to administer the Appliance or use it to pass HL7 traffic for Mirth Connect. Different clients connected to the VPN server can talk to each other through the appliance by selecting the **Enable client to client traffic** checkbox. This is also known as IP forwarding.



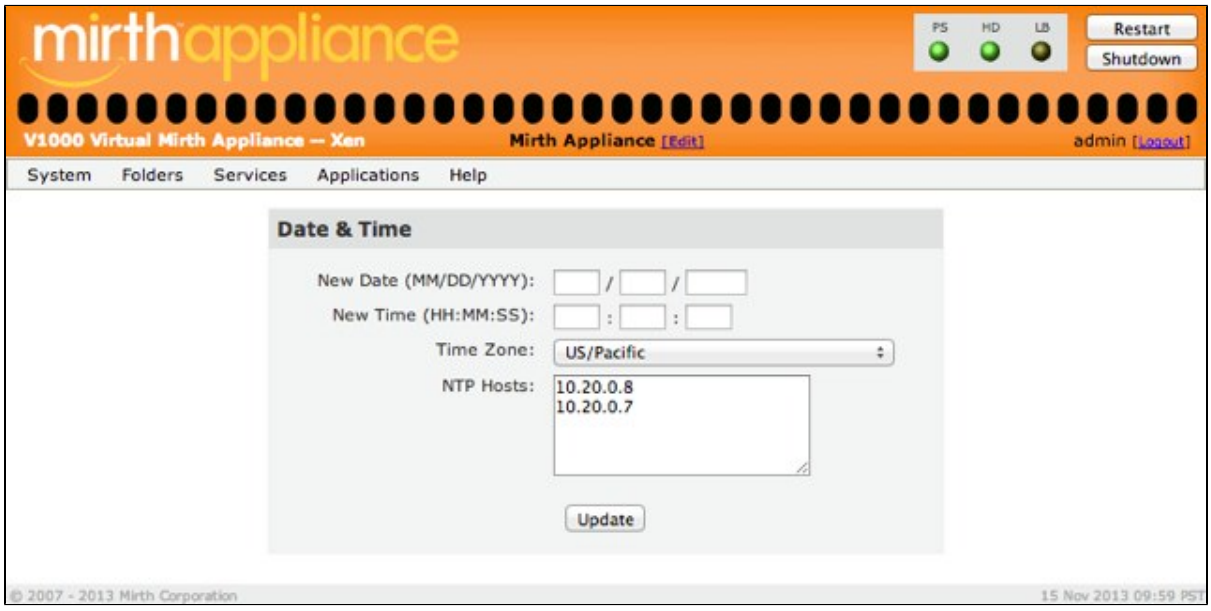
Configuring VPN Settings

Date & Time

The Appliance's date and time are set via network time protocol (NTP). A default setting for public NTP Hosts is provided, but you may want to use NTP servers on your local network. Ask your network administrator if there is a preference.

> ⚠ ***Note:*** *When you make changes to the* ***Time Zone****, you will need to stop and start the Mirth Connect Server for the changes to fully take effect.*

When you configure your Appliance for the first time, you will want to specify the local time zone, via the **Date & Time** page.



Date & Time

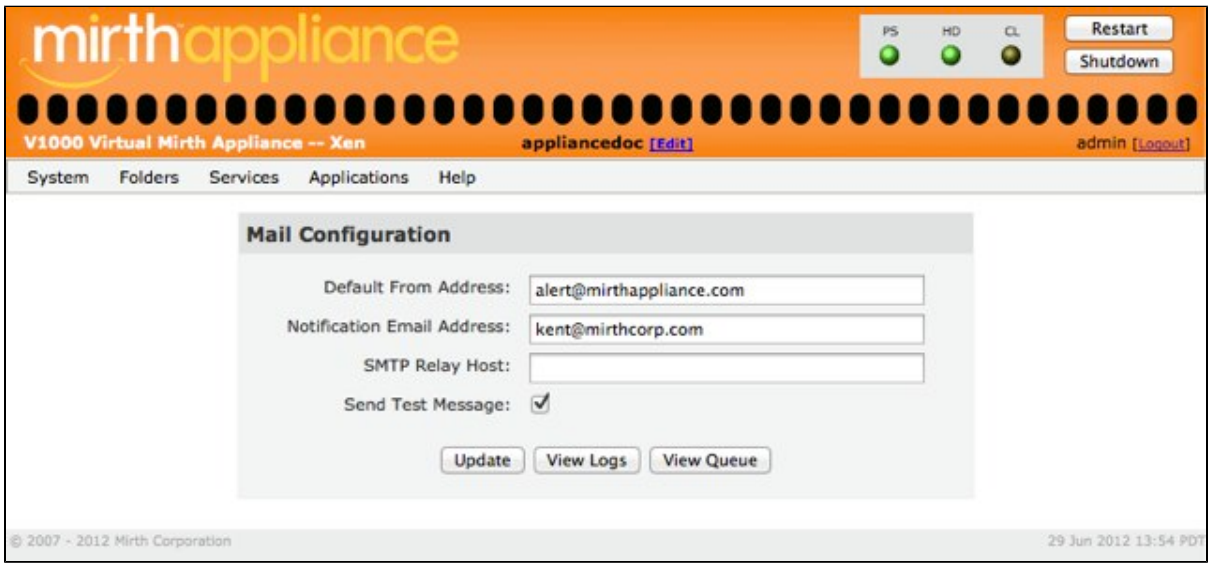
Select your time zone from the pull-down **Time Zone** menu. Use the provided public NTP server in the **NTP Host** field or enter your own. Click the **Update** button to accept the new settings.

Mail

The **Mail Configuration** page allows you to set one or more email notification addresses in the **Notification Email Address** field. To set more than one address, separate each recipient by a comma.

Enter an email address in the **Default From Address** field to identify messages sent from the Appliance. The default from address is alert@mirthappliance.com.

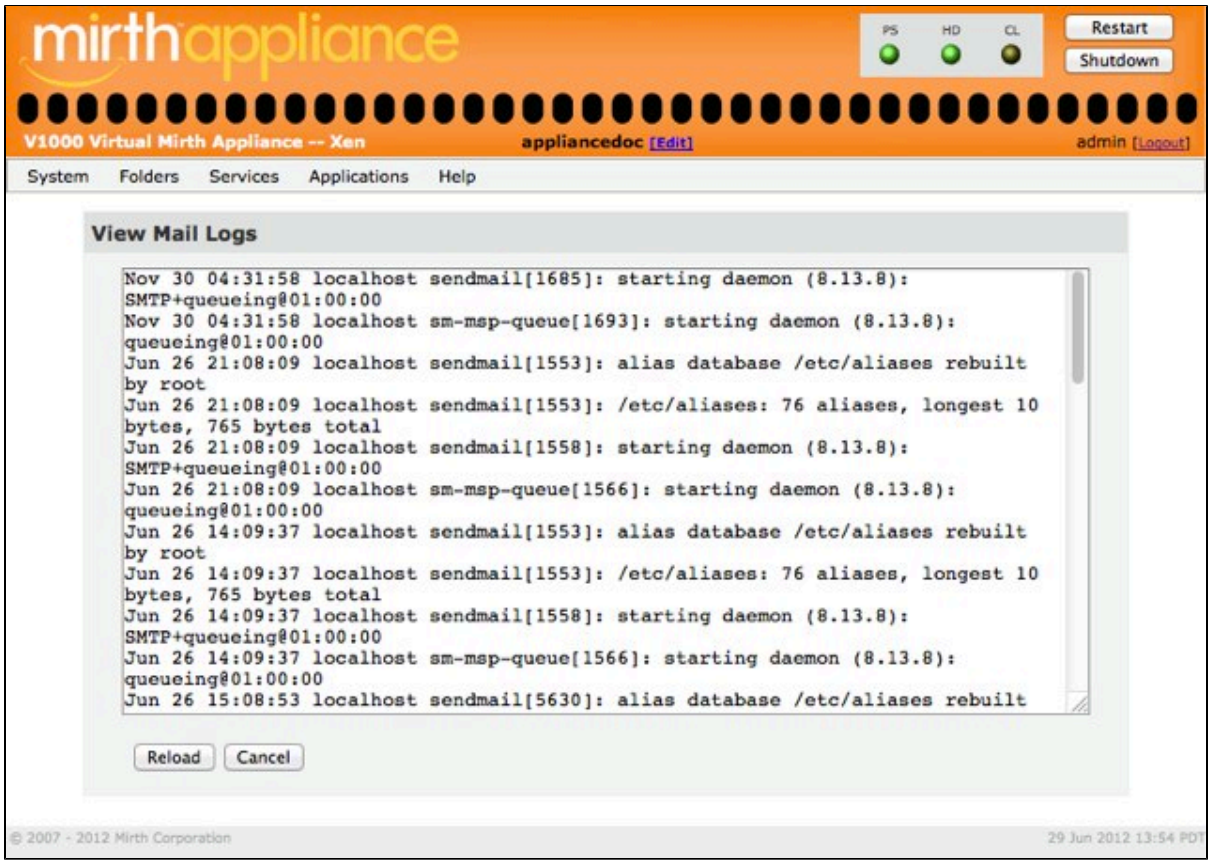
When the **SMTP Relay Host** field is blank (the default value), the Mirth Appliance will attempt direct mail delivery. This setting is the most reliable, but requires outbound network access on TCP port 25. If your network restricts outbound SMTP traffic you will need to talk to your network administrator either to open access for the Appliance or to provide you with an authorized SMTP relay host. You can reference the host by name or IP address.



Mail Configuration

If the **Send Test** Message checkbox is checked (which it is by default), then a test message will be sent to the notification email address(es) when the **Update** button is clicked. This will confirm that the Appliance is capable of sending emails which reach the notification recipients.

The **View Logs** and **View Queue** buttons allow you to view the mail logs and mail queue. The Mail Log keeps a running log of sent emails:



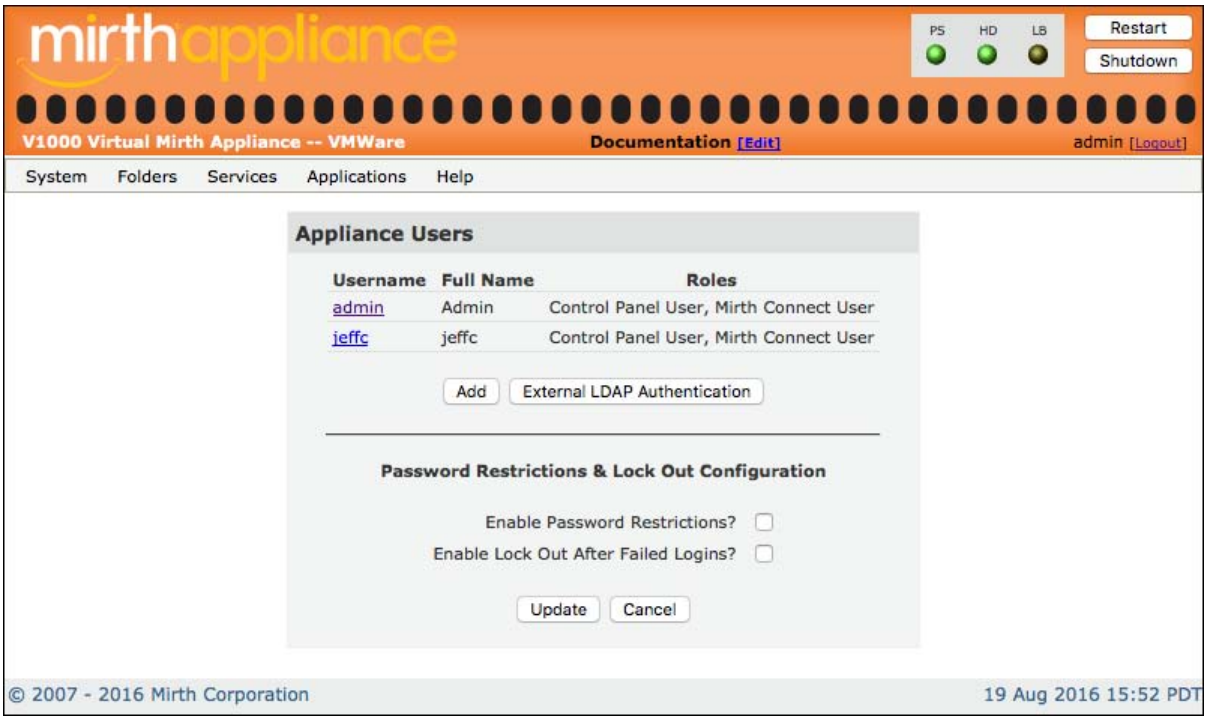
View Mail Logs

The Mail Queue lists all notification emails waiting to be sent:

View Mail Queue

The **Reload** button will refresh the queue to display the most recently queued emails. To clear any queued emails click the **Clear** button.

Users



Control Panel Users

Selecting **Users** under the **System** menu will take you to the **Appliance Users** page. On this page you can click the **Add** button to add a new user, or click the name of an existing user to edit or delete that user. You can also click the **External LDAP Authentication** button to go to a page where you can configure the ability to log in to the Control Panel using accounts from an external LDAP server.

In addition, there is a section where you can enable password restrictions and the locking of user accounts after a certain number of failed login attempts.

These actions are discussed further in the following sections.

Password Restrictions and Lock Out Configuration

Check the **Enable Password Restrictions?** box to require that new passwords (for new users or for existing users changing their passwords) must follow this set of standard rules:

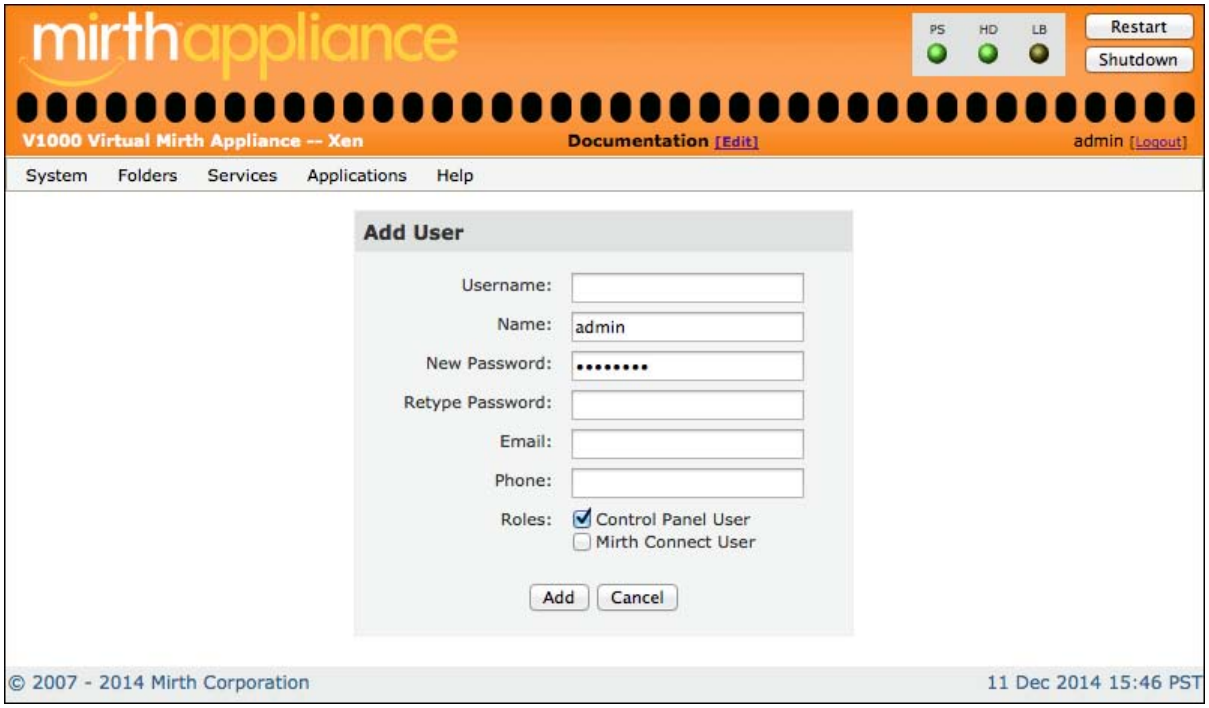
- password characters are limited to letters, numbers, hyphens, and underscores
- passwords must be eight or more characters long
- passwords must contain at least one letter
- passwords must contain at least one number

If some passwords were created previously when the password restrictions were not enabled, and then the restrictions are enabled, users with existing passwords that do not meet the restrictions can continue to use their non-conforming passwords.

Check the **Enable Lock Out After Failed Logins?** box to enable the locking of user accounts after the number failed login attempts reaches a certain number. Checking this box also makes two more items appear that allow you to configure aspects of this lockout process:

- **Number of Failed Login Attempts Allowed** – the number of failed login attempts which will cause the user account to be locked. The default is 5 attempts.
- **Lock Out Time** – the length of time that the user account will be locked after reaching the threshold of failed login attempts. After this time the user can once again try to log in. The default is 30 minutes.

Adding a User



Add a User

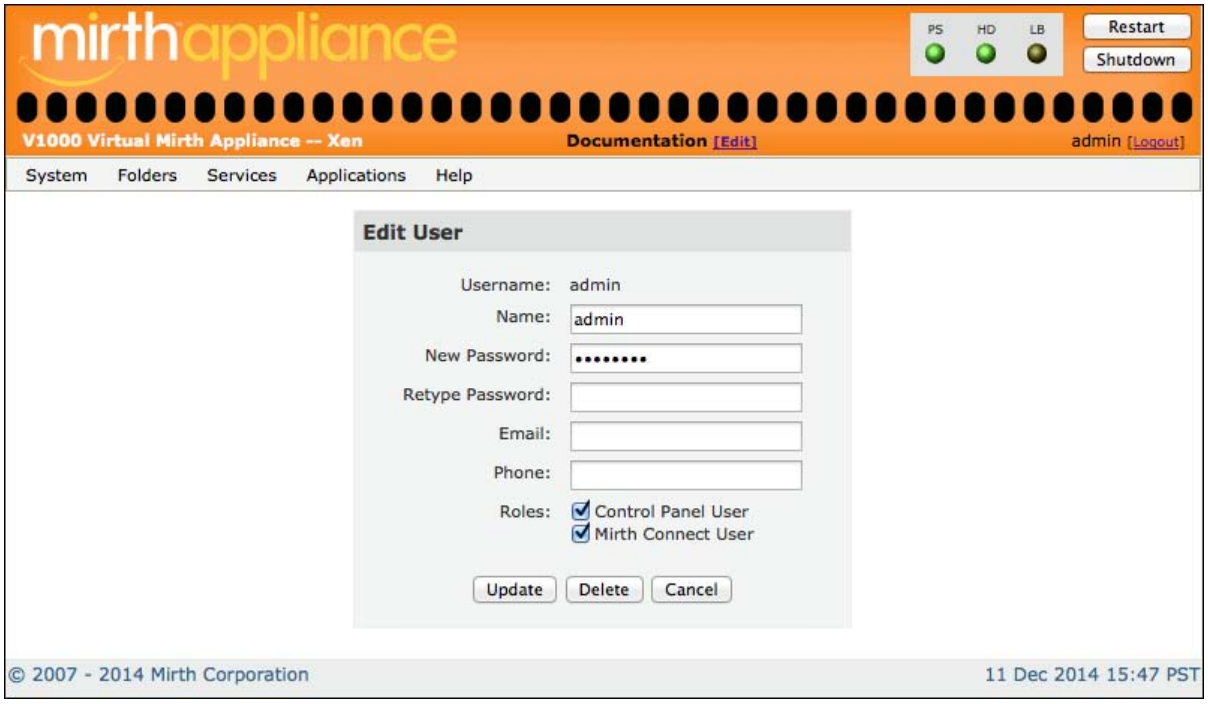
Clicking the **Add** button opens the page. To add a user, enter a username, the user's full name, a password, and confirm the password by entering it again. You can also add the user's email address and phone number.

Under **Roles**, you can set the privileges this user has for the Appliance. If you select the **Mirth Connect User** checkbox, you will also synchronize the user account with Mirth Connect Administrator.

> ⚠ ***Note:*** *Creating a user in the Mirth Connect Administrator will not allow you to create an Appliance User.*

Click the **Add** button to add the new user; click the **Cancel** button to return to the **Appliance Users** page without adding the new user.

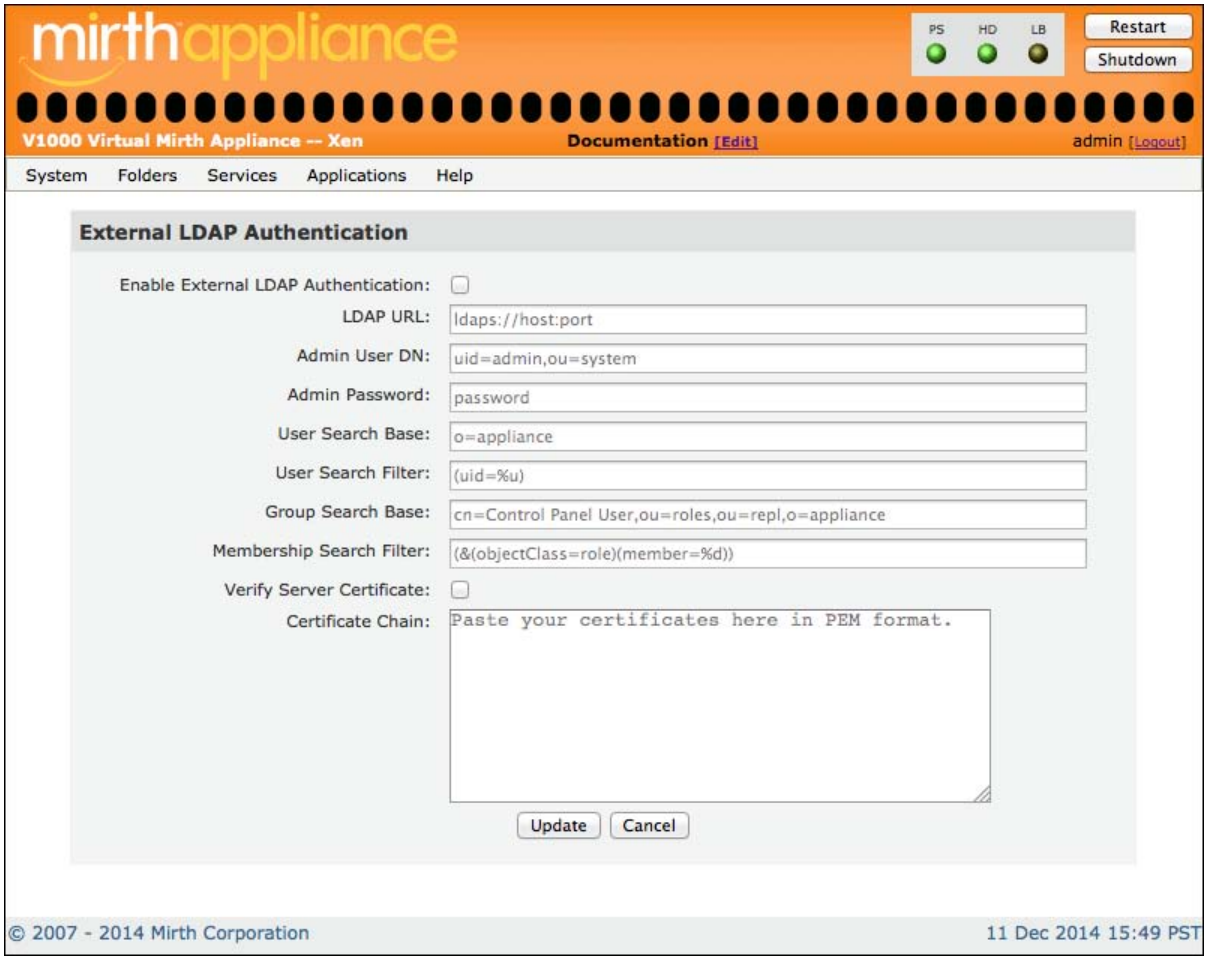
Editing or Deleting a User



From the **Appliance Users** page, click on an existing username to edit or delete the user. From the **Edit User** page you can change a user's full name, their password, their options and their roles. Make any changes and click the **Update** button to save the changes; click the **Delete** button to remove the user (click **OK** in the confirmation dialog to complete the deletion or click **Cancel** to cancel the deletion); or click **Cancel** to return to the **Appliance Users** page without making any changes.

> ⚠ ***Note:*** *Deleting an Appliance User account that had the Mirth Connect User option selected when it was created will not delete the cloned account in the Mirth Connect administrator.*

External LDAP Authentication



The **External LDAP Authentication** page allows you to use logins from an external LDAP server to log into the Control Panel.

> ⚠ ***Note:*** *The local "admin" user will always be able to get in using his regular credentials even if the external LDAP server is inaccessible.*

Example values for the inputs on this page are given in the table below, and you can consult your local network administrator for the appropriate values for your environment. The **Group Search Base** and **Membership Search Filter** inputs are optional; these can be used to restrict which user accounts are able to log into the Control Panel.

Example values for integrating with Active Directory:

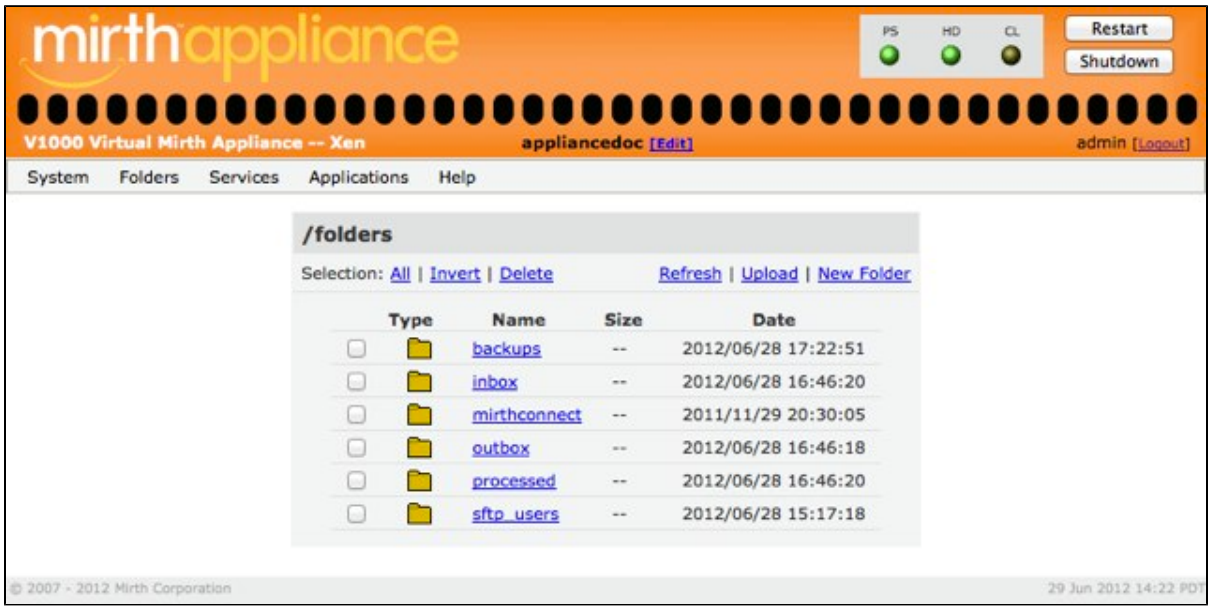
Field	Example Value	Note
LDAP URL	ldap://w.x.y.z	Replace w.x.y.z with the IP or hostname of your Active Directory server.
Admin User DN	CN=Administrator,CN=Users,DC=example,DC=local	Provide a valid DN.
Admin Password	password	Provide a valid password.
User Search Base	OU=Accounts,DC=example,DC=local	Replace as necessary.
User Search Filter	(&(objectCategory=person)(sAMAccountName=%u))	This should work as-is.
Group Search Base	CN=Control Panel Users,OU=Users,OU=Accounts,DC=example,DC=local	This field is optional, to restrict logins to users in the Control Panel Users group.
Membership Search Filter	(&(objectclass=group)(member=%d))	This should be provided if a Group Search Base was provided. If so, this value should work as-is.
Verify Server Certificate	Checked or unchecked	This is optional, and toggles certificate-based verification the AD server.
Certificate Chain	A PEM-encoded certificate	Ask your AD administrator to obtain this certificate.

Folders Menu

The Mirth Appliance Control Panel allows for easy file management of user accessible folders (directories) via the **Folders** menu. Click the **Browse** menu item to access the file manager. Click the Network Folders menu item to manage network folders.

Browse

Navigate into a folder by following the linked folder name. Click the **Back Arrow** button ( ) to leave the current folder and go up one level. Use the **Upload** link to upload a file to the current folder. Click the **New Folder** link to add a folder to the current directory.



The Folders page, at the root folder

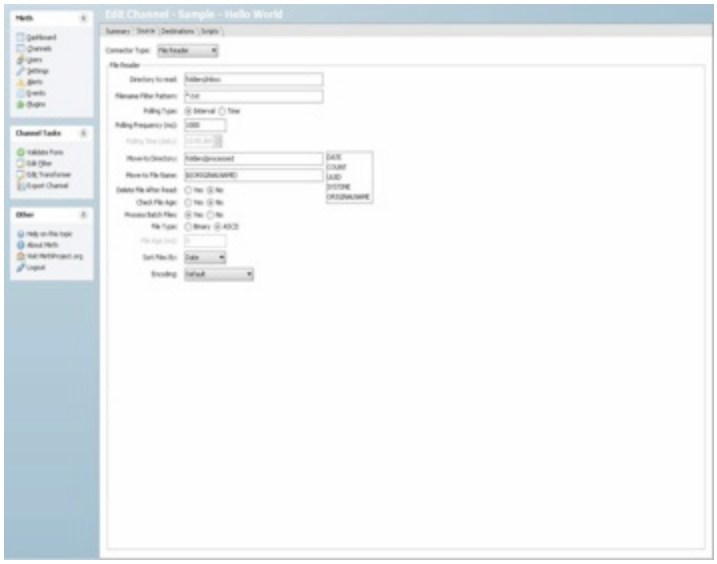
Select all the files in a folder (check all the checkboxes) by clicking the **All** link; de-select all the files by clicking the None link. Reverse the selected/unselected checkboxes by clicking the **Invert** link; delete the selected files by clicking the **Delete** link.

Default Folders

The default folders on the Appliance have different purposes. Some folders are used by Mirth Connect, others are used by services on the Appliance.

> ⚠ ***Note:*** *The inbox, outbox, and processed folders are default locations used by the test channel that comes with your Mirth Appliance. Deleting any of these folders will cause the test channel to fail.*

You can use these same folders for your own channels, or you can create new folders. The current path is displayed in the gray rectangle above the Selection links; that is the path you would use when referencing the directory in a Mirth Connect channel.



Sample channel using the folders on the local file system of the Appliance.

When multiple channels use the same folder, you should specify a **Filename Filter Pattern** that will ensure that only one channel will attempt to process a given file.

SFTP User Folders

The "jailed" file systems for each SFTP user appear under the *sftp_users* folder. There is a separate folder for each SFTP username, and a number of directories under each. The folder for each SFTP user, and the sub-directories described below, are only created after the SFTP user is created.

The *bin*, *etc*, *lib*, and *usr* directories are required for proper operation of the users "jail" in the SFTP server. The user's default directory is the *files* folder. Here you will see the same *inbox*, *outbox*, and *processed* folders that they see when logged into the SFTP server.

Mirth Connect Message Queue

The *msg_queue* folder is the location for outgoing Mirth LLP messages that have been queued for delivery. If messages fail to deliver, you may need to delete the files in this folder to free disk space.

Special Mirth Connect Folders

The *custom_conf* and *custom_lib* folders are used by Mirth Connect for customizing and extending its functionality. New database drivers and custom Java code in these folders can be referenced from within Mirth Connect. See the Mirth Connect documentation or contact your assigned Mirth Engineer for details.

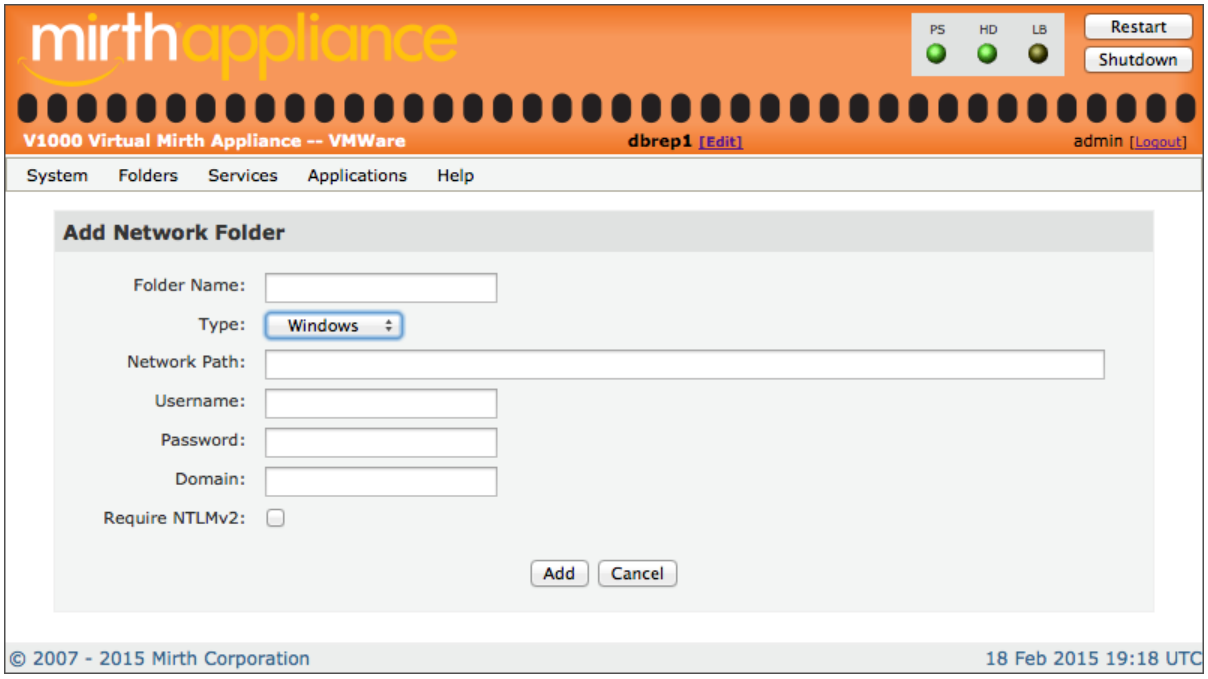
Network Folders

The **Network Folders** menu item allows you to manage network folders.

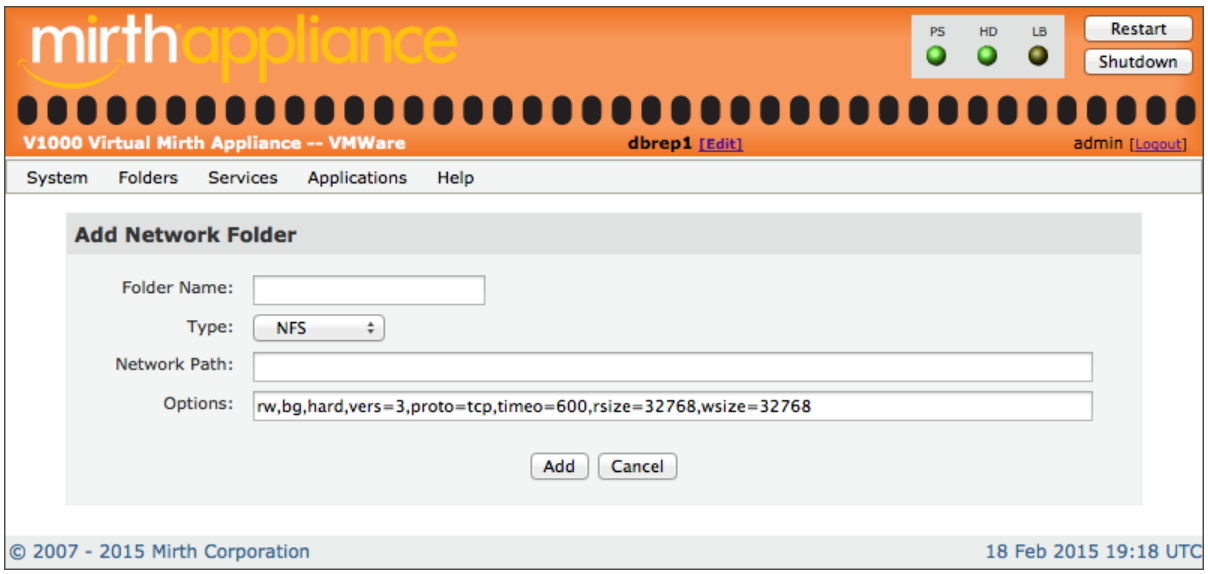
Manage Network Folders

If network folders have been created, they will be displayed on this page. The network folder's name (under **Local Path**) is a link which will open the folder. A **Delete** button will be displayed under **Action**. Click the **Delete** button to remove the network folder.

To create a network folder, click the **Add Network Folder** button.



Add Network Folder, Windows



Add Network Folder, NFS

On the **Add Network Folder** page, provide the following:

- ***Folder Name:*** the local name for the network folder. The name cannot contain any spaces or special characters.
- ***Type:*** the remote server file system. Choose *Windows* for Windows or Samba, or *NFS* for Unix/Linux.
- ***Network Path:*** Network path you wish to attach to. For a Windows share, the format should be: //serverNameOrIP/ShareName. For a NFS export, the format should be ServerNameOrIP:/path/to/mount

If *Windows* is selected as the **Type**, the following fields also appear:

- ***Username:*** Windows user name for Windows share
- ***Password:*** Windows password for Windows share
- ***Domain:*** Windows Workgroup or Domain name; Optional
- ***Require NTLMv2:*** Require NTLMv2 (NT LAN Manager version 2) password hashing; Optional

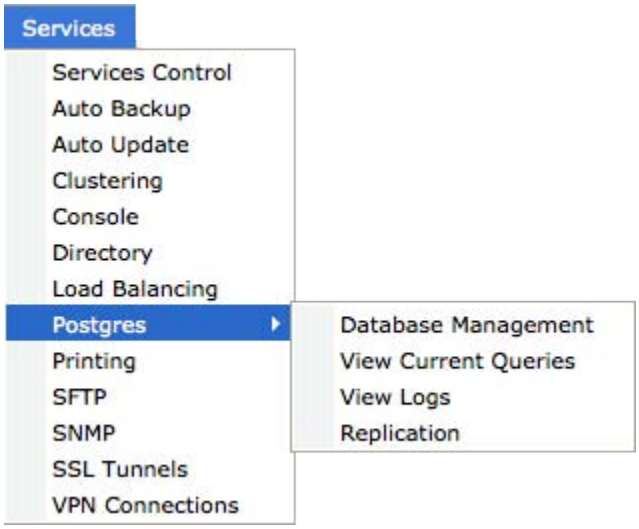
If *NFS* is selected as the **Type**, the following field also appears:

- ***Options:*** a comma-separated list of attributes for the folder. The default options are appropriate for most customers. If you have problems connecting, consult your local network administrator or Mirth Support.

Fill in the fields and click the **Add** button to create the Network Folder, or click **Cancel** to return to the **Manage Network Folders** page.

After adding a network folder, you can find it in the Folder Browser, under the network directory.

Services Menu

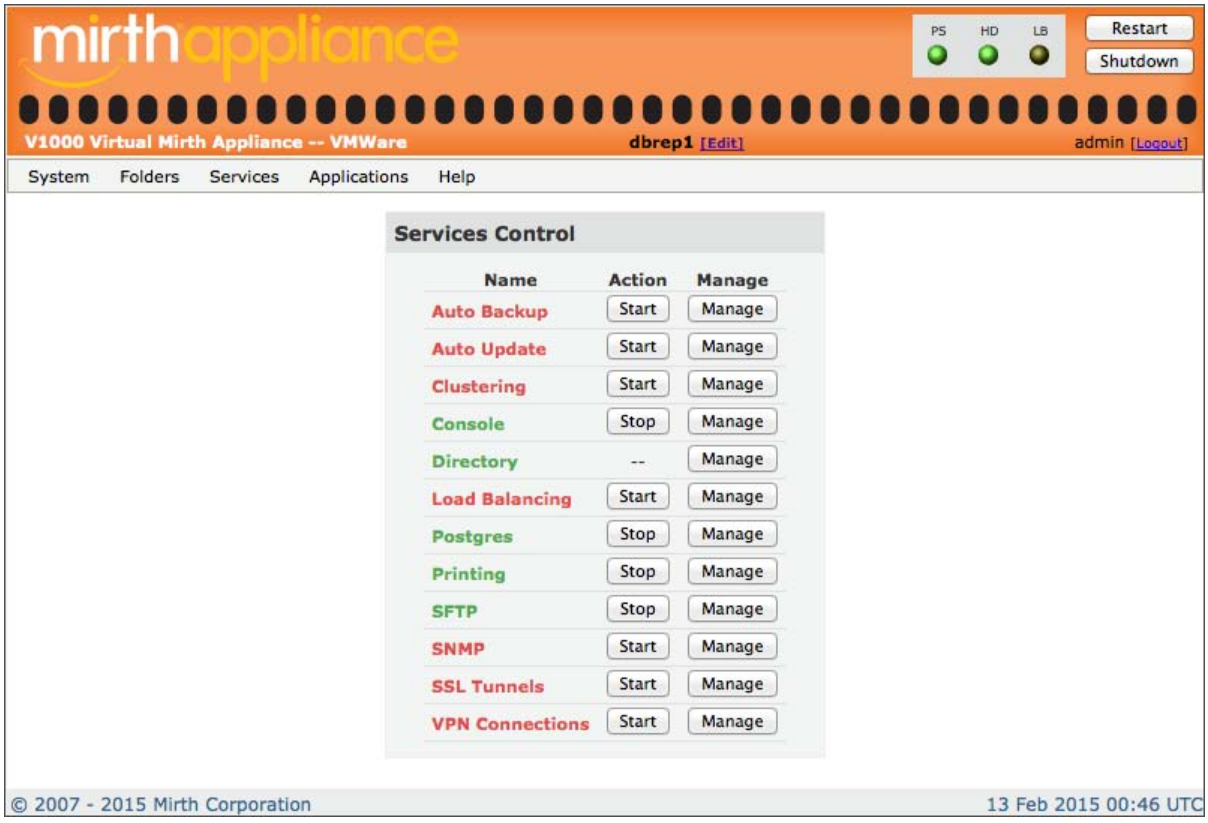


⚠ When one of the Mirth enterprise applications (Match, Results, Care, Mail, etc.) is installed, a **Glassfish** entry will also appear here on the **Services** menu, but it is not part of the default installation.

It is also possible that multiple Glassfish entries may appear in the **Services** menu when you have multiple applications installed, because they may have separate Glassfish instances.

Services Control

Mirth Appliances include a number of components that add features and functionality to the Appliance, in addition to any applications installed on the Appliance. The components, as well as the applications, are managed as services via the Control Panel. Clicking the **Services** menu or the **Services Control** menu item brings up the **Services Control** page.



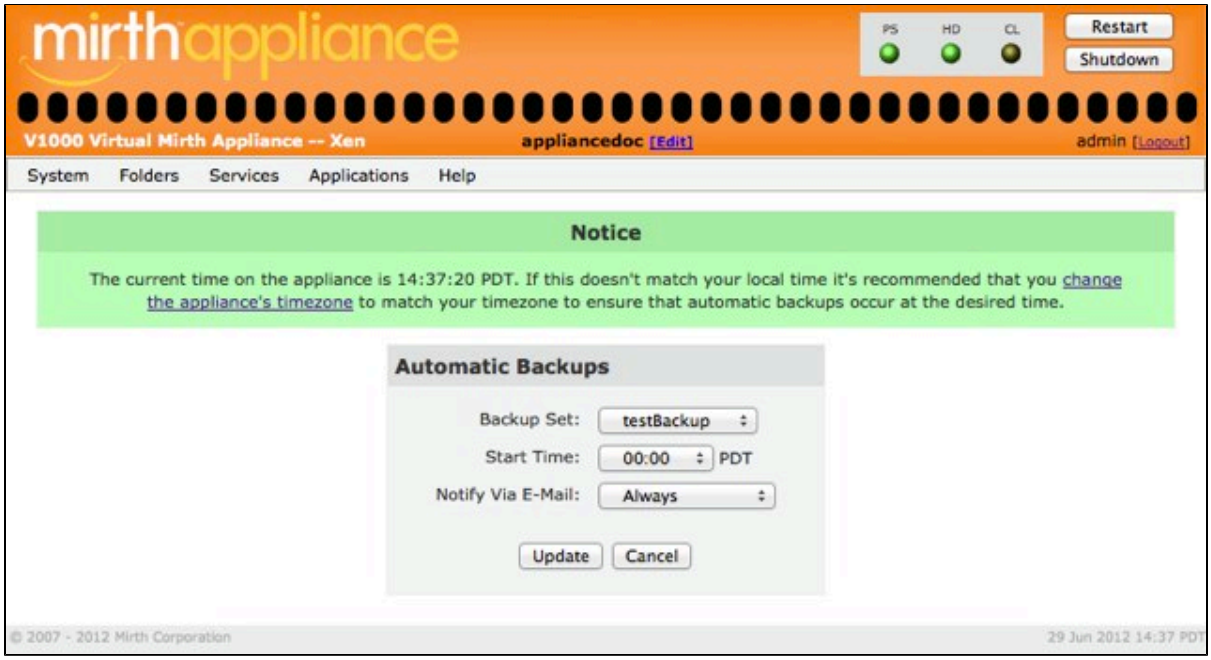
Services Control

From this page, you can view each of the services installed on the Appliance and whether they are running or stopped. A service displayed in green is running; a service displayed in red is stopped. To start a service that is stopped, click the **Start** button. To stop a service that is running, click the **Stop** button.

Click the service's **Manage** button to configure or manage a service.

Auto Backup

The Auto Backup service allows you to configure automatic backup operations. Select a backup set, a start time, and a notification option, and then click the **Update** button**.**

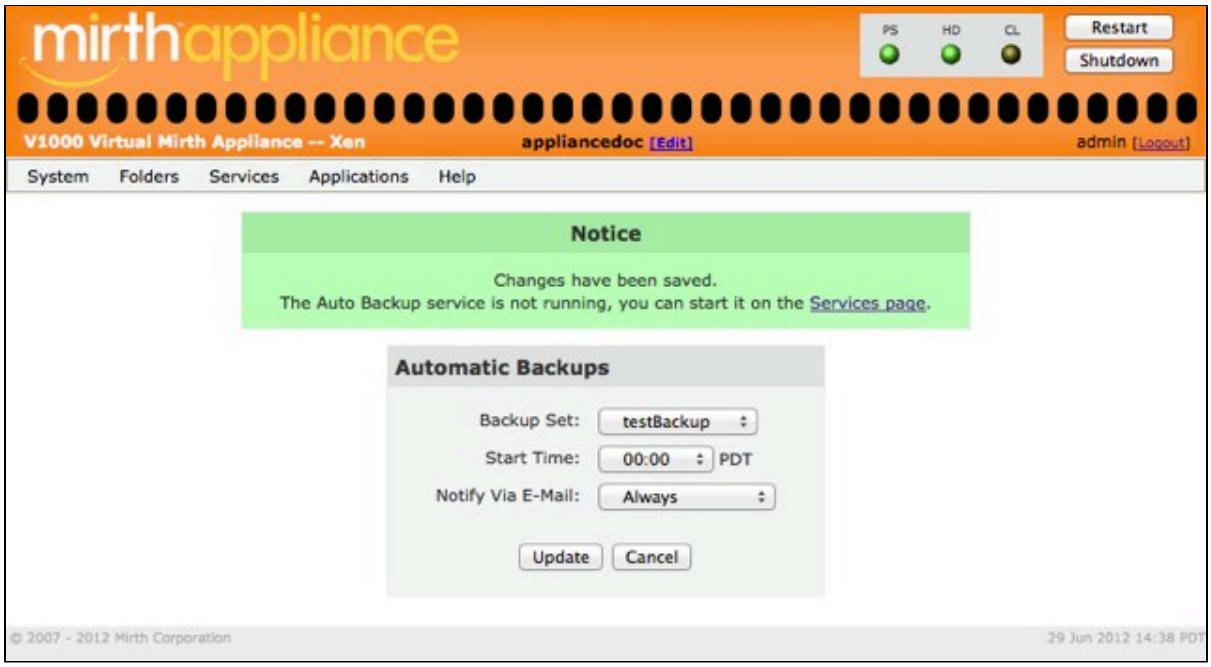


Filling In the Automatic Backups page

The **Automatic Backups** page displays a notice with the Appliance's current time setting, to make sure it matches the user's expectations. The notice includes a link to change the Appliance's time zone and NTP server information if necessary.

The **Backup Set** menu displays any backup set defined in the **Backups** page (**System** menu). The **Start Time** menu displays time in 15 minute increments from midnight (0:00) to 11:45 PM (23:45), and shows the currently set time zone. The notification options are *Always*, *Only on errors*, and *Never*.

After filling in the form, click the **Update** button. This *will not start the service* if the Auto Backups service was not running previously. The Appliance will warn you of this with a notice at the top of the page:



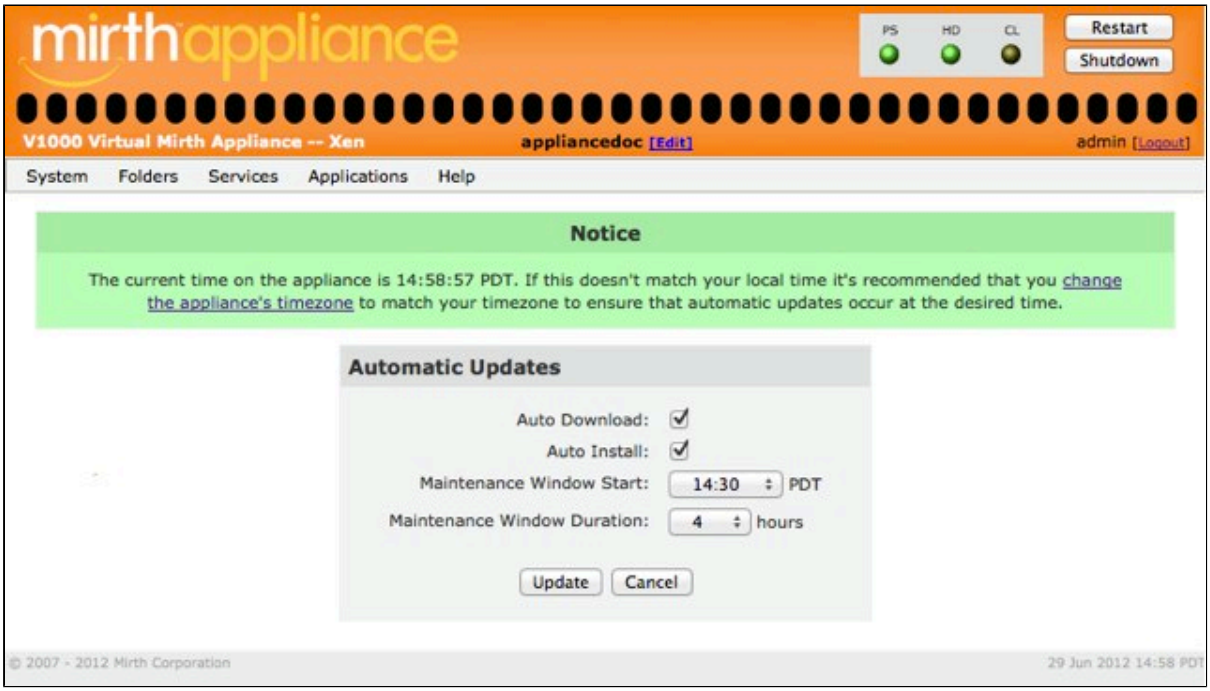
The Automatic Backups page warning that the service is not running

Click the linked words to go to the **Services page**, where you can start the Auto Backup service.

Auto Update

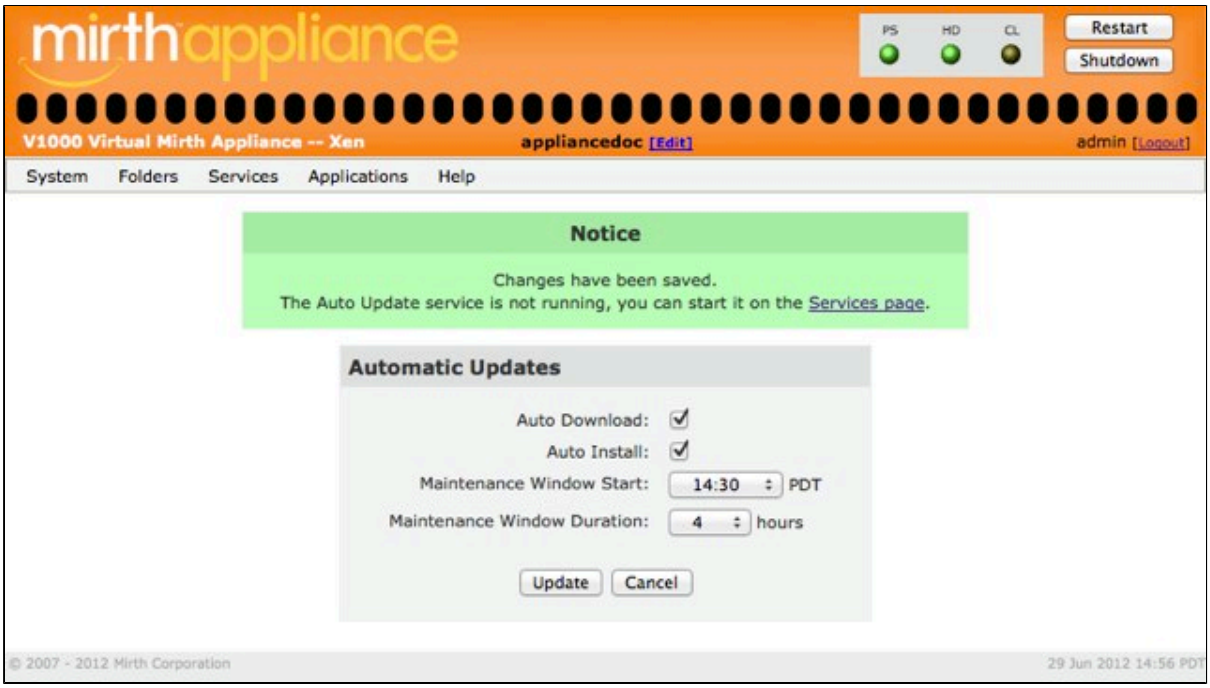
The Auto Update service allows you to set handling parameters for new Appliance updates.

This service allows a certain level of update automation. You can choose to download and install updates automatically. You can also set a start time and duration of when and how long you want to download and install any updates. This is helpful in making sure update activity occurs outside high traffic periods.



Automatic Updates

If the Auto Update service is not running before you configure the service, then the page will display a notice after you update the settings. Click the linked words **Services page** in the notice to be redirected to the **Services Control** page where you can click the **Start** button next to the service.



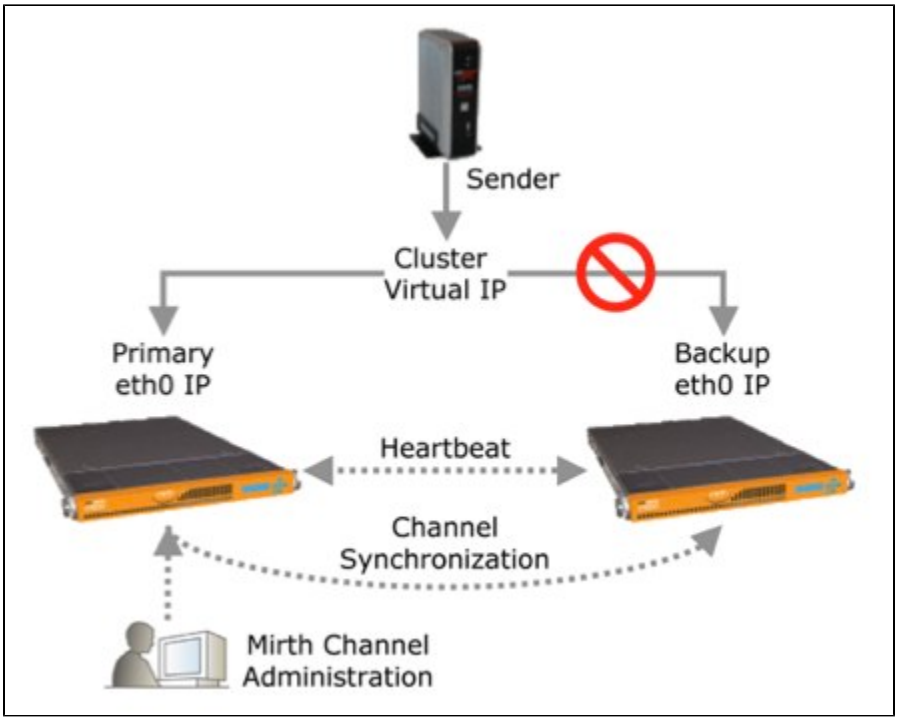
Automatic Updates notice to start the service

Clustering

This **Clustering** functionality and the **Load Balancing** functionality available in the **Services** menu have been deprecated in favor of the **Mirth Connect > Clustering** workflow available through the **Applications** menu.

Two Mirth Appliances can be configured in a fail-over cluster by using the Clustering service. The goal of Clustering is to maximize availability of the Cluster Virtual IP address, which in turn provides a more reliable network endpoint for message receipt and processing. The Appliances must:

1. Be the same model (e.g., two E1000s).
2. Be running the same software version.
3. Have their primary network interfaces (eth0) on the same subnet.



Mirth Appliance Fail-Over

One Appliance is configured as the *Primary*, and the other as the *Backup*. The *Active Appliance* is the node currently providing the Virtual IP address to the network. The *Standby Appliance* monitors the periodic heartbeats sent by the Active Appliance. Only one node will be Active Appliance at a time, and normally this will be the Primary–unless there is a problem: either something wrong with Mirth Connect, or some other hardware, software, or network problem that has caused it to fail or lose connectivity to the network.

If the Backup notices three missed heartbeats from the Primary, it will become the Active Appliance and begin providing the Virtual IP address to the network. When the Primary returns, it will take back

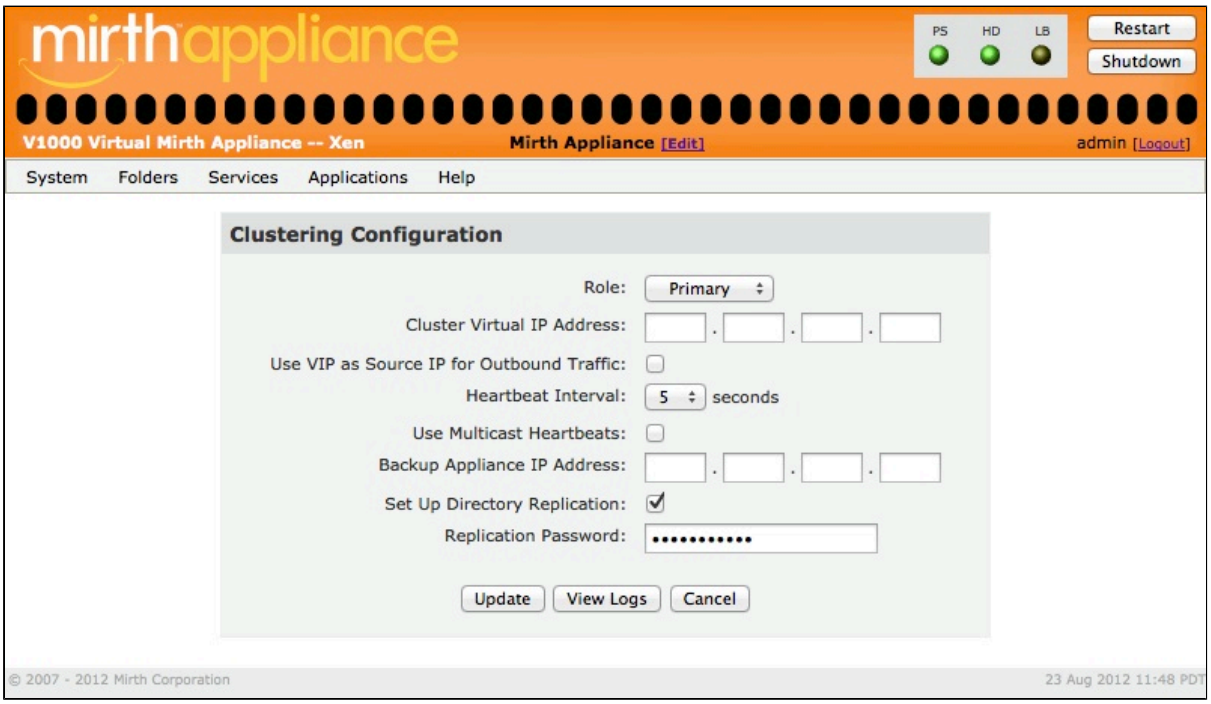
control of the Virtual IP address and become the Active Appliance again; additionally, the Backup will hear that the Primary has resumed its heartbeats, so it will relinquish the Virtual IP address and go back to being the Standby Appliance.

Clustering also provides a synchronization mechanism to help keep the two Appliances running the same Mirth Connect channels. When you start Clustering, or whenever you deploy one or more channels while Clustering is running, the synchronization service will copy over the Mirth Connect configuration from the Primary to the Backup. For this reason, all channel administration should be performed on the Primary.

⚠ The synchronization service is great for keeping your channels in sync, but it does have some limitations:

- Messages (viewable through the Message Browser) are not copied over.
- Custom plugins, jars, or other files are not copied over.
- Other Appliance features like custom Databases, SSL Tunnels, VPN Server configuration and clients, are not copied over.

Managing the cluster is done by managing the each individual node in the cluster. To be certain which Appliance you are connecting to, you should connect directly to the real IP address of each node, not the virtual IP address.



Fail-over clustering is easy to configure and provides a high-availability solution.

To configure the Clustering service, you will need to know the primary IP address (from the eth0 interface) of both Appliances, as well as a third, unused IP to use for the Virtual IP address. On each node, select the **Role** (one *Primary, one Backup*), enter the same **Cluster Virtual IP Address**,

select a **Heartbeat Interval**, and enter the **Appliance IP Address** of the other node.

To avoid an unnecessary failover, you should start the Clustering service on the Primary first, and then start it on the Backup. Likewise, if you are shutting down the cluster, reverse the order: stop Clustering on the Backup first, and then stop it on the Primary. Remember that if you stop the Mirth Connect Server on the Active node, a failover will occur. If a failover occurs, do not restart the Primary until you are ready for a fail-back. To prevent premature fail-back, stop the Clustering service on the primary node when it is in a failed state.

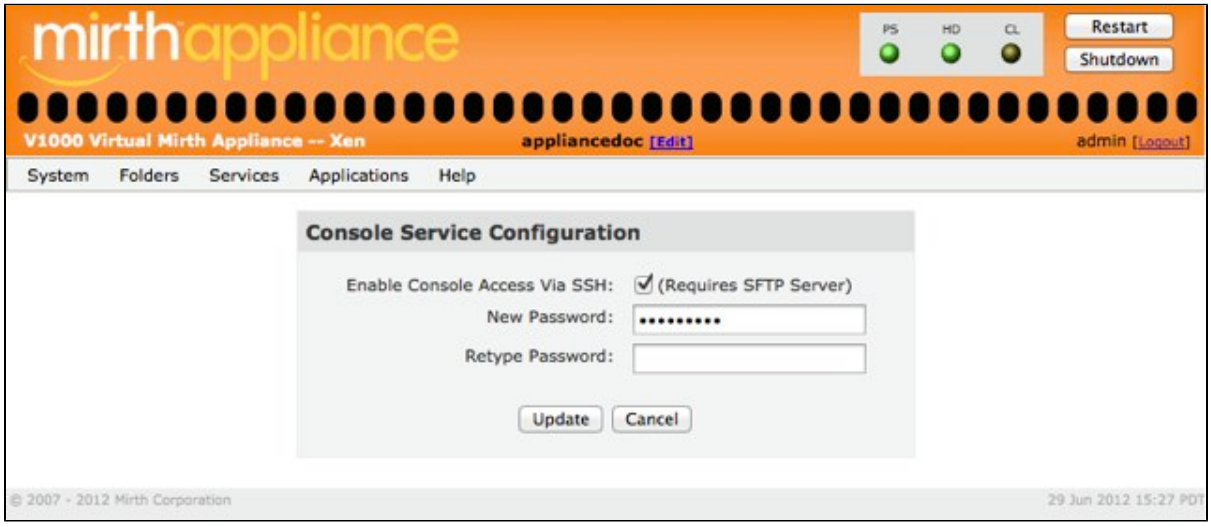
While Clustering is running, the control panel header has a **CL** indicator to show the current status. If this indicator is not green, click it to get more information on the problem.

Whenever a node becomes active, an e-mail notification is sent to the address specified on the **Mail Configuration** page (System Menu > Mail).

You can also use other services, such as SFTP and SSL with the cluster Virtual IP address. You must create matching configurations on both Appliances first however. It is recommended to document all changes made to the Primary so they can be more easily done also on the Backup. We recommend performing a test failover to ensure everything works on the Backup identically to the Primary.

Console

The Mirth Appliance Console allows a direct connection to the Appliance to get IP information, display interfaces and listening ports, manage the connection to SupportNet, shutdown and restart the Appliance, and more. The **Console** item in the **Services** menu allows you to set the password for console access, and to enable or disable network console access (network console access is only via ssh). The console password can also be set from within the console menu.



Console Service Configuration

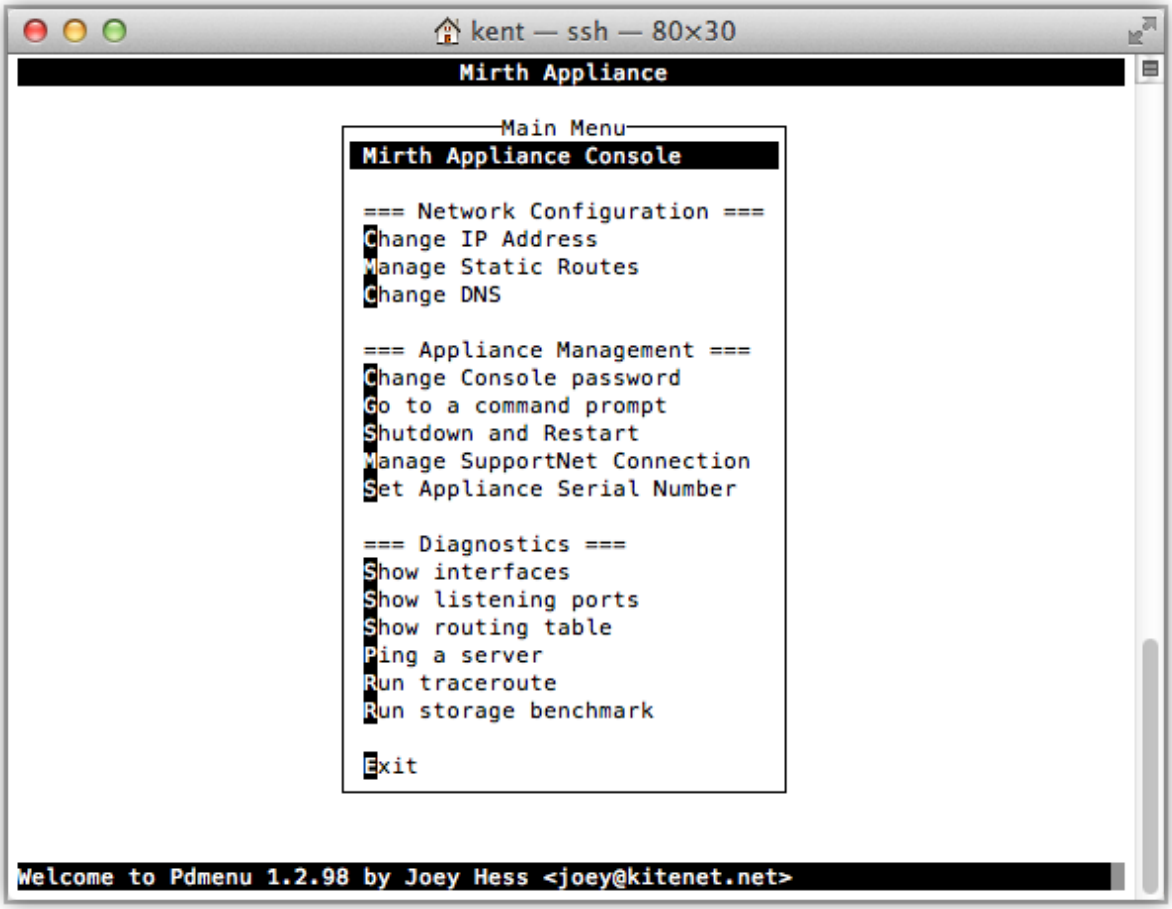
The Console item opens the **Console Service Configuration** page. This page allows you to enable or disable console access via SSH. If this is enabled, then network users can connect to the Appliance's Console over an SSH connection from a terminal program, such as PuTTY on Windows or Terminal on Mac OS X. If this is disabled then console access is only available by connecting a keyboard and monitor directly to the Mirth Appliance.

The **Console Service Configuration** page also allows you to set the console password. By default the password is "console" (see the connection example below).

You can console into the Appliance over an ssh connection or by directly connecting a keyboard and monitor to the Appliance. The default username/password is console/console. For example, from a UNIX command prompt, establish an ssh connection with:

```
$ ssh console@192.168.0.2
console@192.168.0.2's password: console
```

Whether connected directly with a monitor and keyboard or remotely via ssh, the console screen and selections are the same.



Console main menu

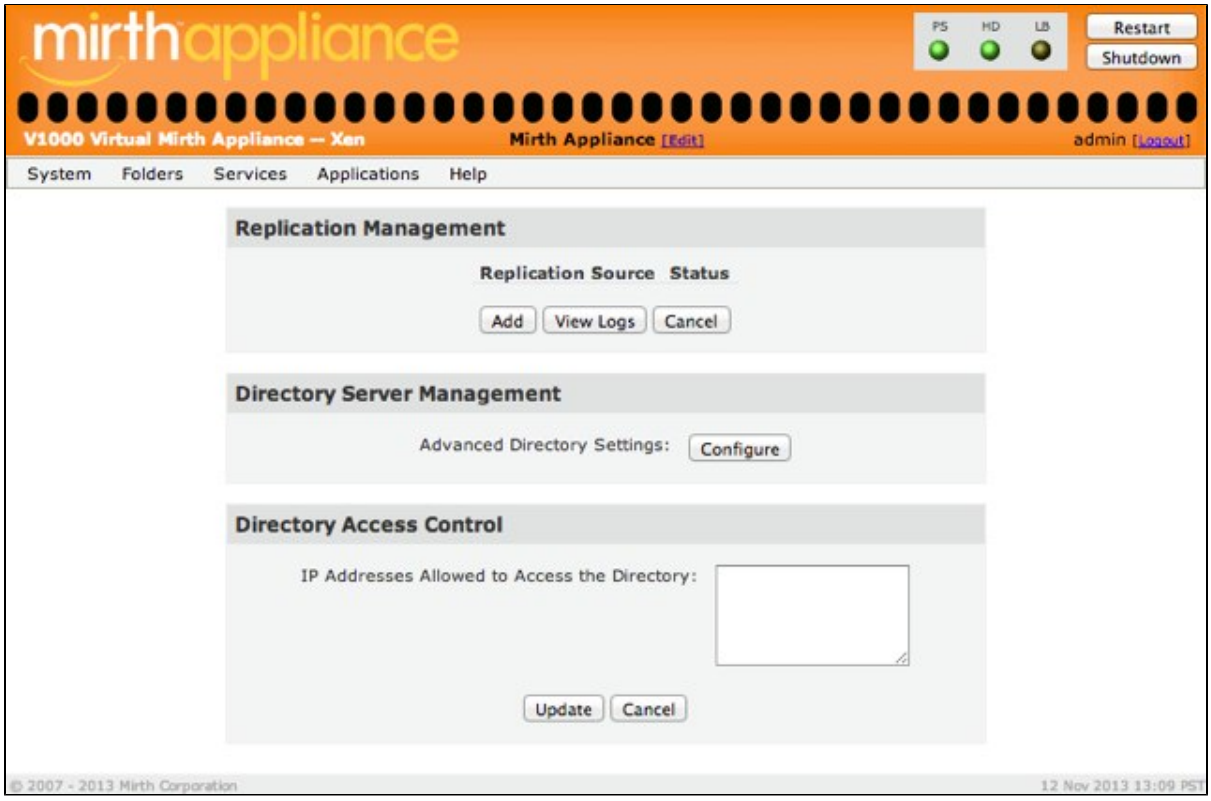
> ⚠ ***Note:*** *To ssh into an Appliance from a Mac use the resident Terminal program. From a Windows machine you can use a third party ssh application like PuTTY.*

Existing Appliances that upgrade will have the console & ssh access disabled by default, with no password set. If they wish to enable console access, they will need to set a password.

Directory

The directory service is intended to provide a single place for user and role management across multiple Appliances. It does not matter which Appliance changes are made to as any new changes will be replicated to all other Appliances added under **Replication Management.**

When you create or modify a user on one Appliance, it automatically replicates the changes to all other Appliances participating in the replication. When you set up clustering, the nodes are automatically set up to replicate, so there is no need to manually add the other Appliance in the cluster here.

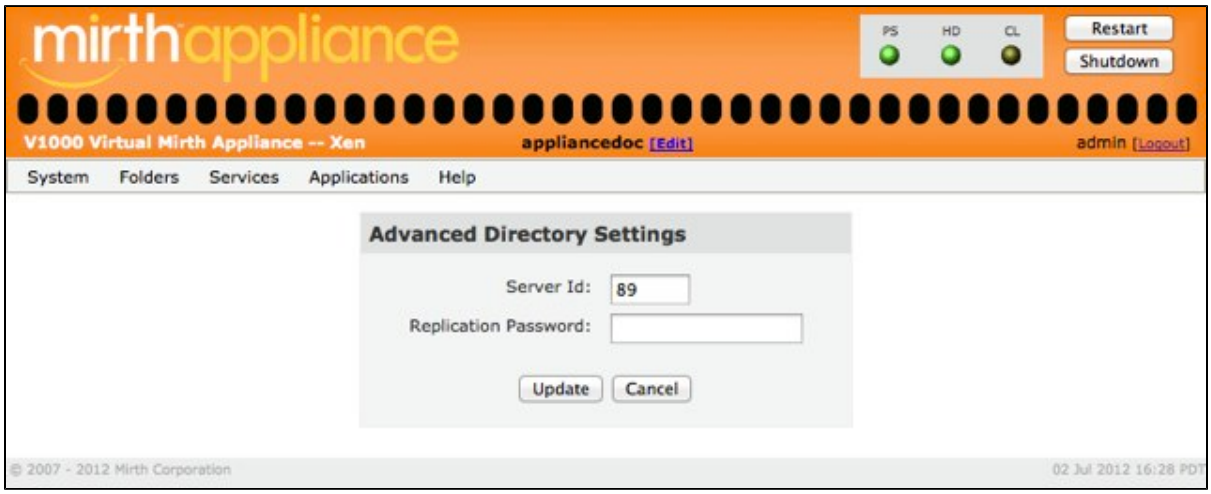


Directory Services

Click the **Add** button to add replication sources.

Add Replication Source

Click the **Configure** button to go to the page to update the advanced directory settings.



Advanced Directory Settings

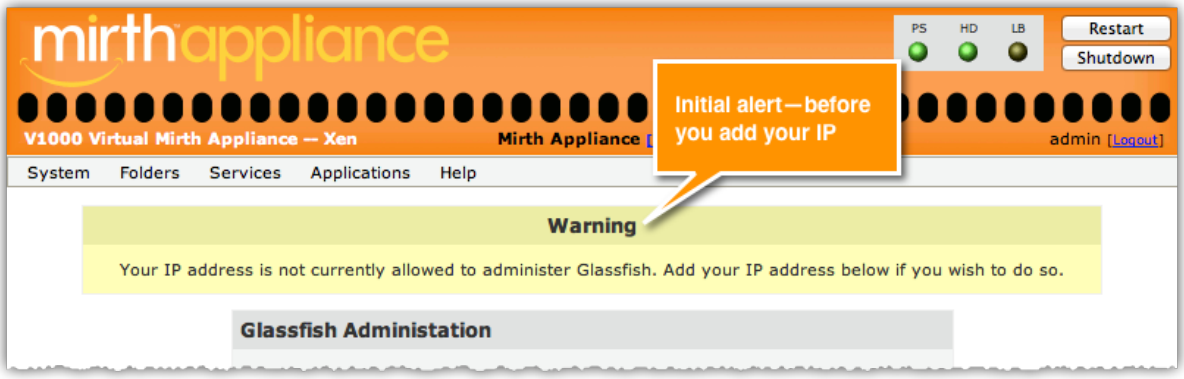
Glassfish

> ⚠ This is not part of the default installation, but when one of the Mirth enterprise applications is installed, a **Glassfish** entry will appear on the **Services** menu.

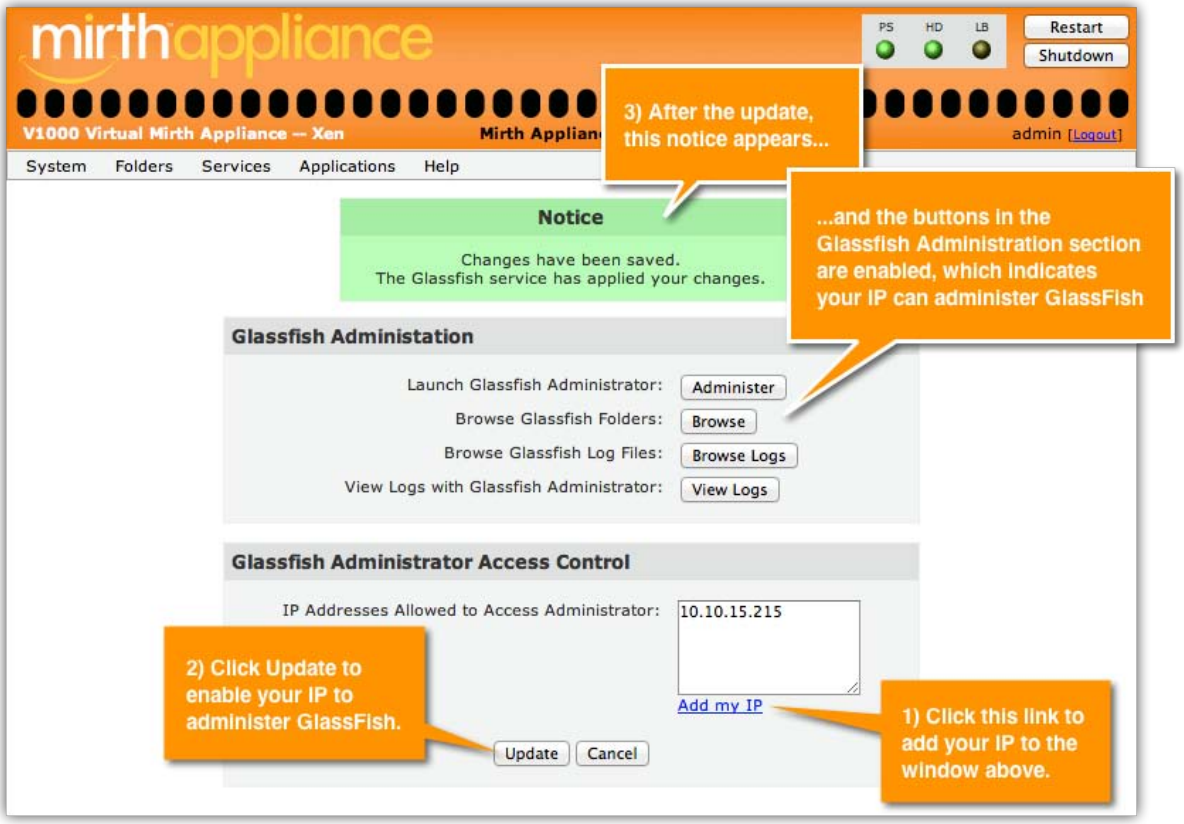
Mirth Corporation uses GlassFish (currently v 2.1.1) to deploy Mirth Mail, Mirth Results, Mirth Match, and Mirth Analytics on Mirth Appliance.

Originally sponsored by Sun and now Oracle Corporation, GlassFish is a free, open-source, application-server project; that is, the server's function is dedicated to the efficient execution of procedures (programs, routines, scripts) to support its applications. GlassFish is licensed under two free software licences: the CDDL (Common Development and Distribution License) and the GPL (GNU General Public License).

To access the GlassFish service, in the Mirth Appliance menu bar, click **Services** > **Glassfish**. The first time you select the GlassFish page, you see a warning that alerts you that you cannot administer GlassFish because you have not added your IP address to the **Administer Access Control** window.



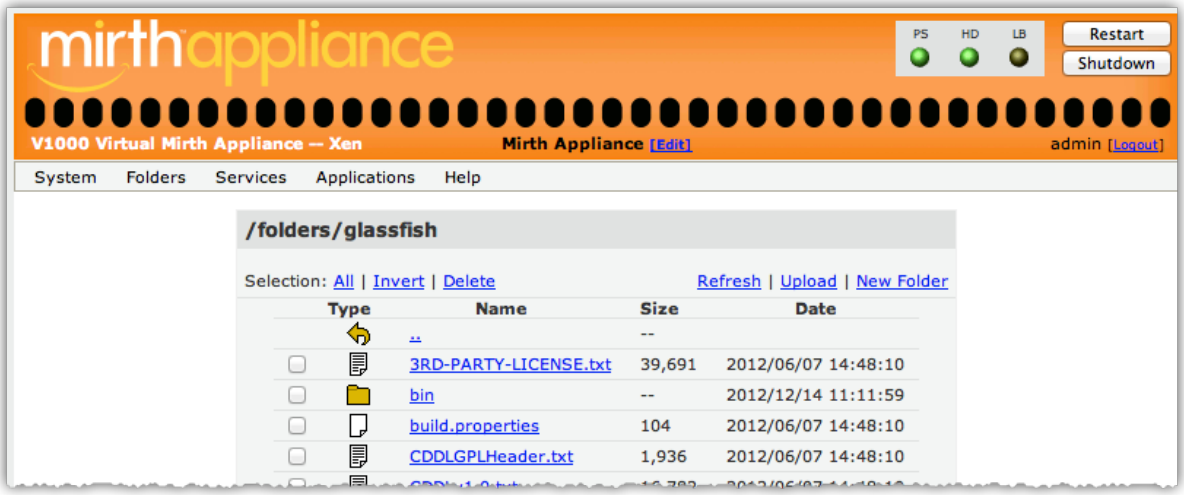
To add your IP, click the "Add my IP" link below the window in the **Glassfish Administrator Access Control** section of the Glassfish page.

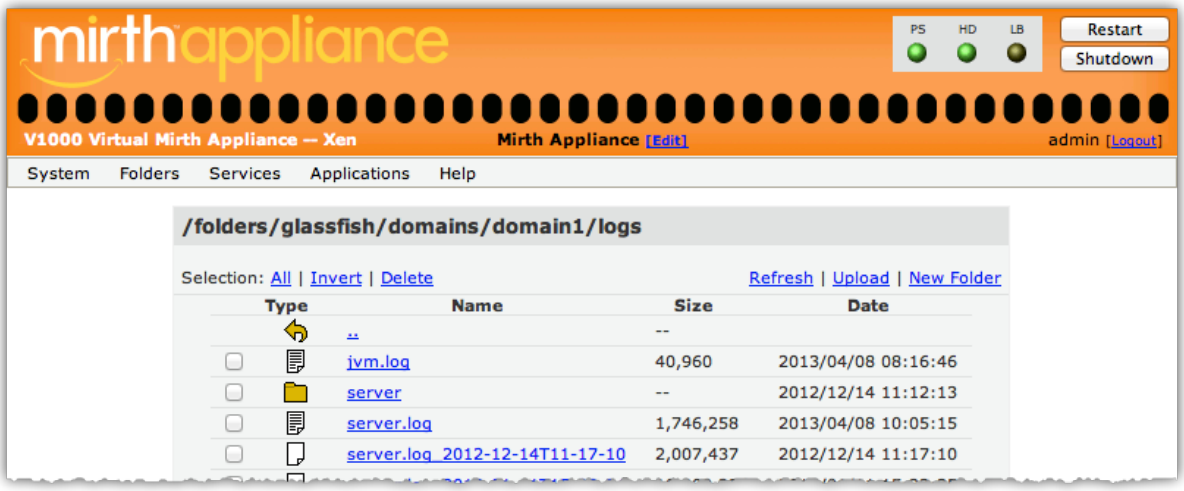


You can use the GlassFish Administrator to customize settings to maximize your system's performance. Launch the GlassFish Administrator via the **Glassfish** page—**Glassfish Administration** section > **Launch Glassfish Administrator** button to display the GlassFish login dialog.

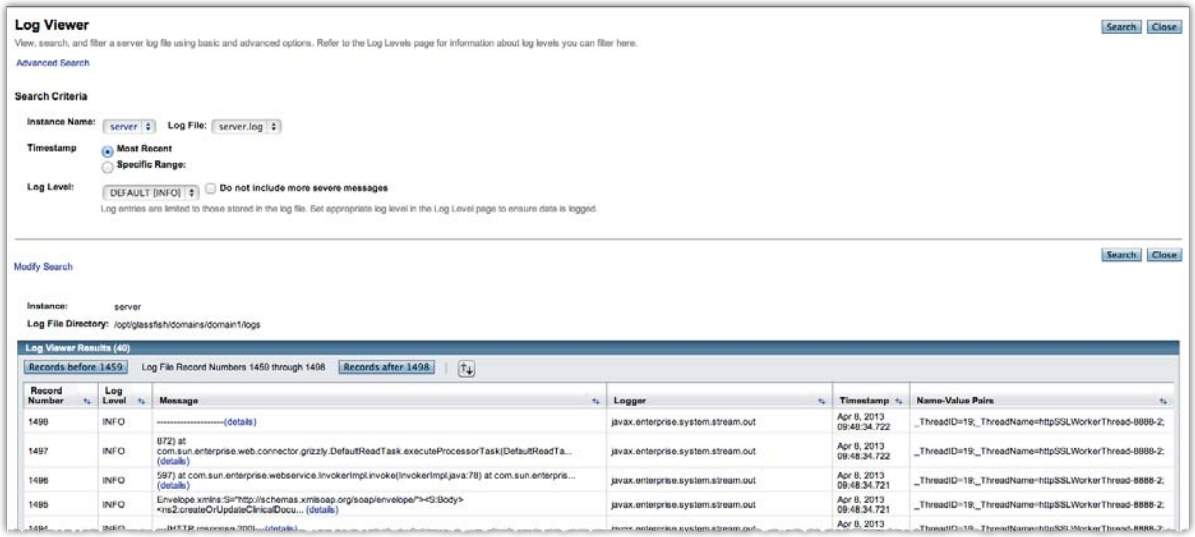
In the **User Name** field, enter *admin*; in the **Password** field, enter *adminadmin*, and click the **Login** button.

On the Glassfish page, you can browse GlassFish Folders and GlassFish Log Files via the **Browse** and **Browse Logs** buttons, respectively:





Also on the Glassfish page, you can View Logs with Glassfish Administrator via the View Logs button:



Load Balancing

This **Load Balancing** functionality and the **Clustering** functionality available in the **Services** menu have been deprecated in favor of the **Mirth Connect > Clustering** workflow available through the **Applications** menu.

Multiple Mirth Appliances can be configured in a load-balanced group by using the Load Balancing service. The goals of Load Balancing are to provide high availability and scalability. Similar to its predecessor, Clustering, Load Balancing maximizes the availability of the Virtual IP address, which in turn provides a more reliable network endpoint for message receipt and processing. Additionally, Load Balancing utilizes all units in the group, increasing potential throughput.
All Appliances in a load-balanced group must:

1. Be the same model (e.g., two E1000s).
2. Be running the same software version.
3. Have their primary network interfaces (eth0) on the same subnet.

One Appliance is configured as the *Primary*, and the others as *Secondaries*. The *Director* is the node currently providing the Virtual IP address to the network and distributing all incoming traffic to itself and the other members of the group. The Secondaries monitor the periodic heartbeats sent by the Director. Normally the Primary is the Director, unless something is wrong: either something wrong with Mirth Connect, or some other hardware, software, or network problem that has caused it to fail or lose connectivity to the network.

If a Secondary notices three missed heartbeats from the Primary, it will become the Director and begin providing the Virtual IP address to the network and handle distributing the incoming traffic. When the Primary returns, it will take back control of the Virtual IP address and become the Director again.

Load Balancing also provides a synchronization mechanism to help keep the Appliances running the same Mirth Connect channels. When you start Load Balancing, or whenever you deploy one or more channels while Load Balancing is running, the synchronization service will copy over the Mirth Connect configuration from the Primary to the Secondaries. For this reason, all channel administration should be performed on the Primary.

Note: *The synchronization service is great for keeping your channels in sync, but it does have some limitations:*

- *Messages (viewable through the Message Browser) are not copied over.*
- *Custom plugins, jars, or other files are not copied over.*
- *Other Appliance features like custom Databases, SSL Tunnels, VPN Server configuration and clients, are not copied over.*

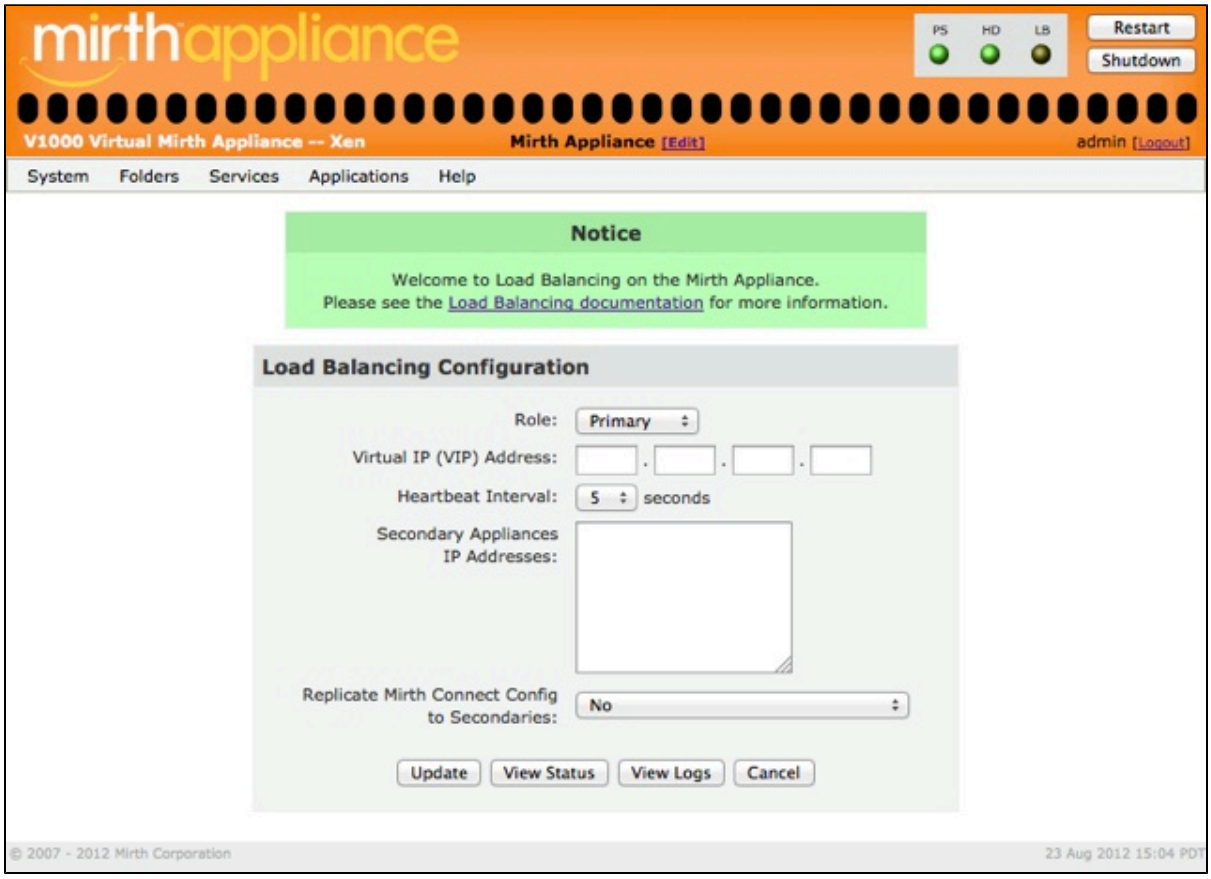
Remember that if you stop the Mirth Connect Server on the Director, a failover will occur. If a failover occurs from the Primary to a Secondary, do not restart the Primary until you are ready for a fail-back. To prevent premature fail-back, stop the Load Balancing service on the Primary node when it is in a failed state.

Configuration and Management

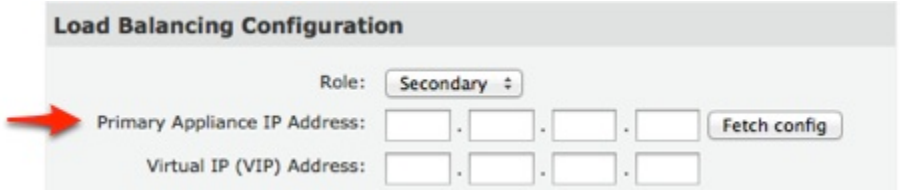
Management of a load-balanced group is done by managing each individual node. To be certain which Appliance you are connecting to, you should connect directly to the real IP address of each node, not the virtual IP address.

To configure the Load Balancing service, you will need to know the primary IP address (from the eth0 interface) of all participating Appliances, as well as an additional, unused IP for the Virtual IP address. On each node, select the **Role** (one *Primary,* all others *Secondary*), enter the same **Virtual IP address**, select a **Heartbeat Interval**, and enter the **Appliance IP address** for each of the other nodes.

When you are configuring the Primary node, the IP addresses for all other nodes go in the multi-line text box, separated by commas or newlines. When you are configuring a Secondary node, an extra line appears for entering the IP address of the Primary node, with a **Fetch config** button that will get the address and fill it in for you. The IP addresses for any other Secondary nodes still go in the mutli-line text box.



Load Balancing Configuration



Extra entry line when Secondary role is selected

To avoid unnecessary switching of which Appliance is the current Director node, you should start the Load Balancing service on the Primary first, and then start it on the Secondaries. Likewise, if you are shutting down a load-balanced group, reverse the order: stop Load Balancing on the Secondaries first, and then stop it on the Primary.

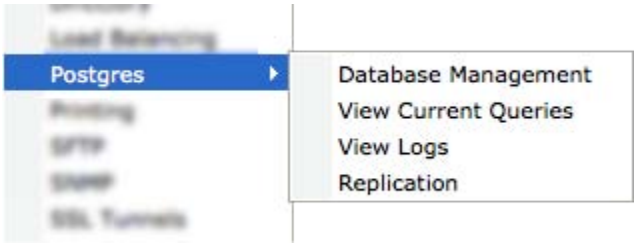
Whenever a node becomes active, an e-mail notification is sent to the address specified on the **Mail Configuration** page (**System** menu **> Mail**).

While Load Balancing is running, the control panel header has an **LB** indicator to show the current status. If this indicator is not green, click it to get more information on the problem. This status information can also be viewed by clicking the **Status** button on the Configuration page. To see a log of the system messages about Load Balancing, click the **View Logs** button.

You can also use other services, such as SFTP and SSL, with the group's Virtual IP address. You must first create matching configurations on all Appliances in the group. It is recommended to document all changes made to the Primary so they can be more easily done also on the Secondaries. We recommend performing a test failover of the Director role to ensure everything works on each Secondary identically to the Primary.

Postgres

The **Postgres** entry on the **Services** menu opens its own sub-menu. If you simply click on **Postgres** , it is the same as clicking on the first entry in the sub-menu, **Database Management**. The other entries in the sub-menu are shortcuts to actions that are available using buttons on the **Database Management** screen.

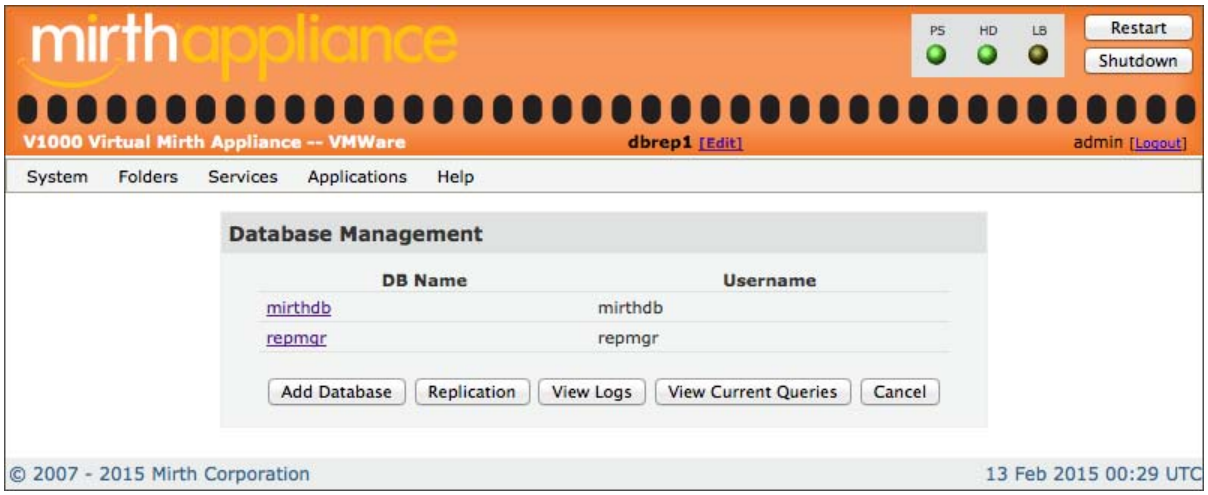


There is an instance of PostgreSQL (a.k.a. "Postgres") running on the Appliance that is used by the Mirth Connect application. With the Postgres service, you can create additional databases for other uses, set up replication of the database, view logs, and view current database queries.

The functionality associated **Replication** button, which allows you to create a duplicate of this database that can be used as a backup in case of a failure, is described in detail in the next section of this guide, titled Replication.

After setting up replication, you can then set up Auto Failover.

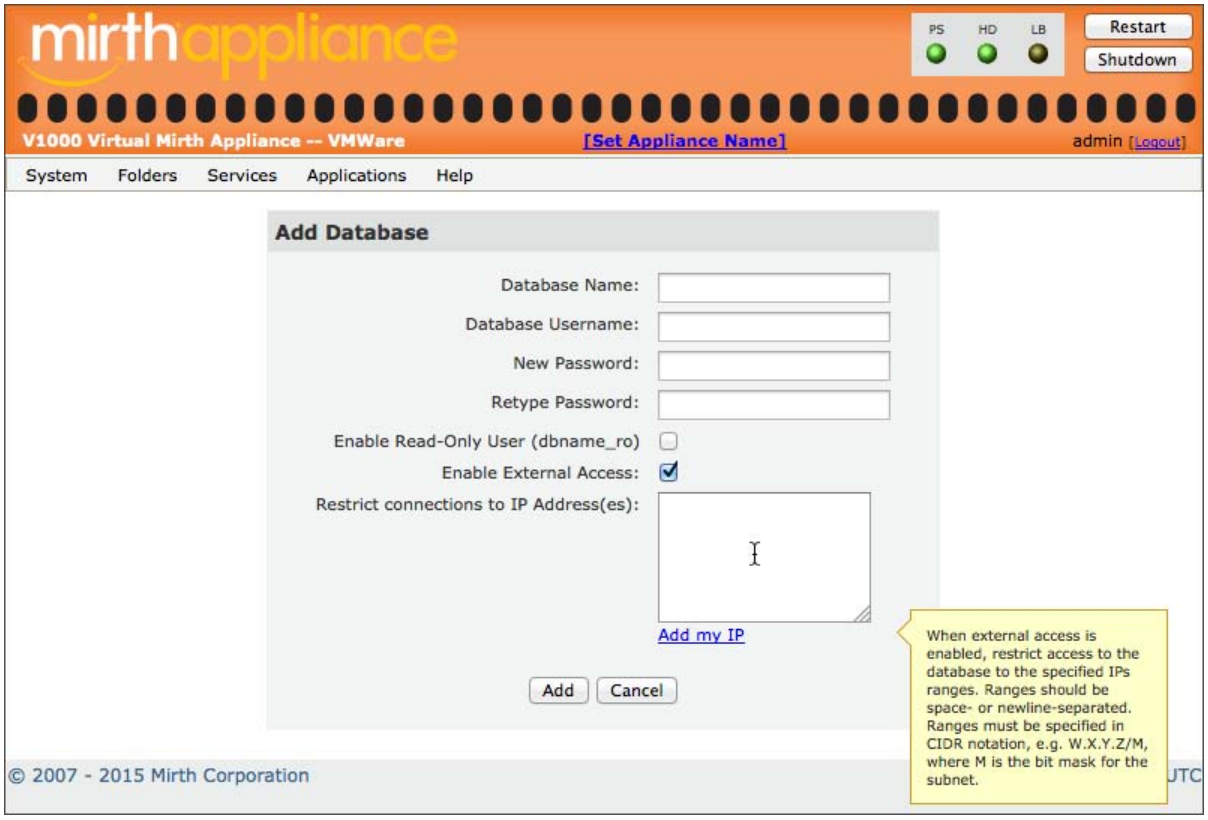
If you want to set up clustering for Mirth Connect, you will need to set up replication and auto failover first. Once these have been set up, you can go to **Applications > Mirth Connect > Manage > Clustering > Configuration**.



Host databases directly from your Mirth Appliance

To set up a new database, click the **Add Database** button. Adding a database would allow you, for example, to create a local database to use as the source or destination of a Mirth Connect channel, or as the backend database for an external application.

Clicking the button brings up the *Add Database* page. Enter a **Database Name** and **Database Username** along with a **Password**. You can optionally **Enable Read-Only User (_ro)** and **Enable External Access.** When external access is enabled, another entry box labeled **Restrict connections to IP Address(es)** appears, which allows you to secure external access. When you click the **Add** button, the database and user will be created. The Database Service only allows one user per database.



Add new databases from the Add Database screen.
This screenshot shows the pop-up tooltip for the restrict connections box.

You can edit an existing database by clicking on the linked name in the list on the *Database Management* page. You will be able to change the user's password, modify external access options, or delete the entire database. When you delete a database, the user will be removed and the database will be deleted, reclaiming any disk space used. Note that you cannot remove the Mirth Connect database (mirthdb).

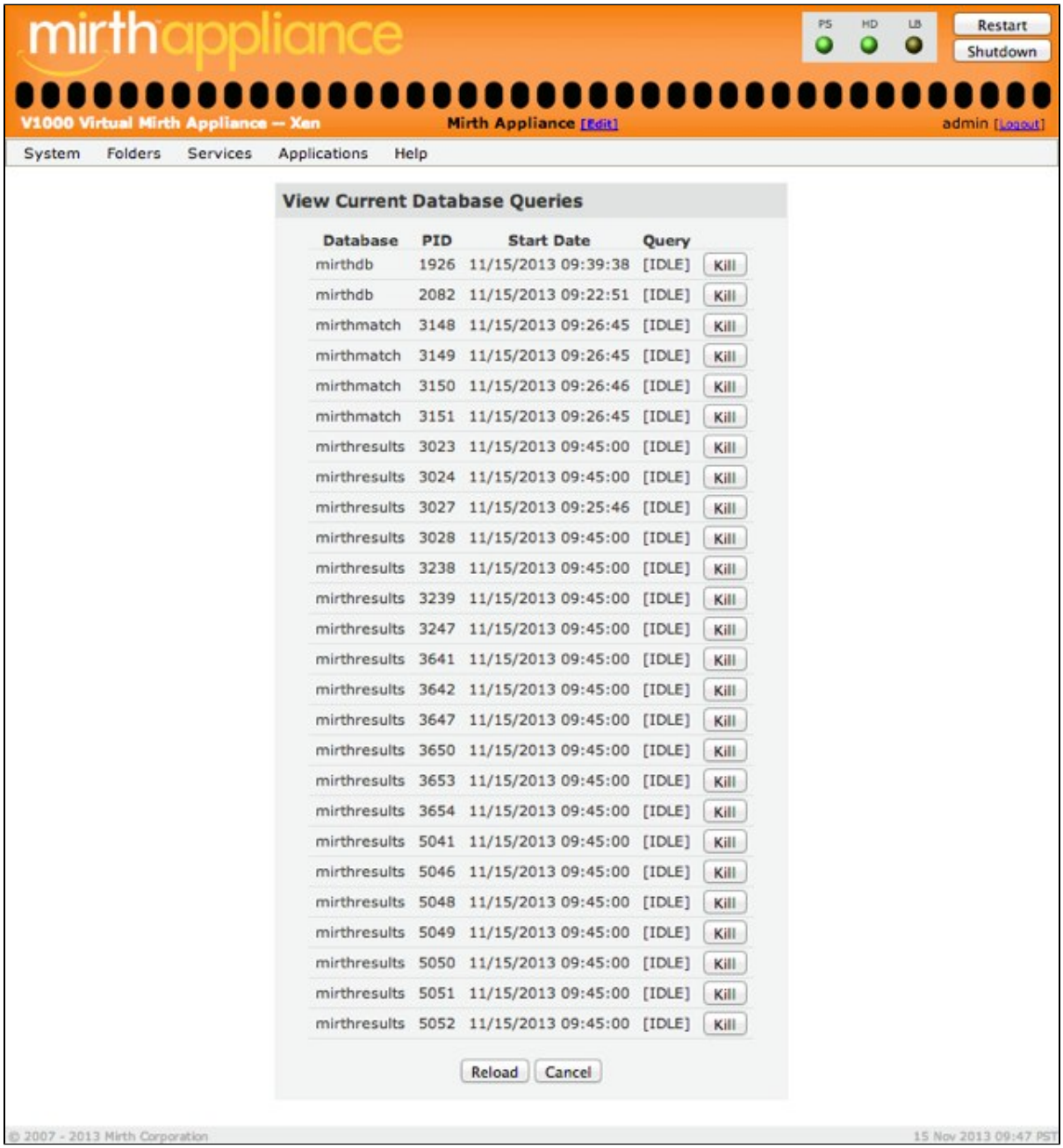
Because the PostgreSQL database used by the Database Service is also used by Mirth Connect, the Database Service must be running when the Mirth Connect Server is running, and vice versa.

You can also view the database logs from the *Database Management* page by clicking on the **View Logs** button. Once you are in the log viewer, you have an option to download the full log by clicking on the **Download Full Log** button at the bottom of the page.

In addition, you can also view and end queries currently running on the databases by clicking on the **View Current Queries** button.

⚠ ***Note:*** *Killing database queries can result in application errors and could potentially lead to*

data loss. You should only kill a query if you are absolutely certain of what you are doing.



View running queries from the View Current Database Queries screen.

Replication

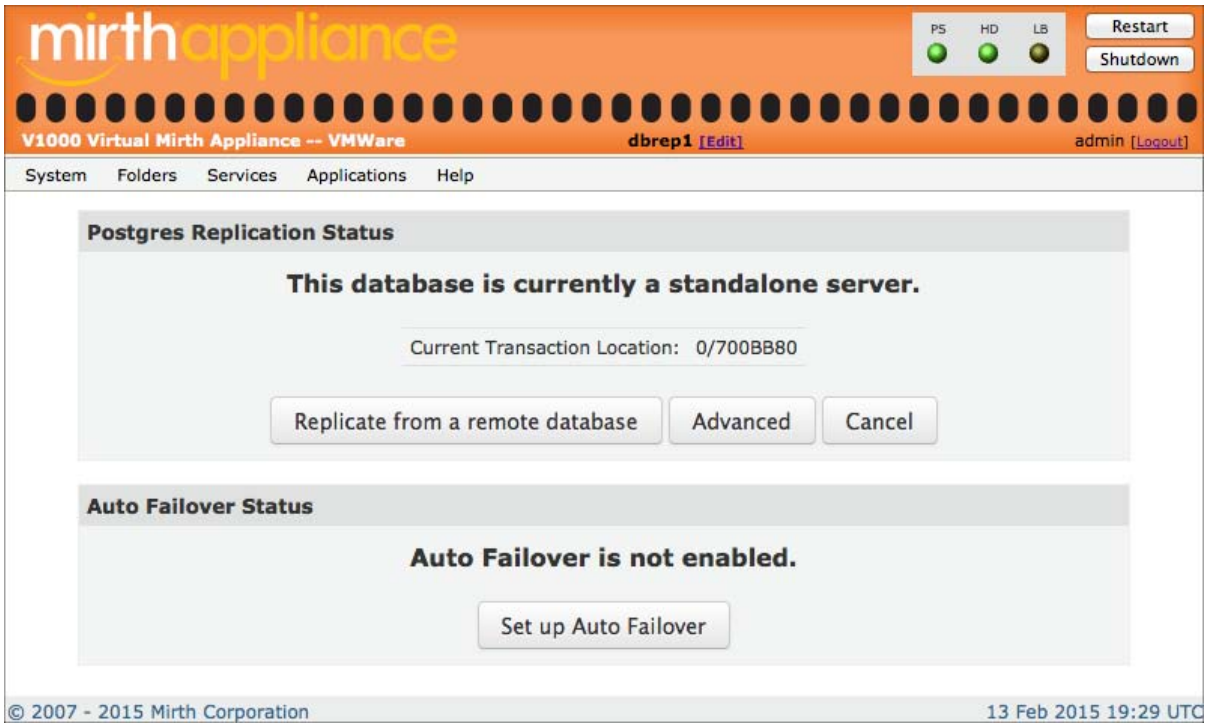
The replication functionality lets you designate a secondary Appliance that will contain a copy of the database that is on your primary appliance. Once everything is set up, and the initial copy of the database has been created on the secondary system, then updates made to the database on the primary system will ripple through to the replica database on the secondary system.

> ⚠ Even though this discussion talks about "database" in the singular, actually all databases contained in the Postgres instance on the primary system will be replicated. The list of these databases can be seen on the **Database Management** page.

One of the primary reasons for setting up replication is so that the secondary database can be used as a failover system if for any reason the primary database becomes unusable. For this reason the secondary database is frequently referred to as a standby database, because it is ready and waiting, standing by in case it is needed. It is also possible to set up multiple standby databases for the same primary database.

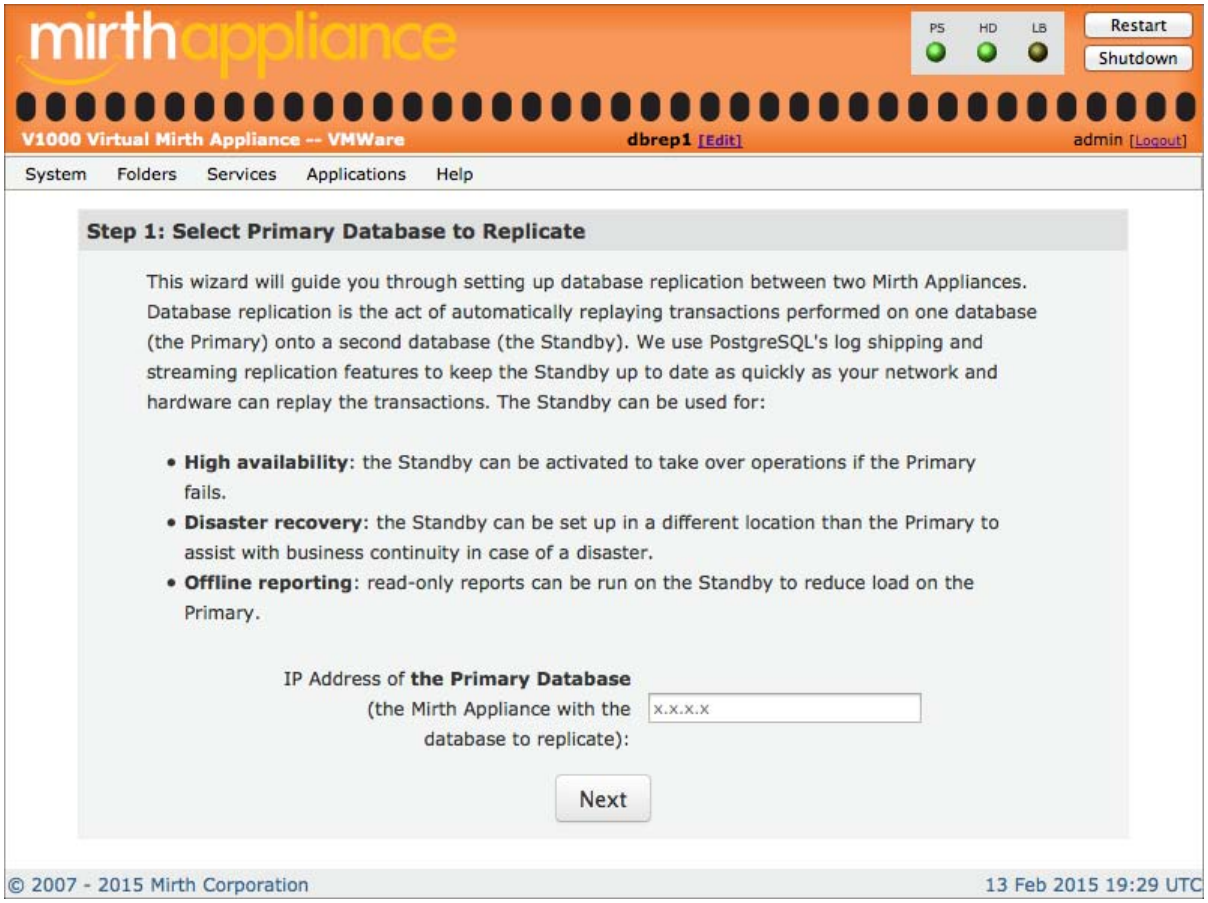
For more information on setting up failover, see the Auto Failover section of this guide.

To get ready to start the configuration for replication for a Mirth Appliance, first log into the control panel of the system which will contain the standby copy of the database, then click on **Services > Postgres > Replication** to go to the **Postgres Replication Status** page. From here you can access a series of screens which act like a wizard to lead you through the configuration steps, as illustrated in the following screenshots.



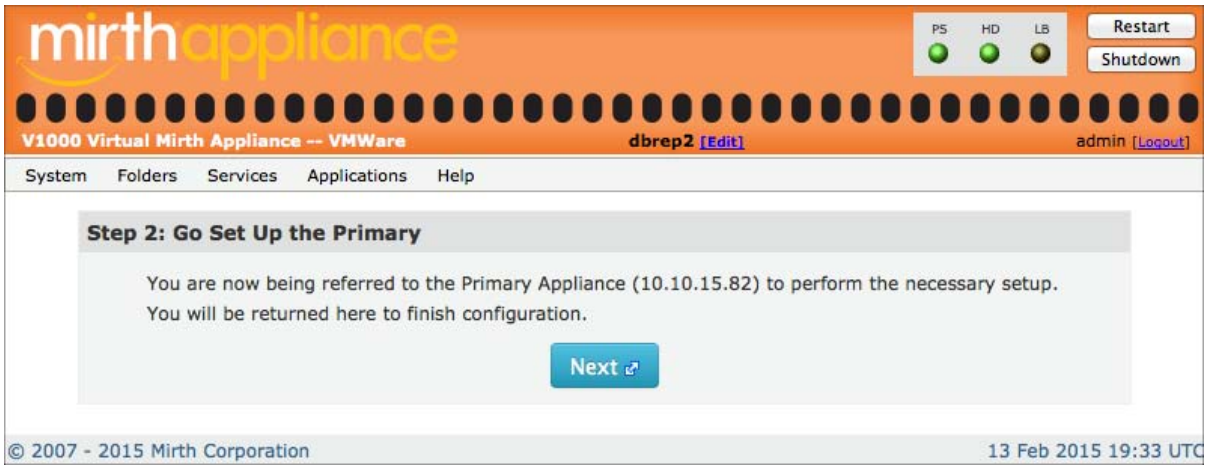
*To start the replication set up,click the **Replicate from a remote database** button.*

Step 1



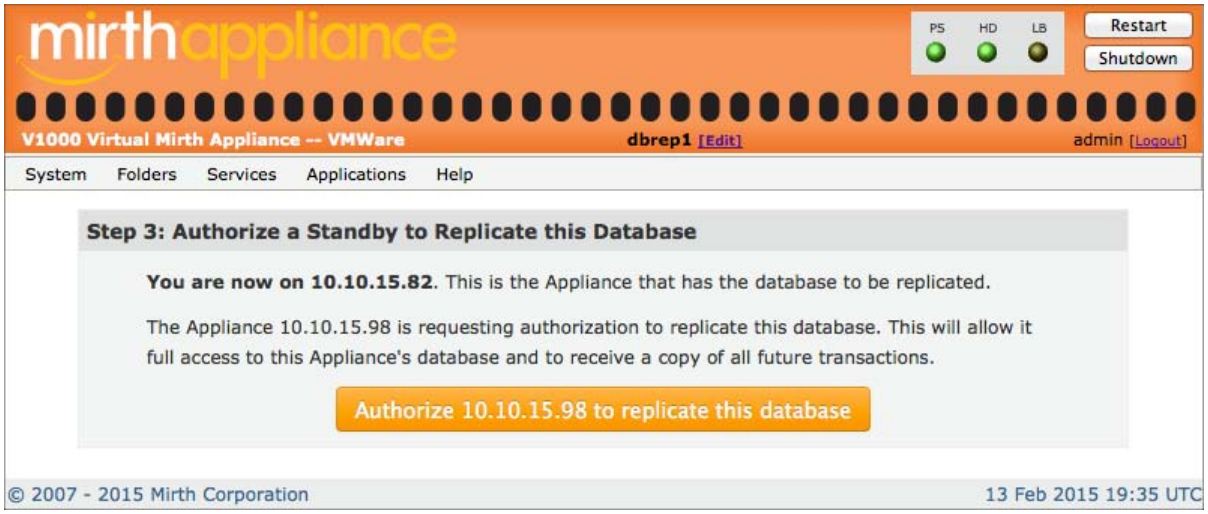
*Step 1: Enter the IP address of the primary database, then click **Next**.*

Step 2



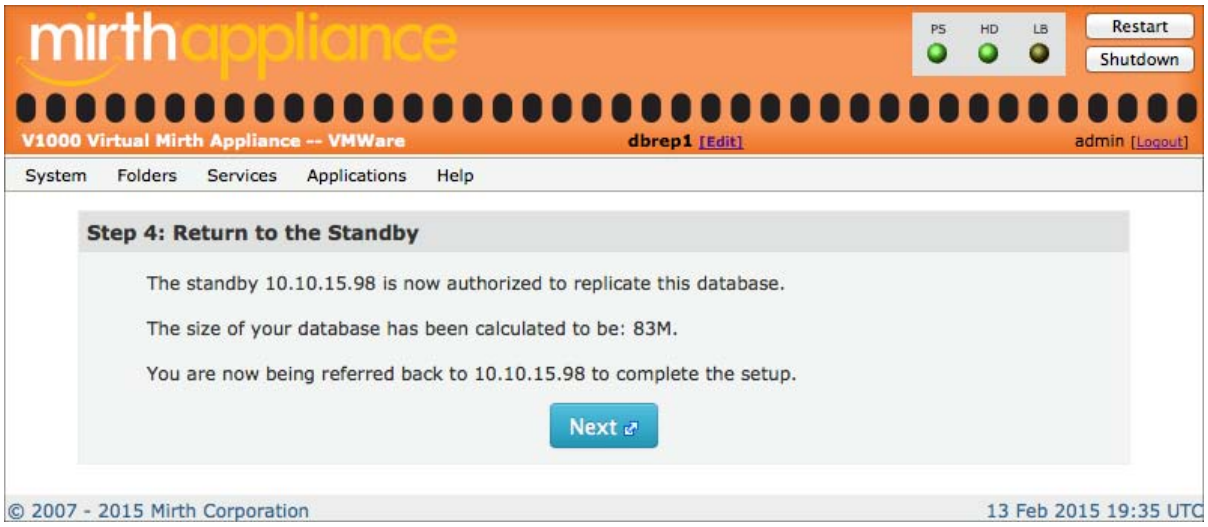
*Step 2: Click the **Next** button to be transferred to the primary Appliance where you will perform the next step.*

Step 3



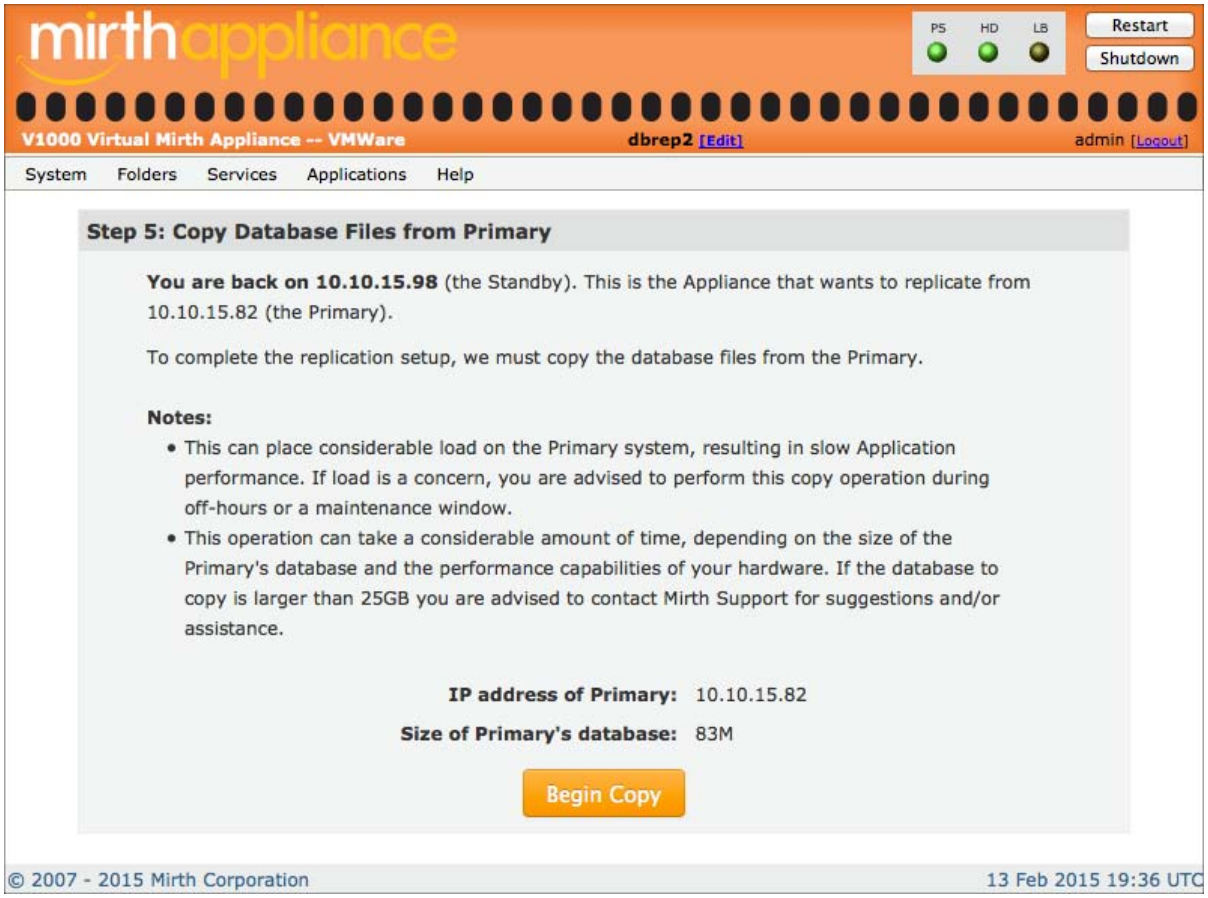
*Step 3: Click the **Authorize x.x.x.x to replicate this database** button to allow replication of the database*

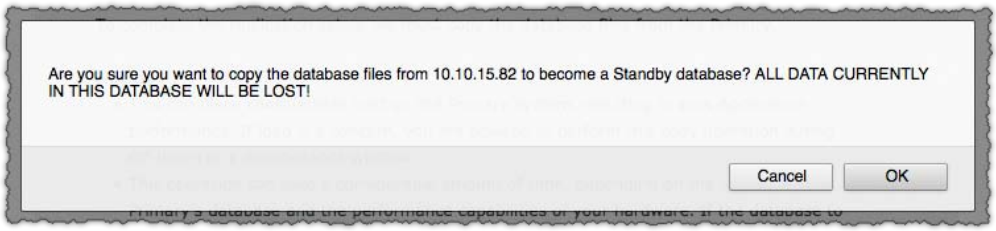
Step 4



*Step 4: Click the **Next** button to be transferred back to the Appliance which will have the standby copy of the database, where you will perform the final set-up steps.*

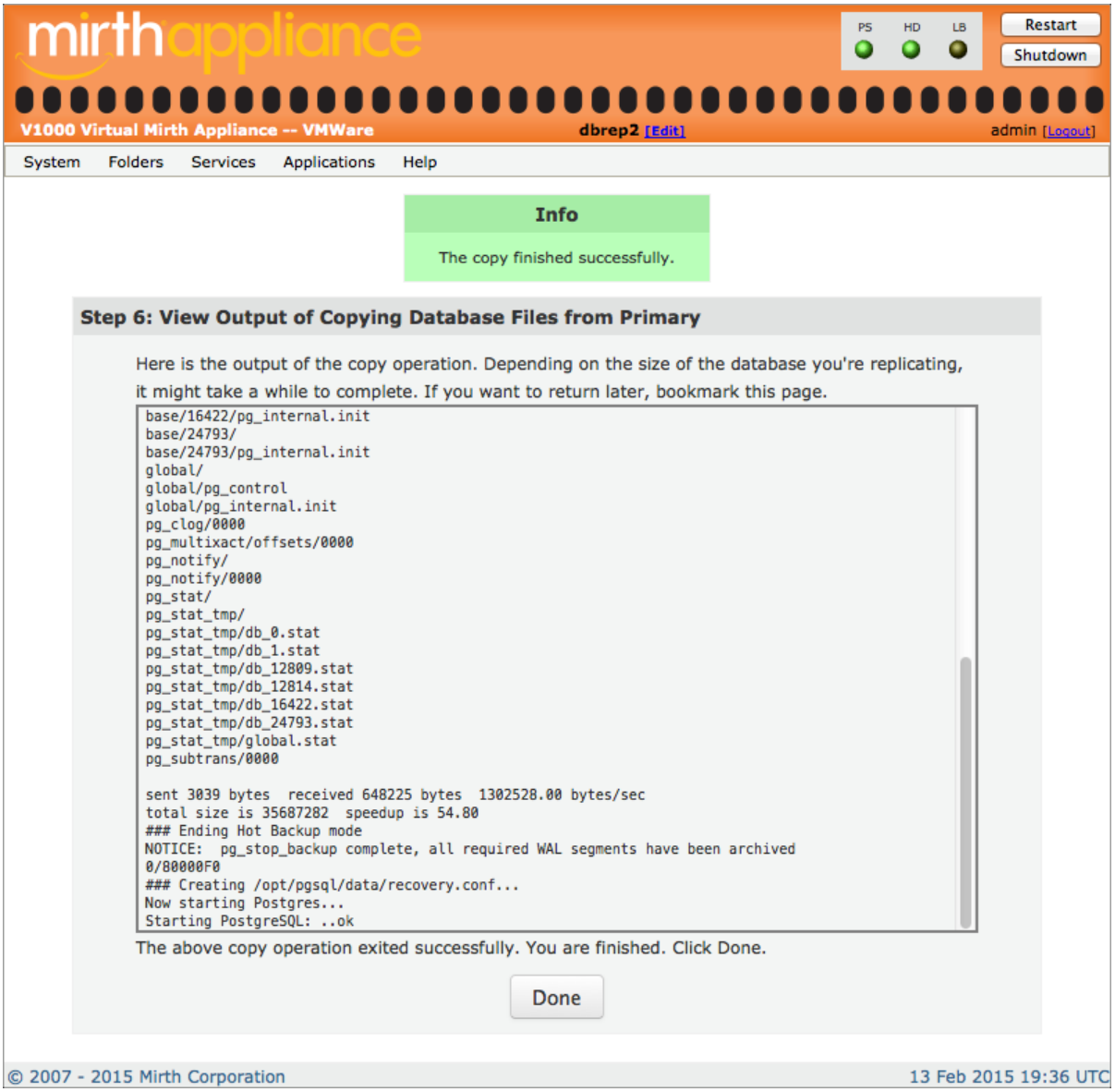
Step 5





*Step 5: Click the **Begin Copy** button to start the copy process. A pop-up dialog will appear requesting confirmation that you want to perform the copy. Click **OK** to start the copy process.*

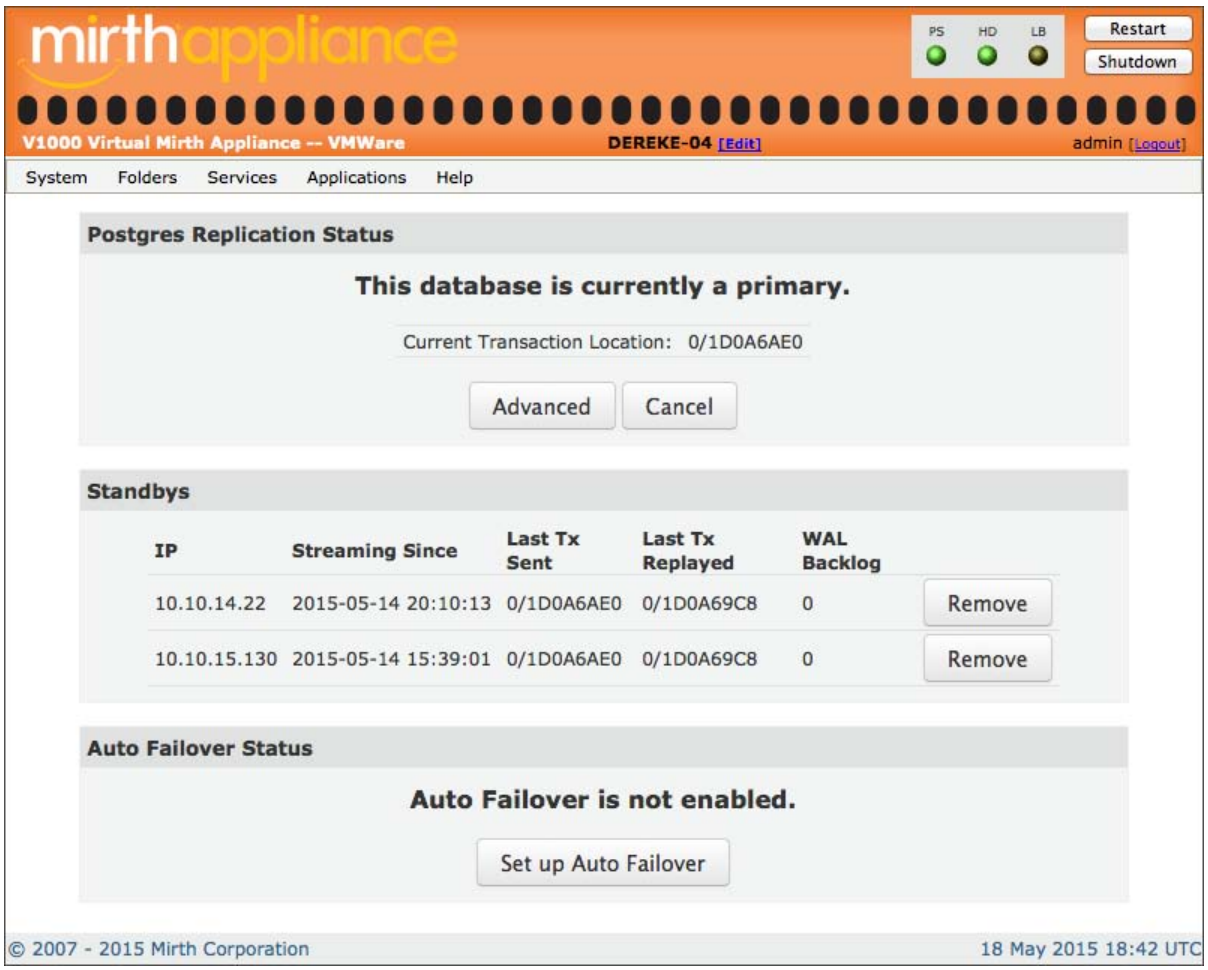
Step 6

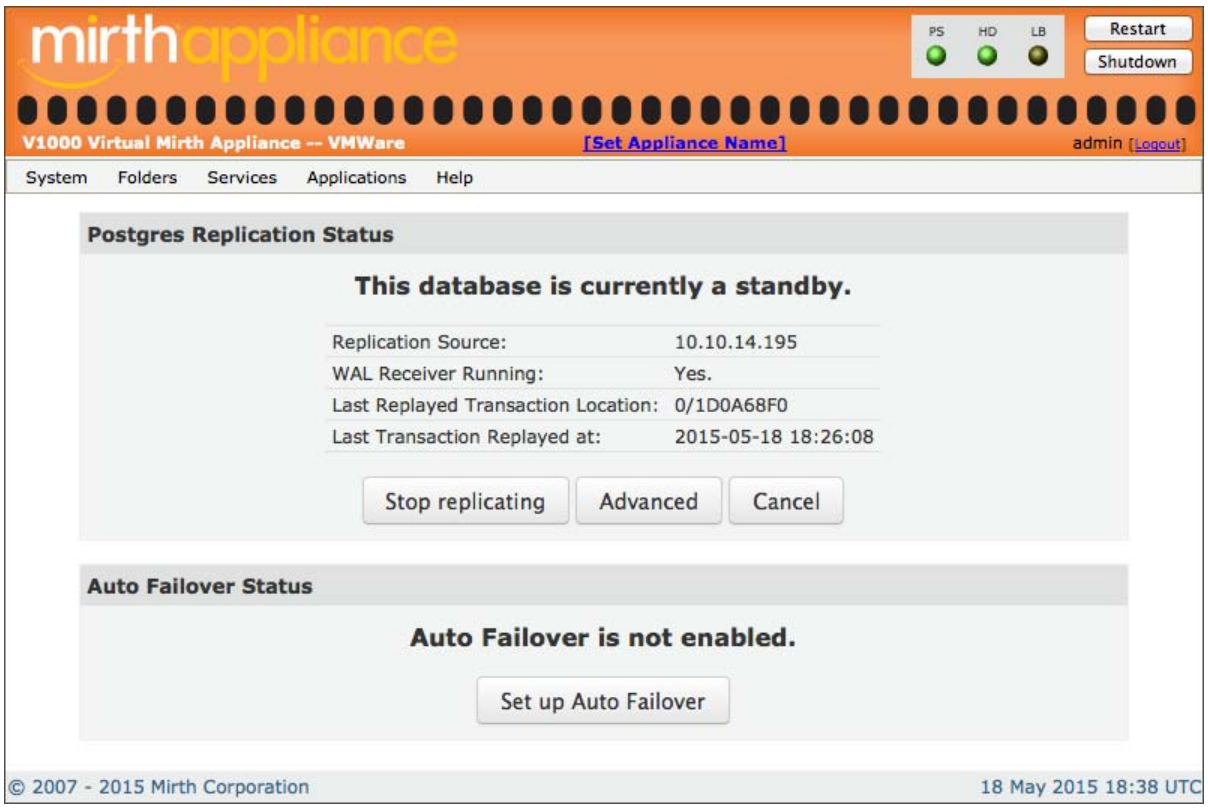


*Step 6: You will be taken to an info page showing the output from the copy operation. When the copy is finished, you can click **Done**.*

After setup is complete

When the replication set-up process is complete, the **Postgres Replication Status** page on the primary Appliance and on the standby Appliance will display their respective statuses.





Click the **Set up Auto Failover** button on either the primary system or the standby system to go to the screen where you can set up automatic changeover to the standby database if the primary database should have a failure for any reason. This is discussed in the next section of this guide, titled Auto Failover.

Advanced configuration

Click on the **Advanced** button to go to the **Postgres Replication Advanced Page**. From here you can edit various configuration files, but it is recommended that you only do this with the assistance of Mirth Support.

The ability to edit *recovery.conf* is only available on standby nodes.

Auto Failover

After setting up replication, you can set up auto failover. Click on the **Set up Auto Auto Failover** button on the **Replication** page on both the primary system and the standby system to get to the **Auto Failover** page.

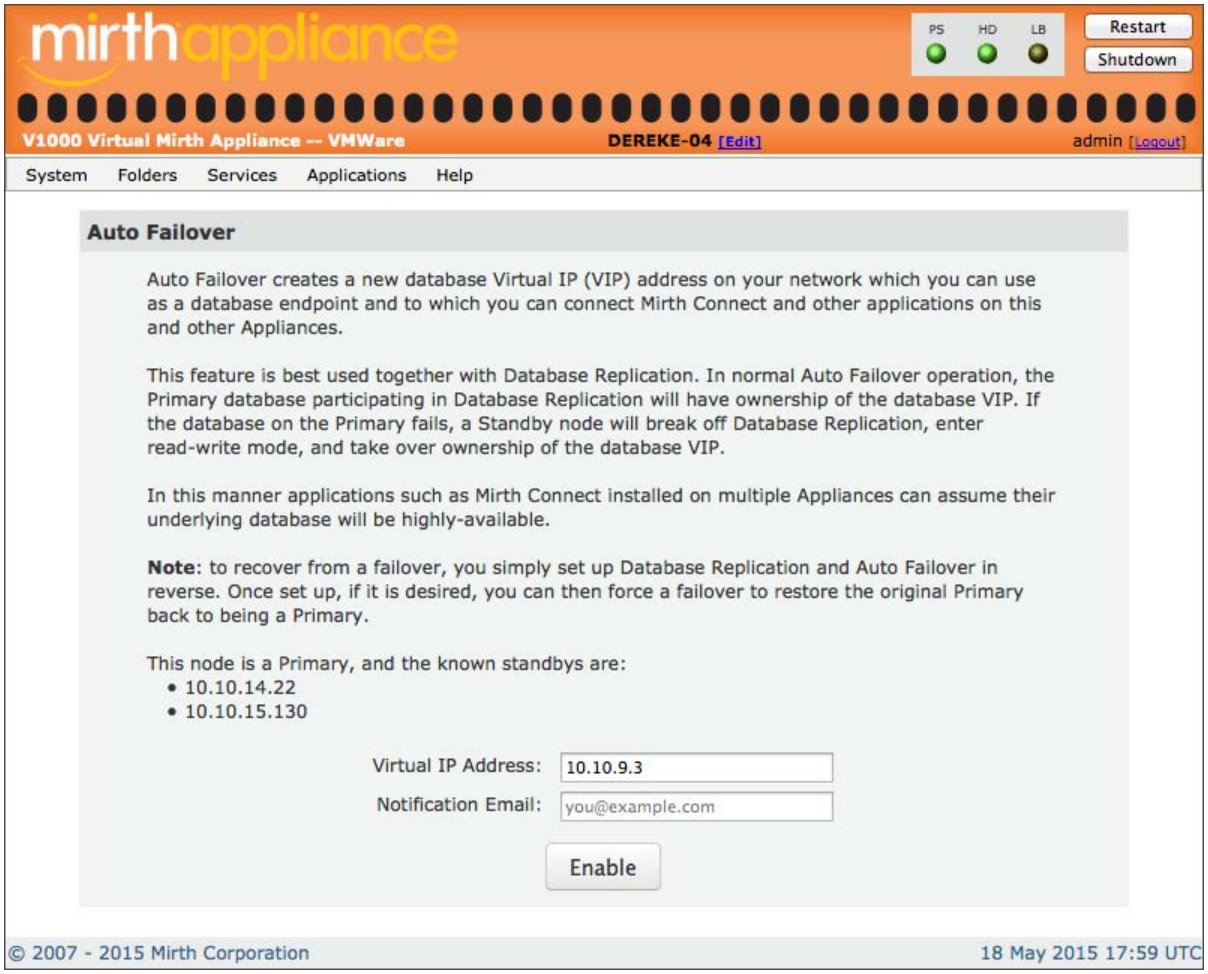
Before you start

You will need an unused IP address to assign as the Database Virtual IP (VIP) address:

- This VIP must be in the same IP network as the Appliances.
- You should ensure it's not already in use on your network, for example by using the `ping` command and verifying you receive no responses.
- Contact your network administrator or Mirth Support if you have any questions.

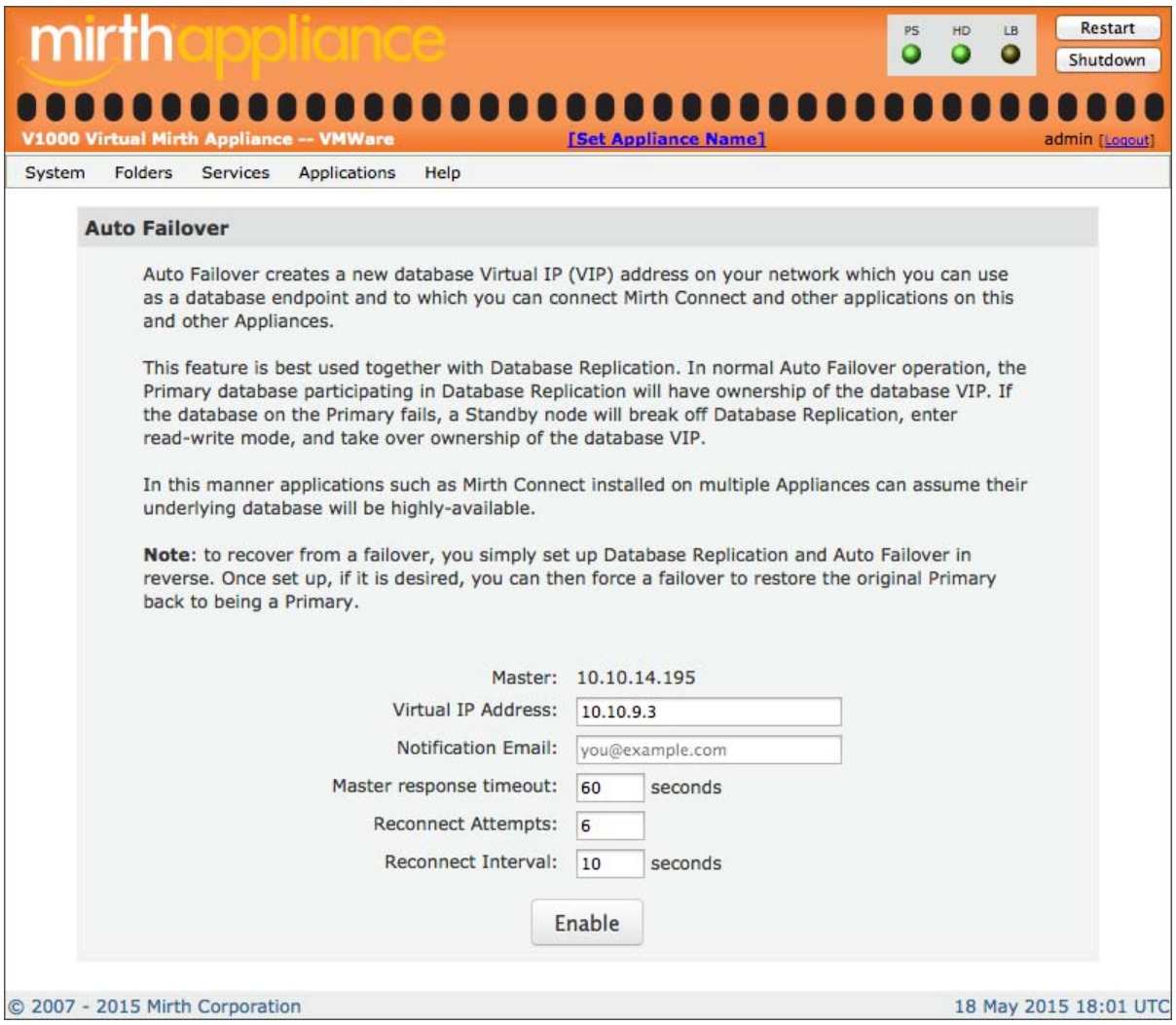
Set up first Appliance (the Primary)

1. Go to **Services > Postgres > Replication**
2. Click **Set up Auto Failover**
3. Enter your Database VIP.
4. Click **Enable**
5. Watch the page; it will reload automatically.
6. Ensure it eventually shows “Actively managing the VIP”



Set up second Appliance (the Standby)

1. Go to **Services > Postgres > Replication**
2. Click **Set up Auto Failover**
3. Enter the same Database VIP that you provided on the Primary. The default values for the timeout, attempts, and intervals should be fine to leave as-is.
4. Click **Enable**
5. Ensure it stays at “Listening for any existing VRRP masters”



After completing setup

At this point you have set up database replication and automatic failover on your two Mirth Appliances. All transactions committed to the Primary are being automatically replicated to the Standby in near real time. The Standby can be used for read-only reporting purposes, if desired (go to **Services > Postgres > Database Management** to set up access controls). Should the Primary unit become inaccessible, the Standby will break off replication, enter read-write mode, take over the Database VIP, and begin serving clients.

Viewing diagnostic information on both boxes

1. Go to **Services > Postgres > Replication**
2. Click **Advanced**
3. Click through the various pages; the **View Auto Failover Log** page reloads automatically and is good to watch while testing failover/failback

Manual Failback

After an auto failover has occurred, the primary database is temporarily out of the picture. Once the primary system is back in operation you may want to switch back to it again, and to do this failback you need to perform a manual series of steps. In short, this manual failback process is basically manually triggering another auto failover.

Failback steps

First, through VMware, resume the Primary VM. Then follow these steps:

1. On the Primary's **Postgres Replication Status** page (**Services > Postgres > Replication**), you will see:
    - “This Appliance currently does not own the VIP” and
    - "Should Own VIP: No, a former standby database has become active, we will defer to it”
2. Remove the old replicating Standby.
3. Click **Turn off Auto Failover**.
4. On the Secondary, click **Turn off Auto Failover**.
5. Click **Replicate from a remote database**.
6. Provide the IP of the Standby, then click through the rest of the wizard, then click **Done**.
7. Set up Auto Failover. (See the **Auto Failover** section of this deployment guide for more information.)
    - On the **Auto Failover** page, your Database VIP should already be present (add if not), leave timings at defaults, then click **Enable**.
8. Back on the **Postgres Replication Status** page, it will say:
    - "No, database is in recovery" and
    - "Listening for any existing VRRP masters"
9. Click **Stop replicating**, say **Okay** to the warning popup.
    - This step is what triggers the failback.
    - There are other ways to cause a failback, such as stopping Postgres on the Secondary and waiting. This way is simply fast.
10. Watch the **Status** page on both systems.
11. The Standby will relinquish the VIP and say “No, a former standby database has become active, we will defer to it”
12. The Primary will take over the VIP.
13. On the Standby:
    a. Click **Turn off Auto Failover**.
    b. Click **Replicate from a remote database**, provide the Primary's IP, click through the wizard, then click **Done**.
    c. Click **Set up Auto Failover**, the values should already be there, then click **Enable**.
    d. Verify you see "No, database is in recovery", and "Listening for any existing VRRP masters"

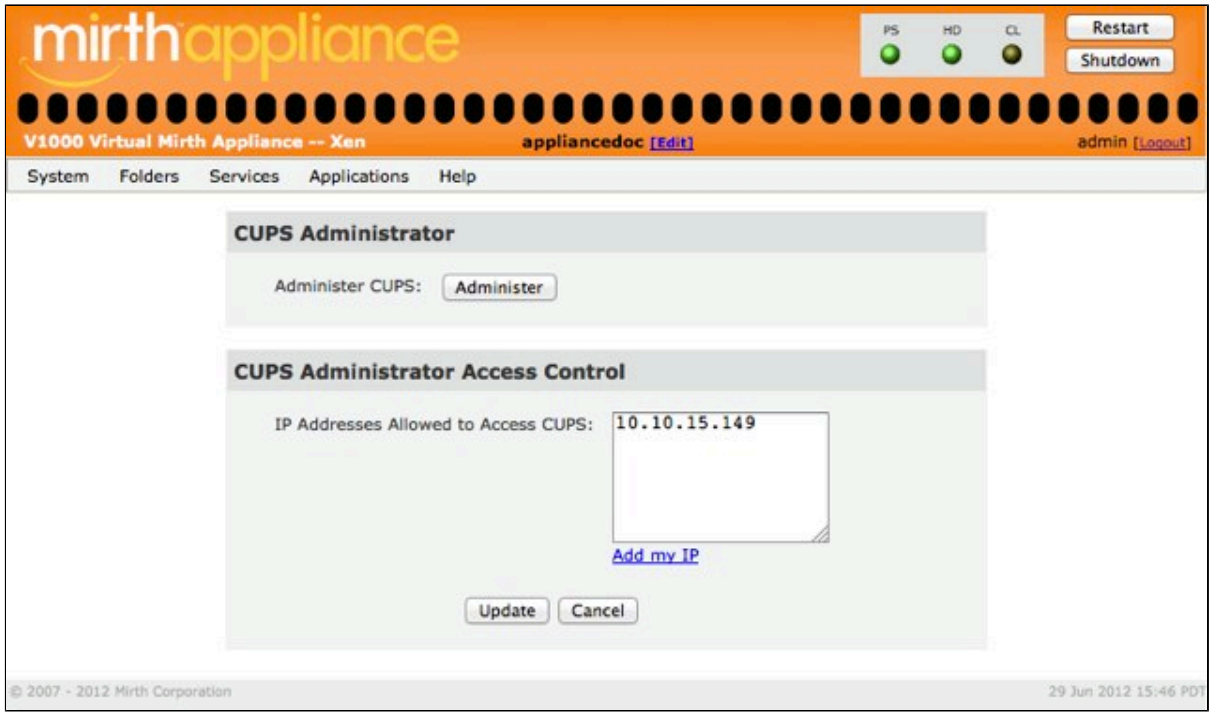
Viewing diagnostic information on both boxes

1. Go to **Services > Postgres > Replication**
2. Click **Advanced**
3. Click through the various pages; the **View Auto Failover Log** page reloads automatically and is good to watch while testing failover/failback

Printing

Mirth Appliances use CUPS (Common UNIX Printing System) to manage printing. The **Printing** service allows you to launch and control who has access to the CUPS Administrator.

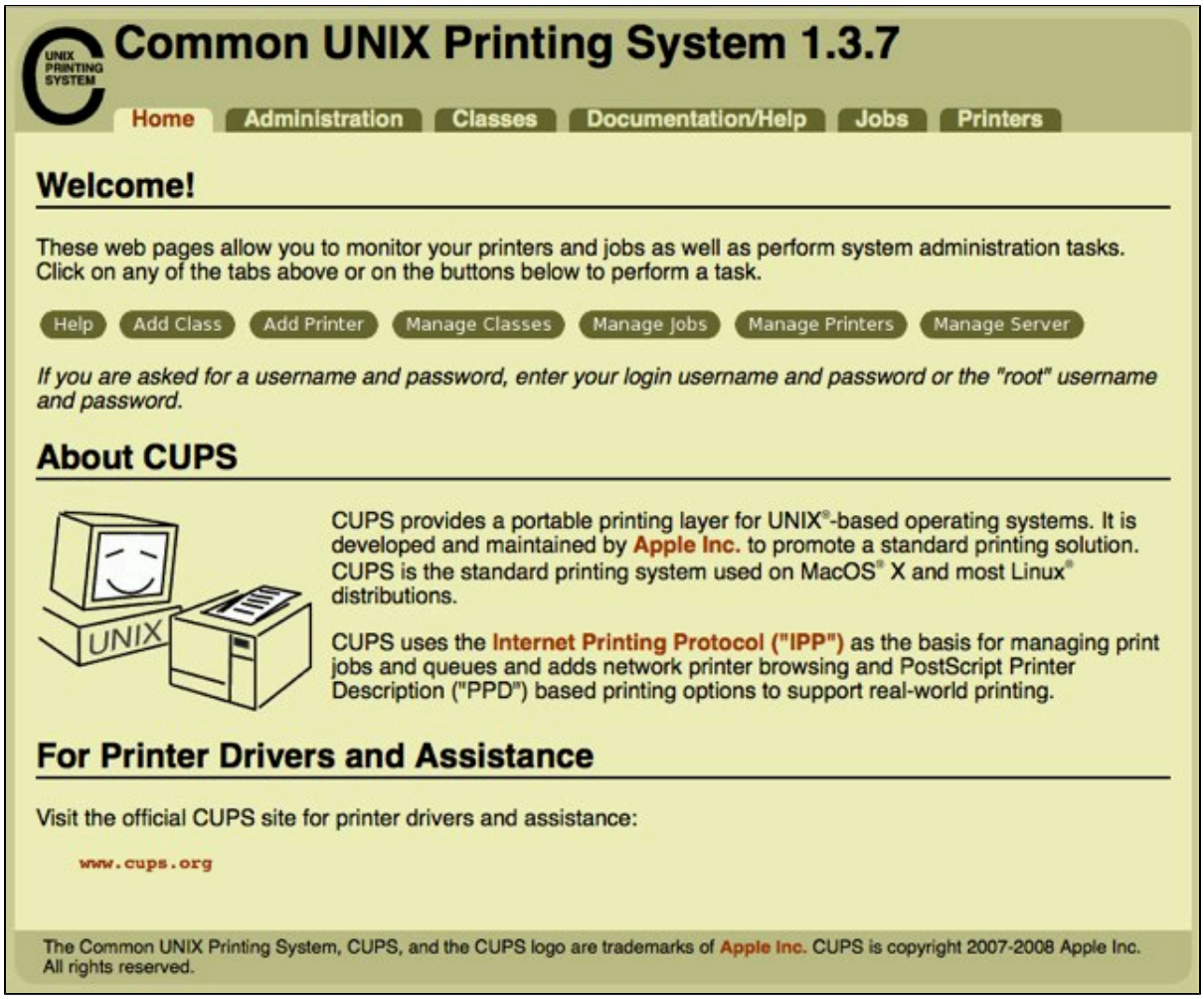
Before you can launch the CUPS Administrator, you must add your IP address to the list of IP addresses allowed to administer CUPS by using the CUPS Administrator Access Control section. You can enter your address manually, or you can click the **Add my IP** link, which will enter your address into the box. After your address appears, click the **Update** button.



Manage Printing Service

When your IP address has been added, click the **Administer** button to go to the CUPS administration page. From here you will be able to perform several print-related tasks such as **Add Printer**, **Manage Printers**, and **Manage Jobs**.

In-depth documentation is accessible from within the CUPS Administrator by clicking the **Documentation/Help** tab at the top of the page.



CUPS Administration Page

SFTP

The Mirth Appliance is capable of hosting an SFTP Server. SFTP is a secure file transfer protocol that uses SSH for authentication and encryption while presenting a user experience similar to FTP. There are many options for SFTP client software ranging from commercial to open source with broad platform support. It provides an easily accessible option for secure connections to the Appliance.

A secure space is setup on the disk for each SFTP user. This space, referred to as a "jail," is unique to each user and is not accessible by any other user. When a user logs in with an SFTP client, they will see three folders: *inbox*, *outbox*, and *processed*. The folder names mimic the default folder names for Mirth, but users are free to delete the default folders, add new ones, or otherwise set up any folder structure that suits their needs.

SFTP User Management

The **SFTP User Management** page allows you to add or modify SFTP users. Click the **Add User** button to add a user; click an existing user's name to modify the user's full name or set the user's password, or to delete the user. Click **Cancel** to go to the **Services Control** page.

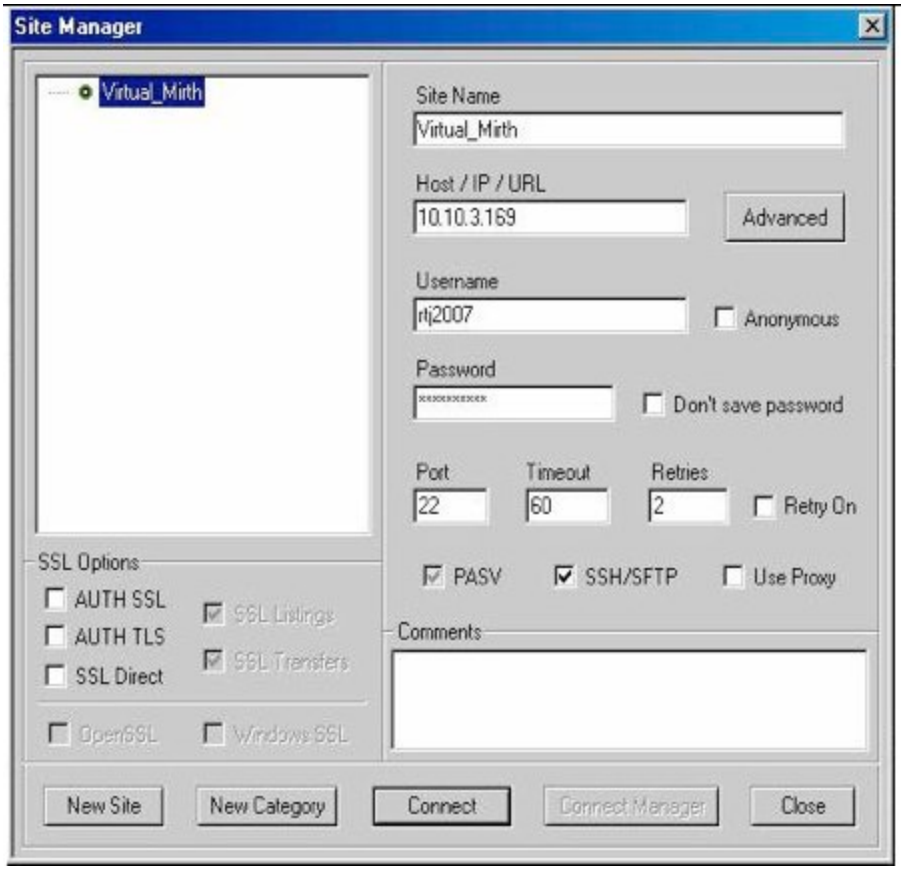
Click the **Add User** button on the **SFTP User Management** page to add an SFTP user. On the **Add SFTP User** page, enter a username for the user, the user's full name, the user's password, and repeat the password to confirm it. Click the **Add** button to add the SFTP user.

Add SFTP User

An existing user can be edited by clicking on the linked name in the list on the **SFTP User Management** page. When editing a user, you can change their **Full Name**, assign a **New Password**, or delete their account. Deleting an account also removes the associated files from the disk.

Edit SFTP User

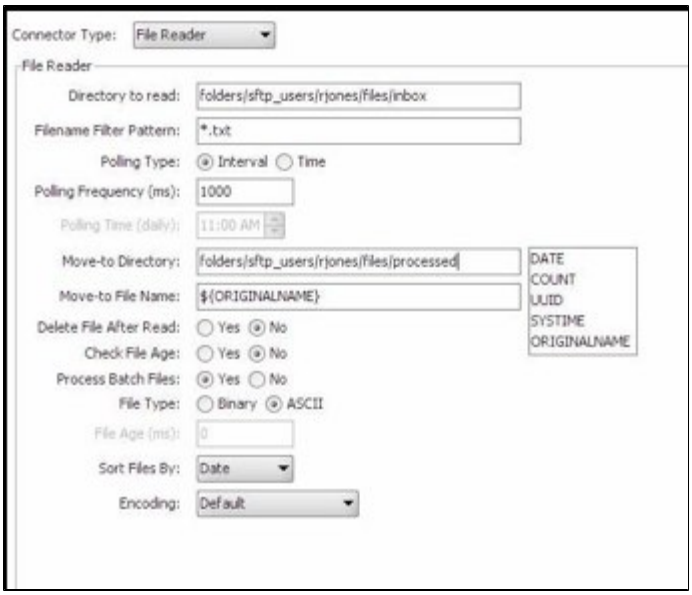
SFTP transmissions are run on port 22. Using the credentials set in creating an SFTP, you can connect to the SFTP folders with a variety of FTP clients. The example below shows a connection from the Windows freeware client Core FTP LE.



Connecting to SFTP folders on a Mirth Appliance.

The username and password must match the credentials for the SFTP account set up on the Appliance.

All SFTP user folders and files are visible through the Folder browser in the Appliance control panel, and the administrator can centrally manage the users' files. Mirth channels can also reference the private user SFTP folders using the File Reader and File Writer connector types. It is not necessary to use the SFTP connector since the folders are stored on the local file system.



Accessing an SFTP user's files with the File Reader connector type

The SFTP user files directory is referenced from the connector with the following path:

```
folders/sftp_users/<username>/files/<folder>/
```

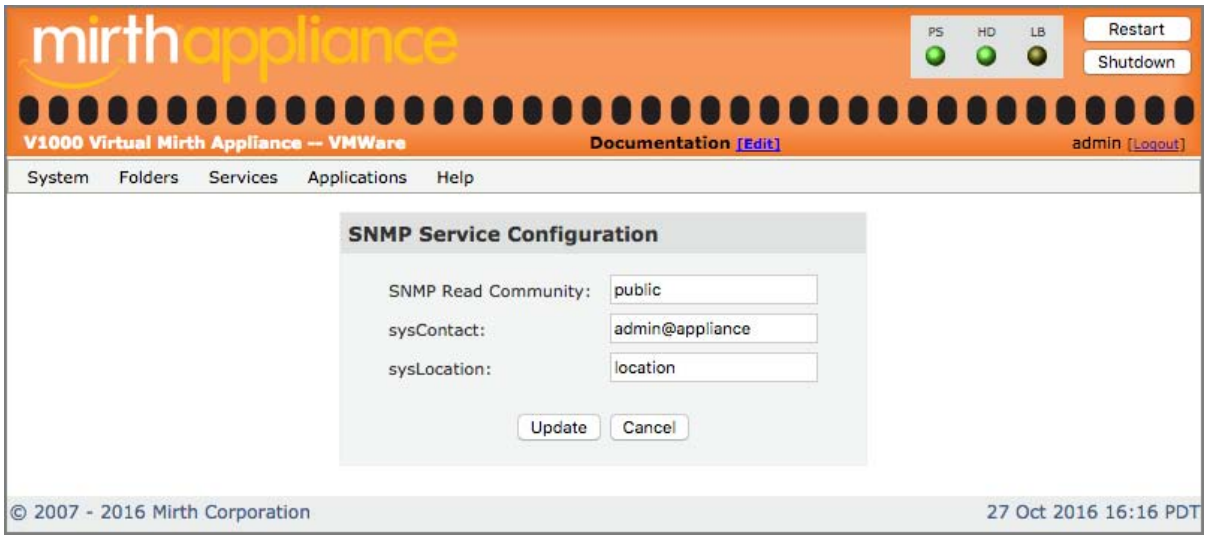
For example, to access the inbox folder for the user *jharris,* you would enter "folders/sftp_users/jharris/files/inbox/" in the **Directory to read** field of the File Reader connector.

SNMP

The Simple Network Management Protocol (SNMP) is part of the Internet protocol suite as defined by the Internet Engineering Task Force (IETF). SNMP is used in network management systems to monitor network-attached devices for conditions that warrant administrative attention. It consists of a set of standards for network management, including an Application Layer protocol, a database schema, and a set of data objects.

SNMP exposes management data in the form of variables on the managed systems, which describe the system configuration. These variables can then be queried (and sometimes set) by managing applications. SNMP version 2c is required to retrieve monitoring information from the Mirth Appliance.

With SNMP you can monitor information about your Appliance such as network utilization, memory usage, and Mirth Connect channel activity. This is accomplished by importing the Mirth Appliance MIB (Management Information Base) into an SNMP browser or your existing SNMP monitoring tool of choice. The Mirth Appliance MIB can be downloaded from your Appliance (Help>Downloads).



SNMP Service Configuration (SNMP community string)

This **SNMP Service Configuration** page allows you to set the community string to access the SNMP server.

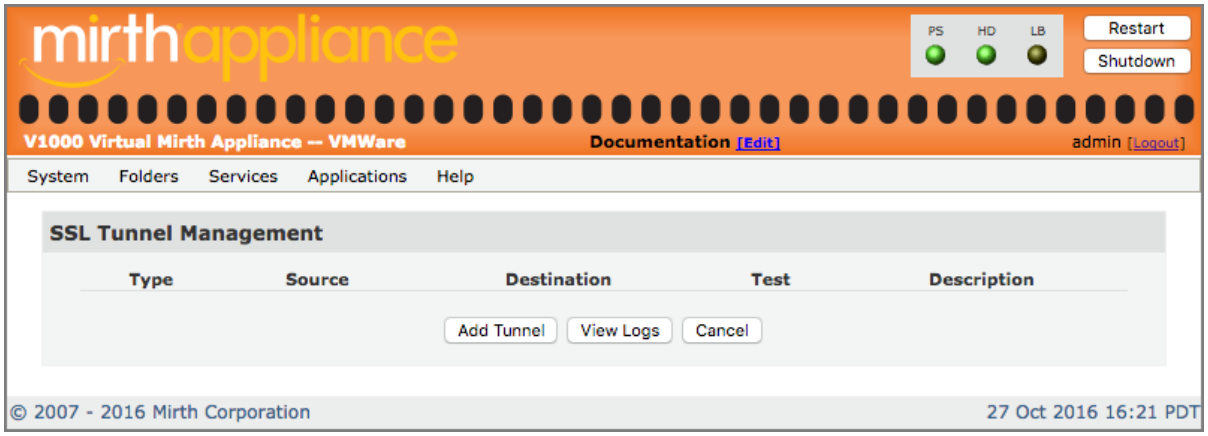
SSL Tunnels

SSL stands for Secure Sockets Layer, and is a cryptographic protocol for providing secure communications over TCP/IP networks. The use of SSL allows you to securely exchange messages over public networks such as the Internet.

The SSL Tunnels service allows Mirth Appliance users to accept SSL connections for any of the listener-based Mirth Connect connector types such as HTTP, LLP/MLLP, SOAP, and TCP. It also allows you to add SSL to the corresponding destination connectors.

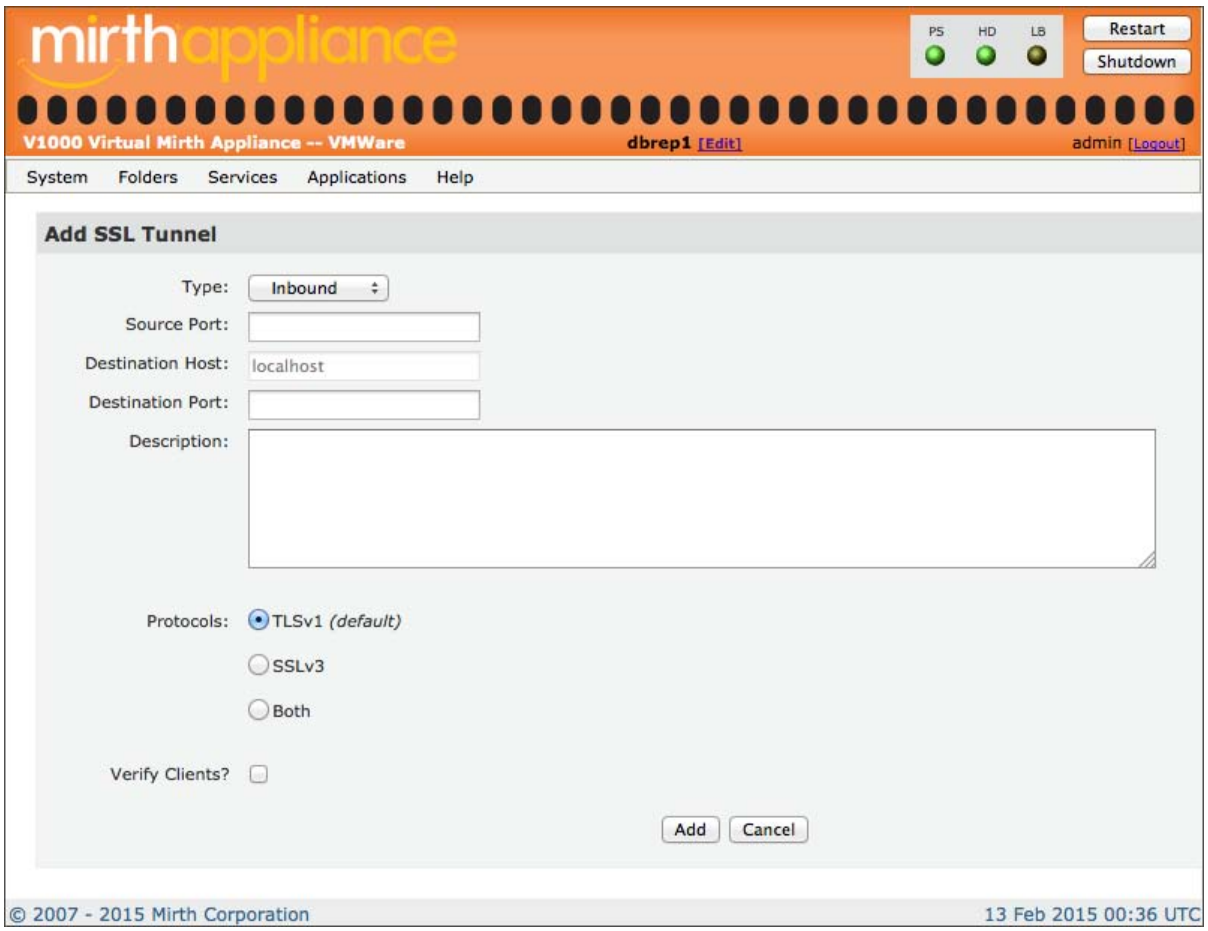
Inbound tunnels accept an SSL connection from a remote host and pass it to the listening port of a Mirth Connect channel on the local system. Outbound tunnels listen on a local port for a Mirth Connect destination connector, add an SSL layer to the connection, and pass it on to a specific remote host.

⚠ Please consult your network admins regarding setting up two-way SSL authentication.



SSL Tunnel Management

The **SSL Tunnel Management** page shows all of the currently configured tunnels on the system. Click the **Add Tunnel** button to create a new inbound or outbound SSL tunnel. Click the name of an existing SSL tunnel to modify or delete it.



Add SSL Tunnel

On the **Add SSL Tunnel** page specify the **Type** of tunnel, **Source Port**, and **Destination Port**. For Outbound tunnels only, you will need to specify a **Destination Host** as well. Click the **Add** button when you are done.

To edit or delete an SSL tunnel, click the source port of the tunnel on the **SSL Tunnel Management** page. This takes you to the **Edit SSL Tunnel** page. On this page, you can modify the destination port on an *Inbound* tunnel or the destination host and port for an *Outbound* tunnel, or delete a tunnel.

To receive HL7 messages via HTTPS, first you would create an HTTP listener as the source connector. Next, you would create an inbound SSL tunnel. Choose an arbitrary source port (we recommend 9000-9999), and set the destination port to match the listener port. Communicate the port you chose to the message sender to use as their destination.

In order to send HL7 messages over HTTPS, first you would create an outbound SSL tunnel. Choose an arbitrary source port (we recommend 9000-9999), and then supply the destination host and port of the recipient. Next, you would create an HTTP sender destination using a URL in the form of http://localhost:<port> where <port> is replaced with the source port you chose for your SSL tunnel.

⚠ ***Note:*** *For SSL certification, see Certificates under System Administration.*

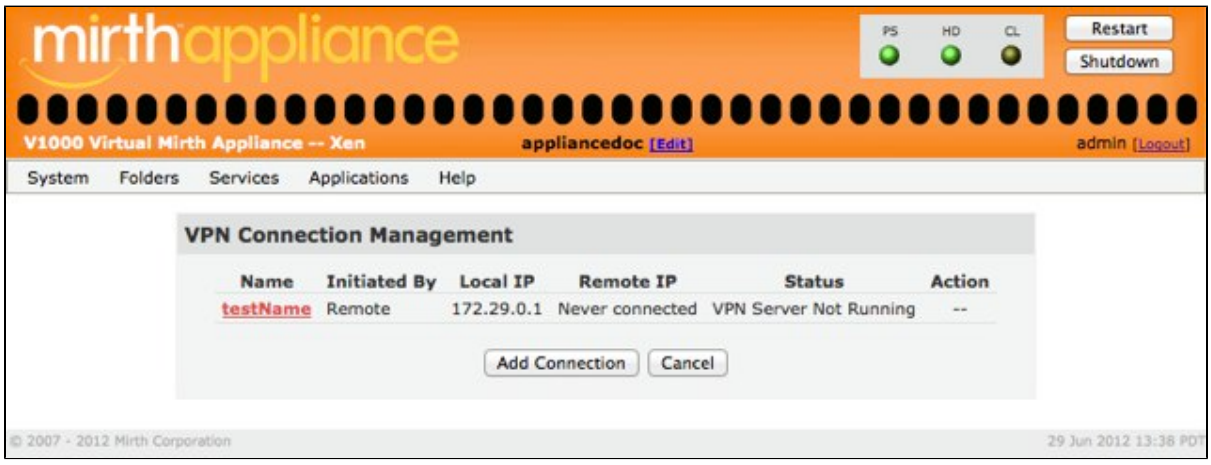
VPN Connections

VPN stands for Virtual Private Network. A VPN allows you to create a secure channel of communication (a.k.a. a "tunnel") over a public network such as the Internet. Security is provided through authentication, to ensure that the entity connecting is authorized, and through encryption, to protect the data in transit.

The VPN service uses certificate-based SSL authentication. This means that each VPN user that you configure will have a unique certificate generated and assigned to them. When a user attempts to connect to the service, their VPN client must present a valid certificate for the VPN to be established. The VPN service uses the Advanced Encryption Standard (AES) cipher algorithm in Cipher Block Chaining (CBC) mode with a 256-bit key.

VPN connection management allows you to terminate client-based VPN connections directly on your Mirth Appliance. Once established, these connections provide a secure path for administrative or message traffic. Each connection is authenticated with a unique digital certificate, and all traffic is encrypted. The VPN Service is for inbound VPN connections only and will not connect to a different vendor's VPN.

> ***Note:*** *Before you can manage a VPN connection, you must personalize your Appliance by setting the name for the Appliance (Applications > Control Panel Management > Manage Control Panel) and setting a contact email address (System > Mail). The contact information and e-mail address are used when setting up new VPN users.*



User list on VPN User Management page shows connection status.

The **VPN Connection Management** page shows a list of all currently configured VPN connections.

If a connection has never connected to the Appliance, the Remote IP status will display "Never connected," and the connection's name will be displayed in red.

Connections that have previously connected will show an assigned private IP address, displayed in green if their connection is active and red if it is not. When a user is actively connected, the Appliance can initiate a connection to the client over the VPN by using the listed private IP address.

Adding a User

Click the **Add Connection** button to get to the **Add VPN Connection** page.

Add VPN Connection

From this page select the type of connection. There are two type options. The default type is *Connection to this appliance* and is used to create a package that allows Windows, Linux, or another appliance to connect to you. The second type is *Connection to another appliance* and requires you to have a VPN package already downloaded from another Appliance onto your PC. Enter a unique name for the connection. Click **Add** to add the connection. You will be taken to the **Download VPN Software Bundle** page.

Downloading a VPN Client Software Bundle

After adding a connection, the next step is to download a VPN Client Software Bundle to send to the user. On the **Download VPN Software Bundle** page, select the VPN user's **Platform** (*Windows* or *Linux*), the **Public Server Address**, and a password for encrypting the software bundle's contents.

Download VPN Bundle

The **Public Server Address** field is the IP address that the client will use to connect to the Appliance. If the user is connecting over an existing private network, they may be able to connect to the actual IP address of the Appliance (this is the default value). More than likely, the user will be on the other side of a firewall and it will be necessary to give them an external IP address. You can attempt to look up the external IP address of the Appliance using the **Detect External IP Address** button. If there are any questions about which IP address to use, contact your network administrator.

> ⚠ ***Note:*** *If there is a firewall between the user and the Appliance, then the Public Server Address displayed on the Download VPN Software Bundle page is probably NOT the correct IP address for the user.*
>
> *For a "typical" network configuration, where the Mirth Appliance is behind a firewall, with NAT enabled, you can click on the "Detect External IP Address" link to get your Appliance's external IP address.*
>
> *If the IP address provided by the link does not work for your external users to connect to the Mirth Appliance, then consult your Network Administrator to find a valid IP address for the Appliance.*

The optional password you can enter in the **Password for Software Bundle** field is used to protect the client software and certificate in transit. The user will need the password from this page to open the bundle (zip file).

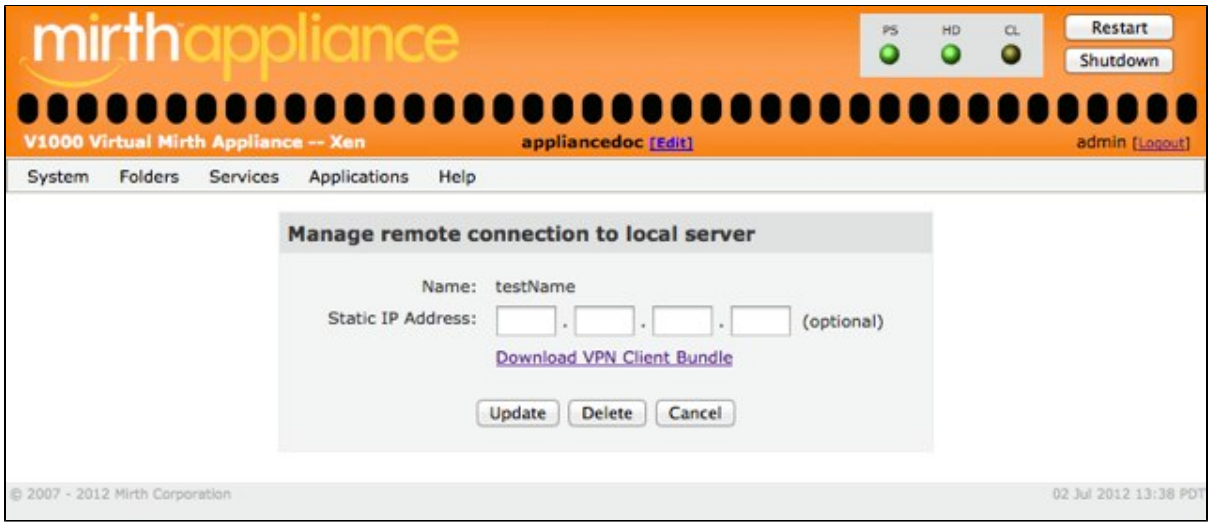
When you are finished with all entries, click **Download** to download the software bundle. Send the bundle to the VPN user. After following the simple instructions, the user will be able to connect using the provided digital certificate without having to use a password in the VPN client.

Editing or Deleting an Existing User

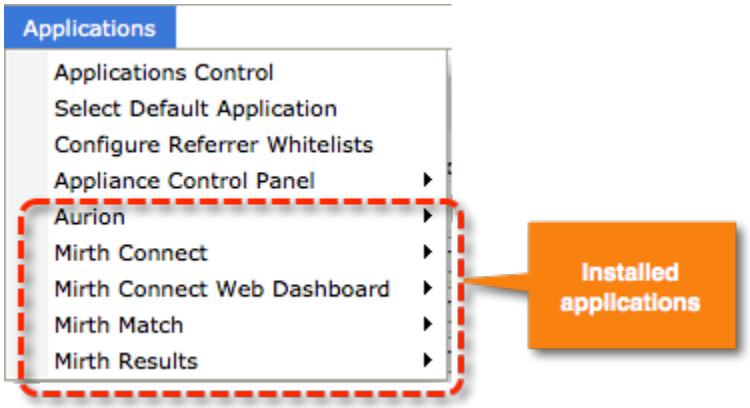
To edit an existing user, click on the linked name in the list on the **VPN Connection Management** page. You can update the IP address, download an updated client software bundle to send to the user, or delete the user.

To delete the user, click the **Delete** button and verify you want to delete the connection. To return to the **VPN Connection Management** page without making any changes, click the **Cancel** button.

Deleting a user immediately revokes the digital certificate and disconnects them from the system. The number of VPN users is limited by the size of the private network defined. The default private network configuration allows for 63 VPN connections. The number of concurrent connections is only limited by the processing capacity of your Mirth Appliance.



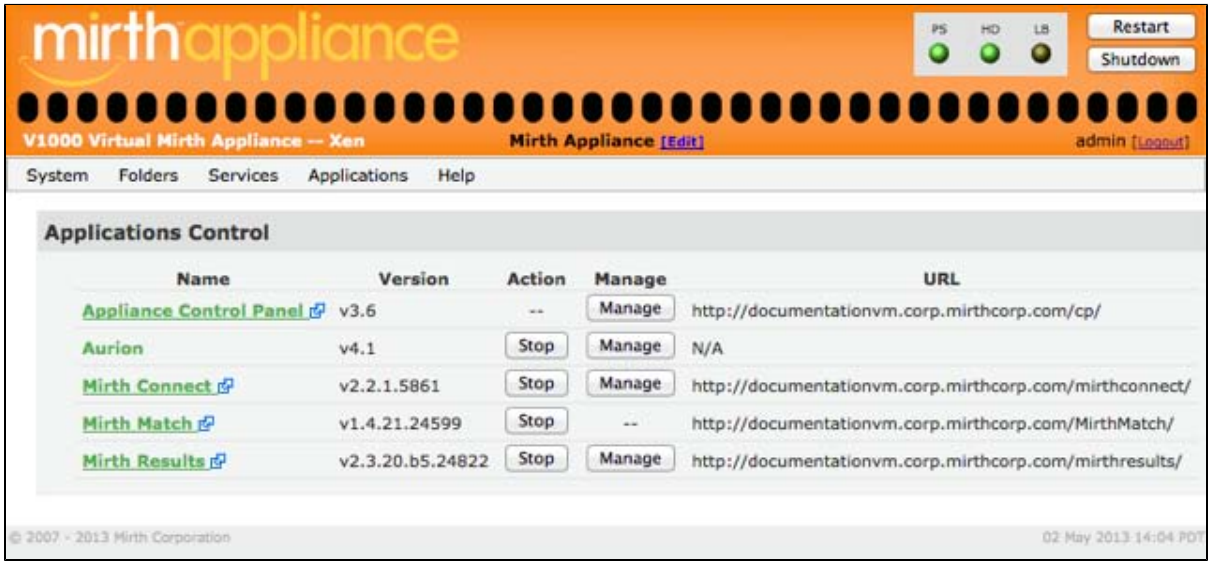
Applications Menu



The **Applications** menu allows you to configure the Control Panel and any applications installed on the Appliance. The Control Panel and each installed application will appear in the menu, with a sub-menu allowing you to **Launch** and/or **Manage** the application. You can also do these tasks directly from the **Applications Control** page.

It is likely that you will have Mirth Connect installed as one of your applications. The sub-menus for Mirth Connect contain some extra choices, including **Clustering**, which is discussed in the **Mirth Connect > Clustering** section of this guide.

Applications Control



Applications Control

The **Applications Control** page displays a list including the Control Panel and all installed applications. The name of each application is a link; clicking the link launches the application in a separate browser window. The list also shows the version of the application, an **Action** button which allows you to start or stop the application (depending on whether or not it is currently running), a button to **Manage** the application, and the URL for accessing the application directly.

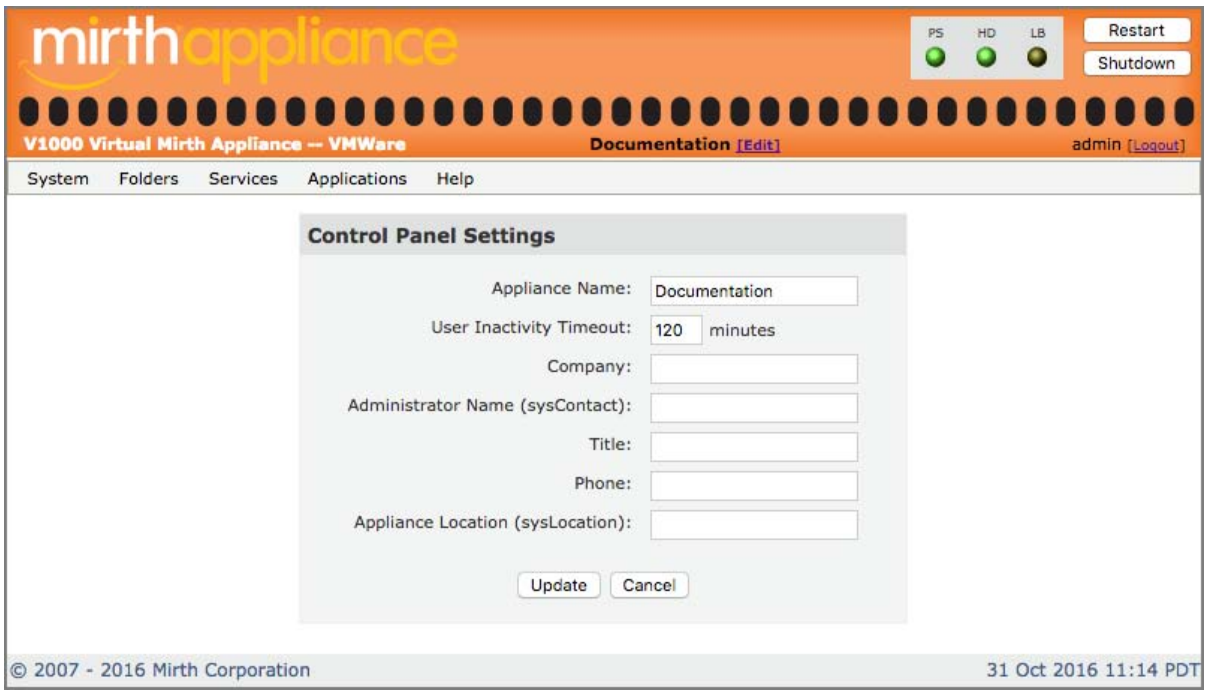
(In previous versions of the control panel software, this page was also used to set the default application. To do that now, choose **Applications > Select Default Application** from the menu to go to the **Select Default Application** page.)

⚠ The functions available here on the **Applications Control** page are also available by going to the menu entry in the **Applications** menu for each application, and selecting **Launch** or **Manage** in the sub-menu that appears. In some cases, the **Manage** entry will itself have another sub-menu.

The pages that you go to to perform any of these functions are the same regardless of whether you go to them through the **Applications Control** page or through the entries for the applications on the **Applications** menu; these are simply alternate paths to get to the same places.

Manage Control Panel

Clicking the Control Panel's **Manage** button opens the **Control Panel Settings** page.



Control Panel Settings

The **Control Panel Settings** page allows you to personalize the Mirth Appliance. You can (and should) set a unique **Appliance Name** to identify the Appliance; you can also set the **User Inactivity Timeout** period, the name of your company, and the name, title, and contact number for the Appliance's administrator. It is very important to set the **Appliance Name**, especially in cases where there is more than one Appliance on the same network or managed by the same person.

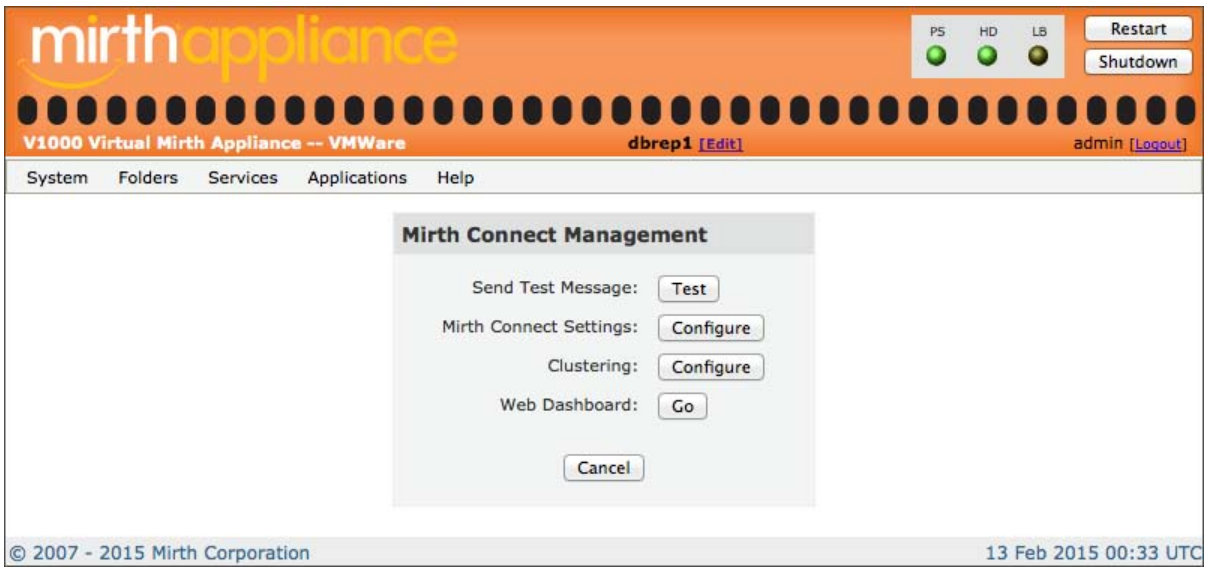
The Administrator information will be included in the VPN instructions sent to VPN users, as the administrative contact in case of problems with the VPN.

After making these settings, click the **Update** button to save the settings. Click the **Cancel** button to return to the **Control Panel Management** page.

If you update the **Administrator Name (syscontact)** and/or **Appliance Location (syslocation)**, these changes will also appear in the **sysContact** and **sysLocation** fields on the **SNMP Service Configuration** page (which you get to by going to **Services > SNMP**).

Manage Mirth Connect

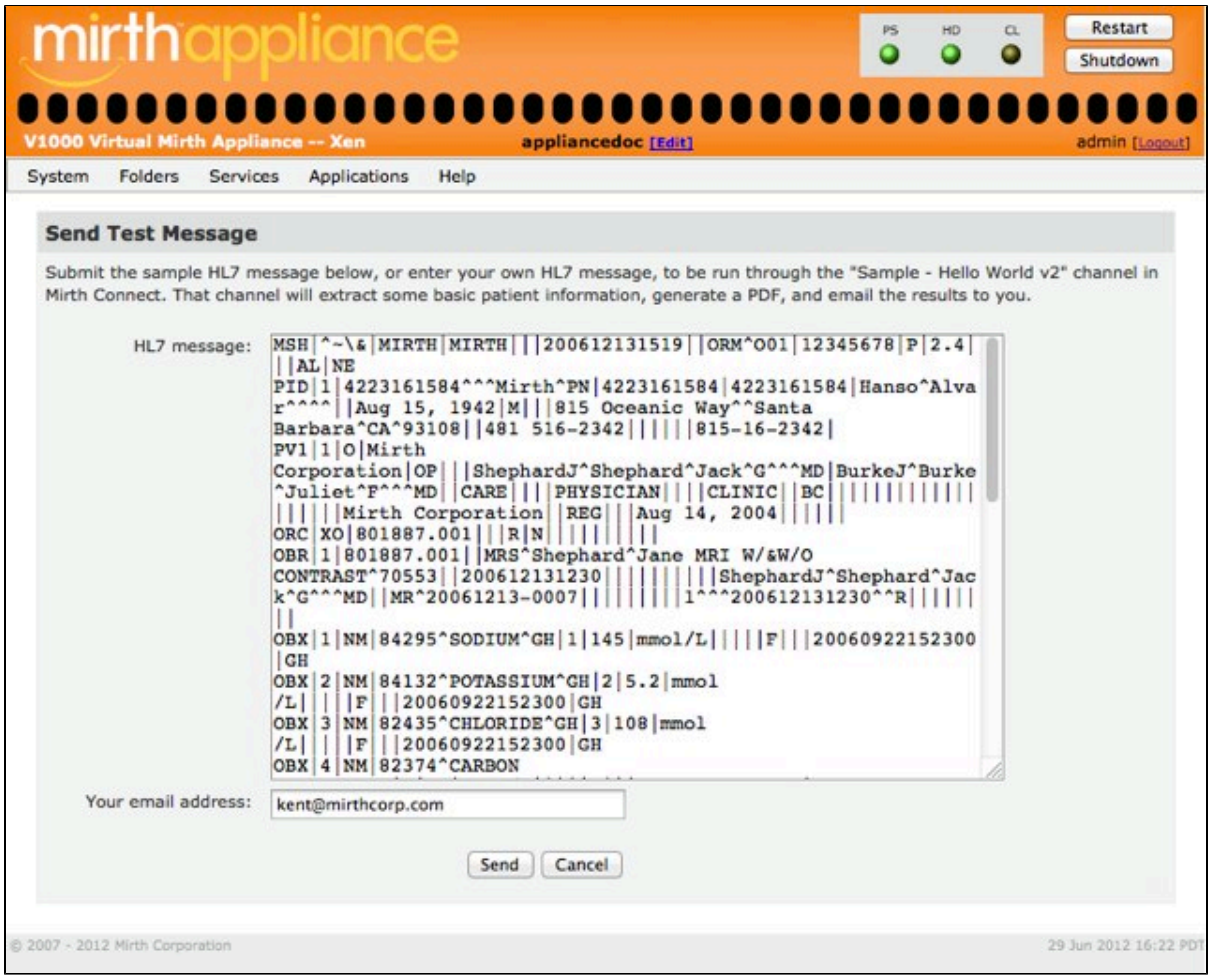
There are two ways to go to the **Mirth Connect Management** page: (1) on the **Applications Control** page, click the **Manage** button on the row for Mirth Connect, or (2) from the menu, select **Applications > Mirth Connect > Manage**.



Mirth Connect Management

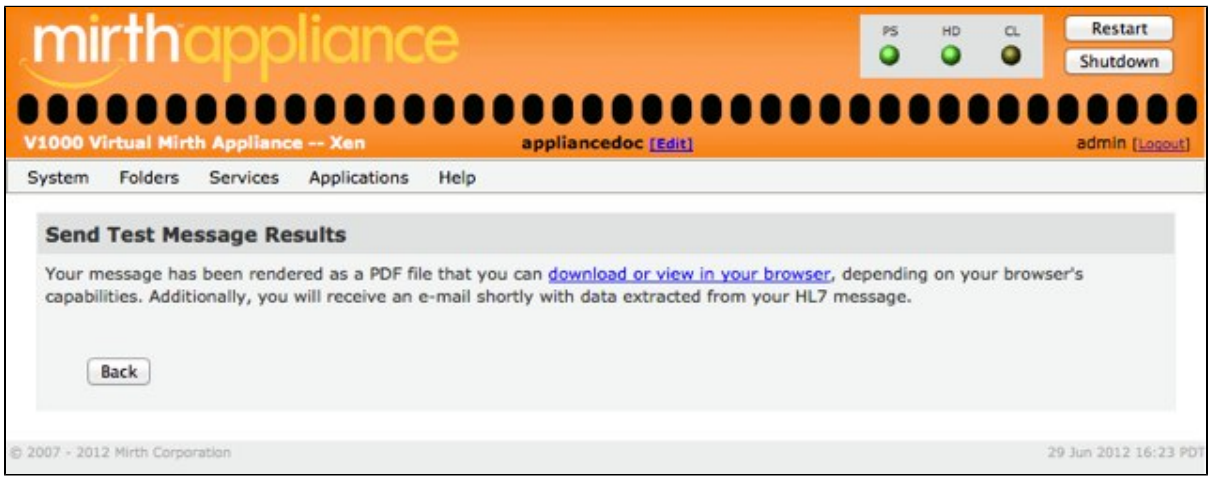
On the **Mirth Connect Management** page you can send a test message through Mirth Connect to confirm that it is working and that email delivery is properly configured. You can also configure Mirth Connect by adjusting the maximum heap size (the amount of memory allocated to Mirth Connect) and adjusting the Mirth Connect and database logging levels.

Click the **Test** button on the **Mirth Connect Management** page to go to the **Send Test Message** page.



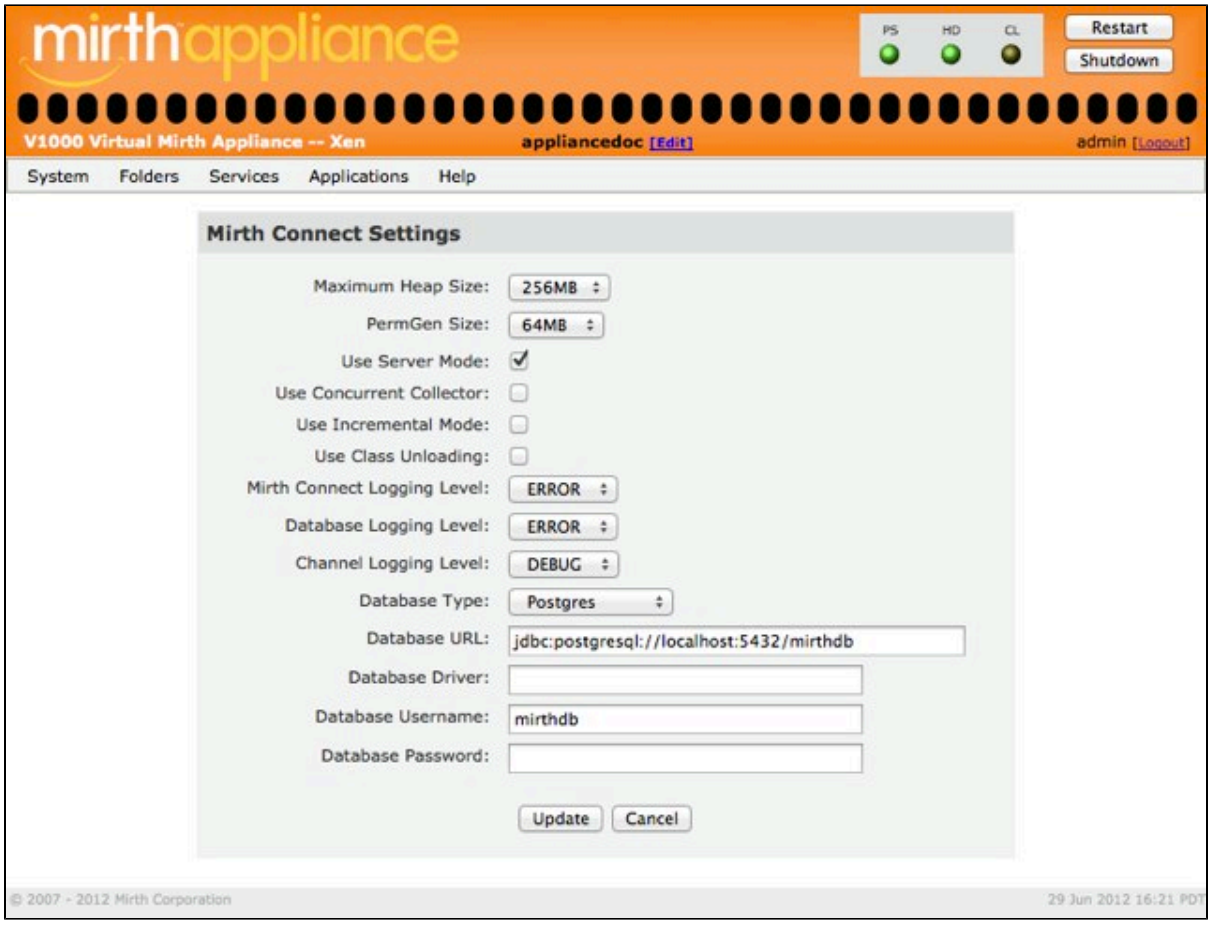
Send Test Message

Click the **Send** button to send the sample HL7 test message to the sample Mirth Connect channel (or send your own message). The test message will extract some sample data, generate a PDF, and email the results to you (if the email address displayed on the page is correct).



Send Test Message Results

Click the **Configure** button on the **Mirth Connect Management** page to go to the **Mirth Connect Settings** page.



Mirth Connect Settings

On the **Mirth Connect Settings** page you can set various memory settings for Mirth Connect. In most cases, the default options are sufficient, and we recommend not changing the options unless you are an advanced user, and you are trying to solve a specific memory problem as described below:

- ***Maximum Heap Size:*** sets the maximum heap size (amount of memory) allocated to Mirth Connect. The default setting is the minimum amount recommended for Mirth Connect. The amount should only be increased if Mirth Connect reports OutOfMemory errors.
- ***PermGen Size:*** sets the permgen size. The amount should only be increased if Mirth Connect reports OutOfMemory: Permgen space errors, or other errors that may indicate a problem with insufficient permgen space (e.g., String, intern or ClassLoader.defineClass exceptions).
- ***Use Server Mode:*** the default setting is to use server mode, and we recommend not changing this.
- ***Use Concurrent Collector:*** check this option to enable the concurrent collector.
- ***Use Incremental Mode:*** check this option to use concurrent collector in incremental mode. This is useful when running on a machine with a small number of processors (e.g., 1 or 2).

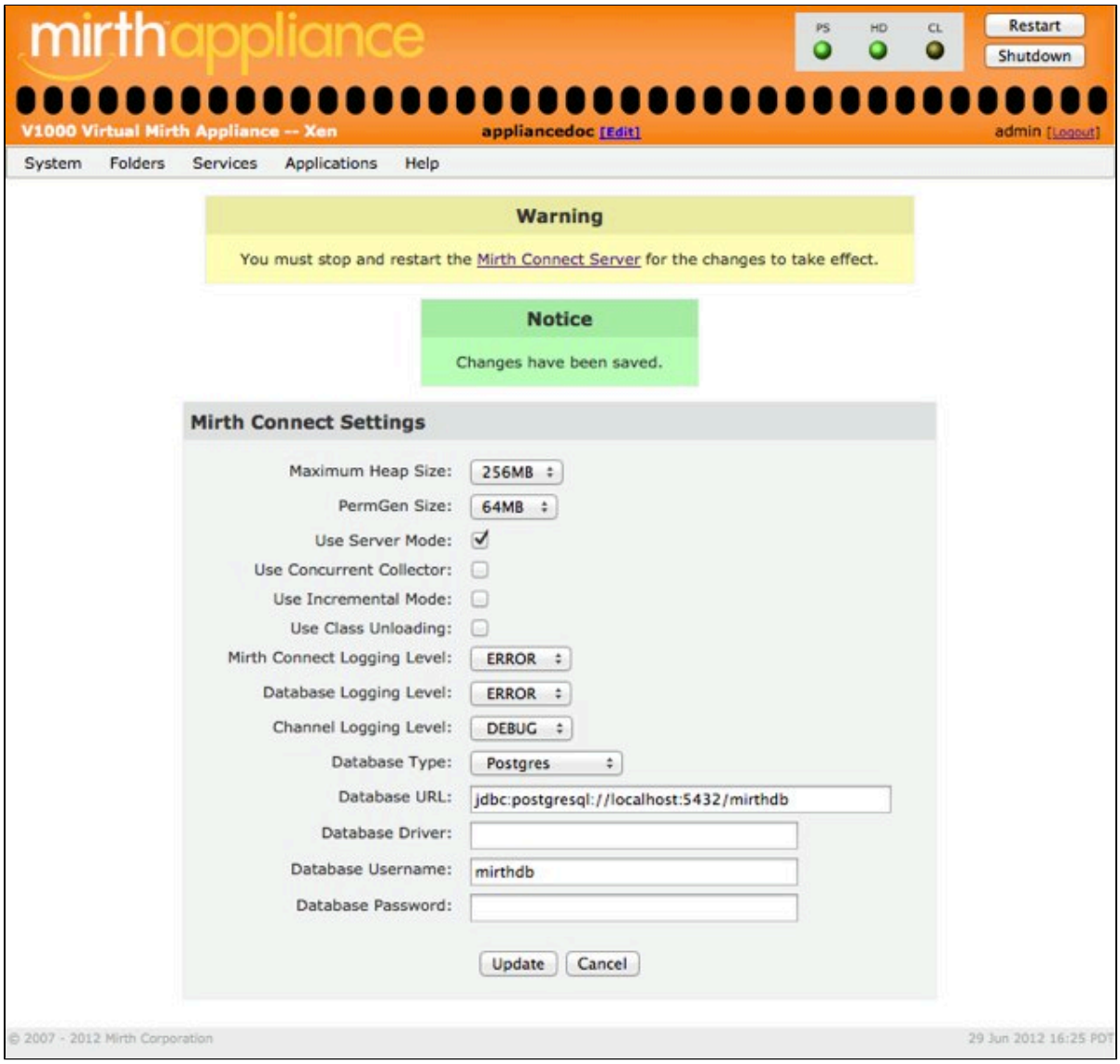
- ***Use Class Unloading:*** check this option to enable class unloading in the concurrent collector. This may help resolve permgen errors.

You can also adjust the logging levels for the Mirth Connect application, the Mirth Connect database, and the Mirth Connect channels. This can be useful for debugging problems.

If you are interested in using an external database with Mirth Connect, you can modify the following settings below:

- ***Database Type:*** sets the type of the database to be used. The choices are: *Derby*, *Mysql*, *Postgres*, *Oracle*, *Sqlserver2000*, and *Sqlserver*.
- ***Database URL:*** sets the JDBC URL with which to connect to the database.
- ***Database Driver:*** an optional setting. Enter the driver here if it differs from the standard one.
- ***Database Username:*** the username with which to connect to the database.
- ***Database Password:*** the password with which to connect to the database.

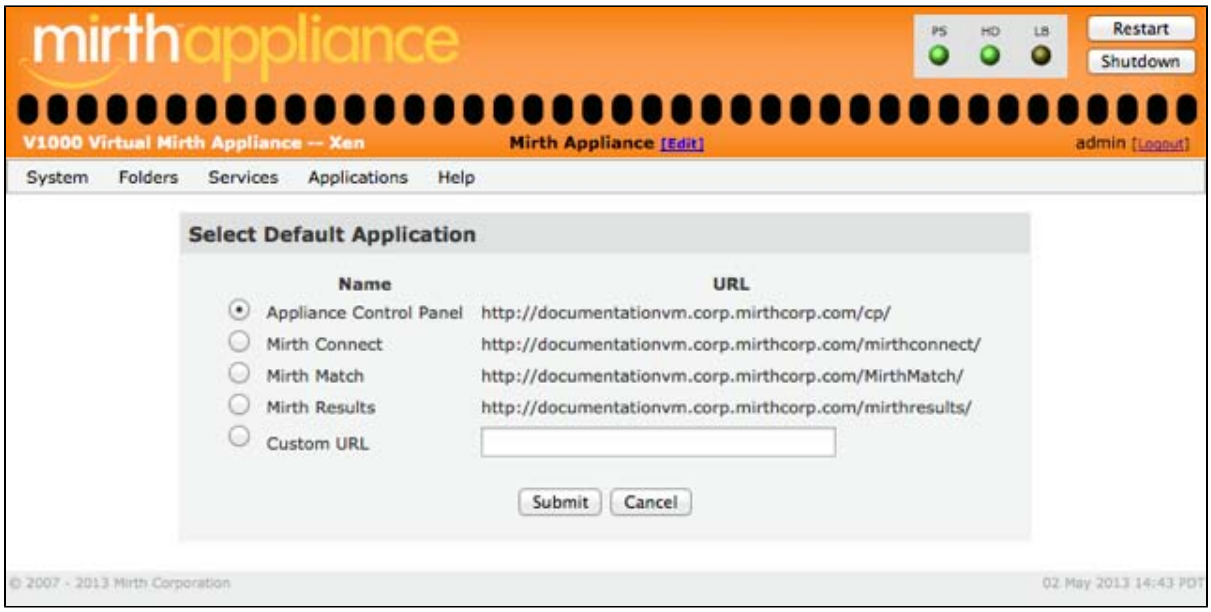
After adjusting settings, click the **Update** button. The Appliance must be restarted for changes to take effect.



After changing Mirth Connect settings, the Appliance must be restarted

Select Default Application

You can use the **Select Default Application** page to designate the application that is displayed in a web browser when you go directly to the Appliance's base URL.

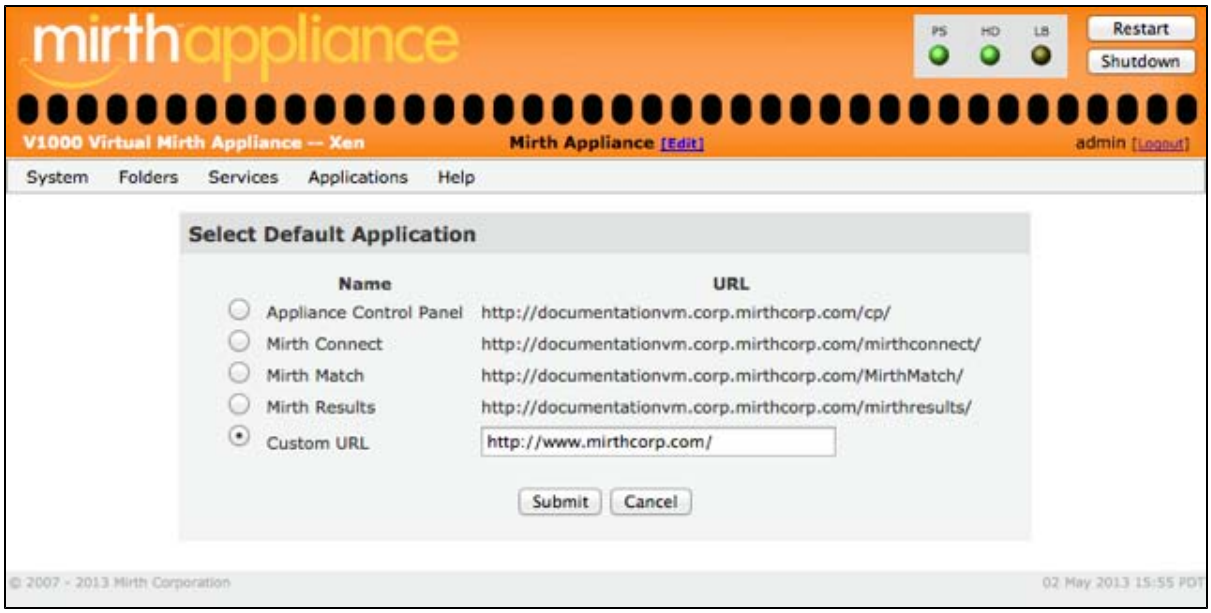


Select Default Application

The default for the default application is *Appliance Control Panel*. This means that for a new Appliance, when you type **http://<appliance_base_address>/** into your browser's address bar (where <appliance_base_address> is the host/domain name or IP address of the Appliance), the **Appliance Control Panel** page will be loaded. To go to a different application, you would need to use the full URL for that application, which generally has a form of the application name added to the to the base URL.

If you come here to the **Select Default Application** page, select any listed application, and then click **Submit**, that application becomes the new default. Now when you go to **http://<appliance_base_address>/** in your browser, you will be redirected to the selected application. This also means that to get to the control panel, you now need to use its full **http://<appliance_base_address>/cp/** address.

The last choice in the list is *Custom URL*. If you select this item, you can type any web address into the box, and then click **Submit**. Now when you to go to **http://<appliance_base_address>/**, you will be redirected to the address that you typed in. In the example below, the Appliance base URL would take you to the Mirth Corporation home page, http://www.mirthcorp.com/.

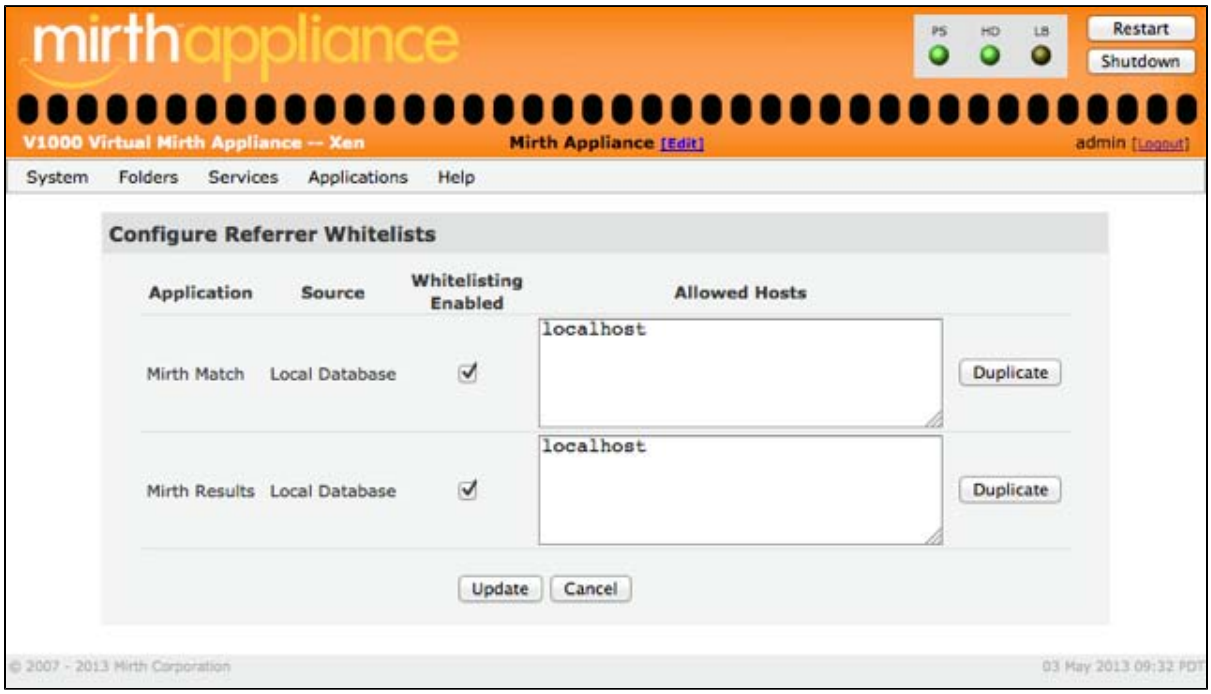


Select Default Application, Custom URL

Configure Referrer Whitelists

This is an advanced configuration page which will not normally need to be accessed in the day-to-day operation of the Appliance.

Several of the Mirth applications have a security feature to help prevent CSRF (Cross-Site Request Forgery) attacks. The HTTP referrer header on every page access is checked to verify that the referrer is from a list of trusted domain names. This list cannot be automatically determined, however, and must be configured manually for every single installation. This page is available here in the Control Panel to assist in managing this list of trusted domains.



Mirth Connect > Clustering

Mirth Connect is likely to be installed on your appliance, which means there will be a Mirth Connect menu entry in the **Applications** menu that will give you access to the configuration screens for Mirth Connect clustering that are described here.

Overview

Mirth Connect has the ability to run in a clustered environment to provide high availability and improved performance. Enhancements to clustering are provided by Mirth Appliances, as well as an Advanced Clustering Plugin made available to Platinum subscribers.

This section describes how to set up two Mirth Appliances, previously set up with Database Replication and Auto Failover, and Mirth Connect's Clustering plugin, to provide a highly-available network endpoint for message processing backed by a single, highly-available database.

You can perform the setup process in two different ways, which are described in the following sections of this guide:

- **Mirth Connect Clustering Wizard** – this guides you step-by-step though the setup process
- **Manual Setup for Mirth Connect Clustering** – this method uses the Appliance Control Panel screens to do the setup

Appliance Clustering

The following clustering features are shipped on all Mirth Appliances, regardless of the customer's subscription level:

- ***Heartbeat***
  - Each node in the cluster records a heartbeat at a regular interval that every other node in the cluster monitors to detect a failure.
- ***Active/Standby Mode***
  - The active node has polling channels running and is assigned a VIP address through which it receives inbound messages.
  - The standby node has polling channels paused and does not receive inbound messages.
  - When the active node fails, the standby node will become the new active node.
- ***Active/Active Mode***
  - Multiple nodes will receive inbound messages through a round-robin load-balancer provided by the appliance.
  - One node in the cluster will be automatically designated to run polling channels as well as execute the data pruner on its defined schedule.
  - Nodes may be added or removed on the fly.
- ***Database Replication***
  - The appliance provides a highly available, clustered database. If the primary database node fails, the standby database will automatically take its place.
- ***Benefits of a Shared Database***
  - All nodes in the cluster share the same set of channels. Modifications to channels are effective for the entire cluster.
  - The ability to view and manage messages processed by any node in the cluster from a single Message Browser window.
  - Beginning with Mirth Connect version 3.0: the ability to manually reprocess incomplete

messages from a failed node on another node.
- Other data such as code templates, alerts, users are also shared across all nodes in the cluster.

Without the Advanced Clustering Plugin, appliance clustering will have the following limitations:

- Channels must be manually redeployed on each cluster node after making channel modifications.
- Users are not able to start, stop, pause, halt, resume channels across the entire cluster with one command.
- In order to view statistics for each cluster node, the user must log into each node individually.
- The user cannot easily monitor the status of nodes in the cluster or channels across the cluster.
- When one node fails, incomplete messages on that node remain so until a user manually reprocesses them on another node.

Mirth Connect Clustering Wizard

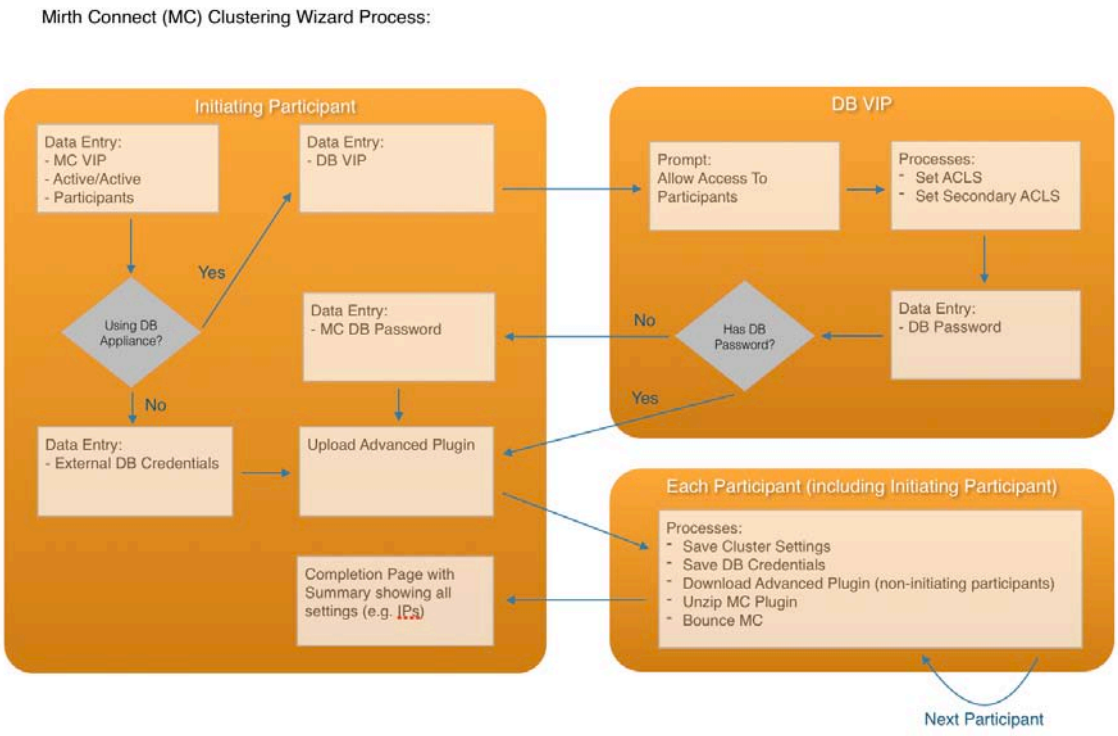
Introduction

This section describes how to set up Mirth Connect Clustering using the **MC Clustering Wizard**. The wizard will guide you through setting up the Mirth Connect Clustering plugin. Mirth Connect's Clustering plugin improves upon and replaces the Appliance's Clustering and Load Balancing services by allowing easier management of channels across multiple instances.

The Clustering plugin requires that all participating Mirth Connect instances use the same database. The database included with the Mirth Appliance now has support for replication and auto-failover to a second Appliance, so two Appliances set up in this manner make an ideal choice for use with the Mirth Connect Clustering plugin.

> The feature allowing the use of the VIP as the source IP for outbound traffic is no longer included in the present version of MC Clustering. A JIRA ticket has been opened to bring back this feature in a future version.

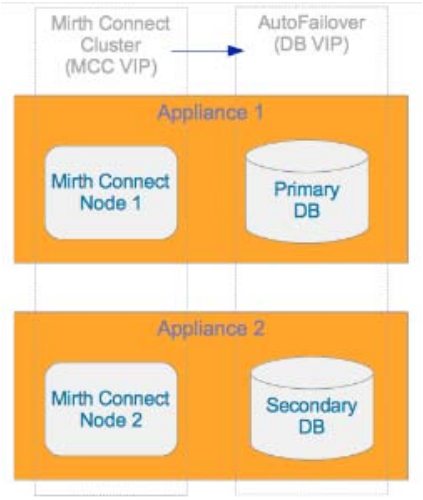
Flowchart



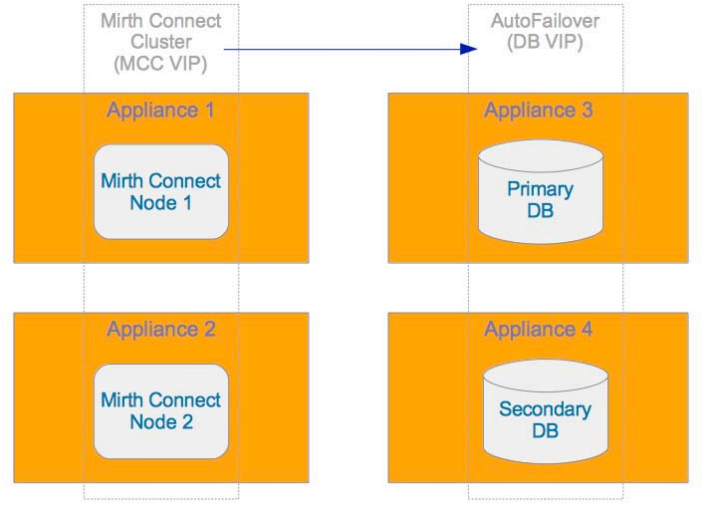
Mirth Connect Cluster Database Connection Setup

Below are three suggested setups for production and the fourth diagram is suggested for QA testing to emulate the three production setups.

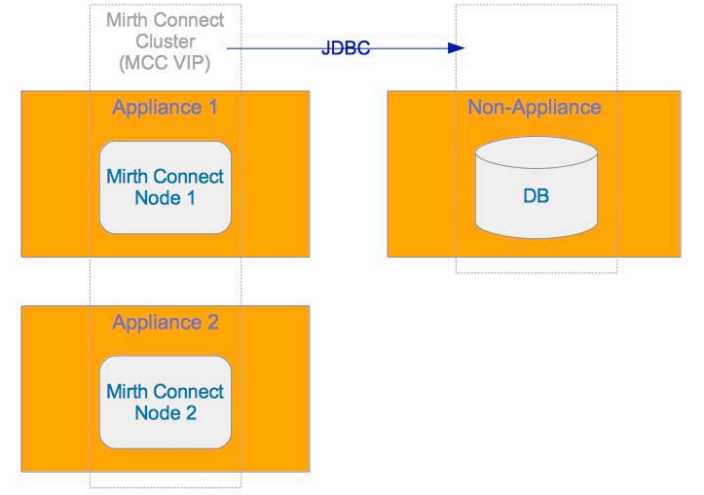
1. Initiating participant's Mirth Connect Appliance is one of the Db Auto Failover nodes



2. Initiating participant's Mirth Connect Appliance is not a DB Auto Failover node and is connecting to an external group of Appliances with Auto Failover

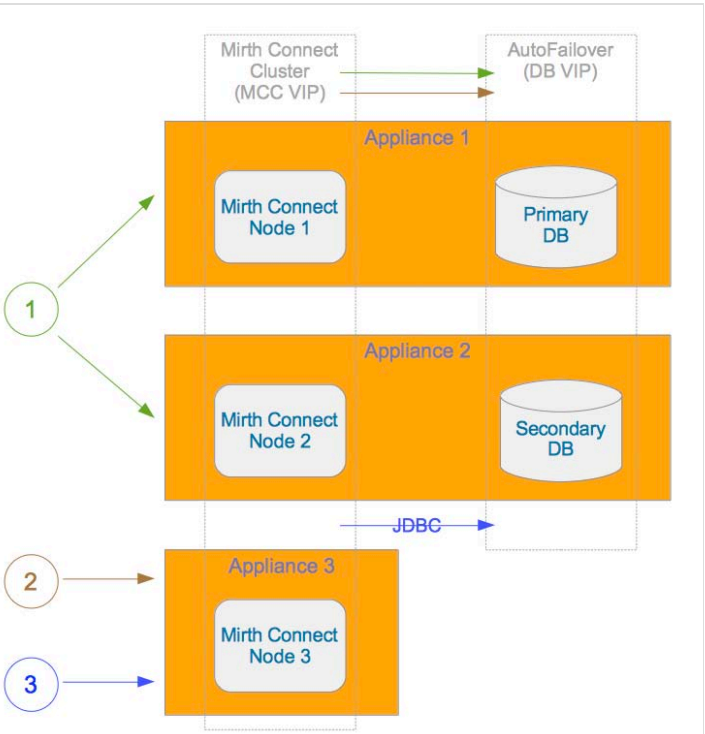


3. Initiating participant's Mirth Connect Appliance is not a DB Auto Failover node and is connecting to an external non-Appliance Database



This is for QA testing and setup emulation:

1. In green, initiating participant can be MC node 1 or 2 and will be using the DB Auto Failover.
2. In brown, initiating participant is MC node 3 and will be using the DB Auto Failover.
3. In blue, initiating participant is MC node 3 and will be using the JDBC connection settings (use DBVIP as database connection ip.)

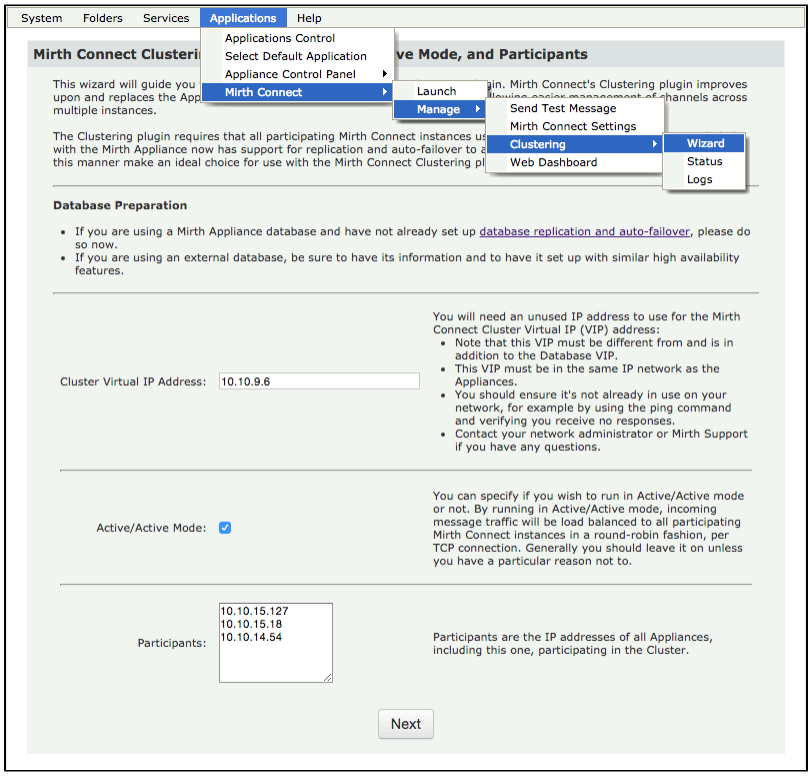


Before You Start

- Take a snapshot of each VM before proceeding.
- If you will be using an Auto Failover setup configured on one of the cluster nodes, or on an external group of Appliances, first ensure you've followed the steps in the Replication and Auto Failover sections of this guide.
- If you will be using an external non-Appliance database, be sure to have its information, ACLS set, and to have it set up with similar high availability features.
- You will need an unused IP address to assign as the Mirth Connect Virtual IP (VIP) address:
  - Note that this VIP must be different from and is in addition to the Database VIP.
  - This VIP must be in the same IP network as the Appliances.
  - You should ensure it is not already in use on your network, for example by using the `ping` command and verifying you receive no responses.
  - Contact your network administrator or Mirth Support if you have any questions.
- Prepare the following:
  - MC Clustering VIP
  - Participant IP addresses
  - If using Appliance database:
    - Database VIP
    - Database Password
  - If using non-Appliance database:
    - Database credentials (type, URL, driver, username, password)
  - If testing Advanced Clustering plugin:
    - Download Advanced Clustering Plugin.

On Any Cluster Node:

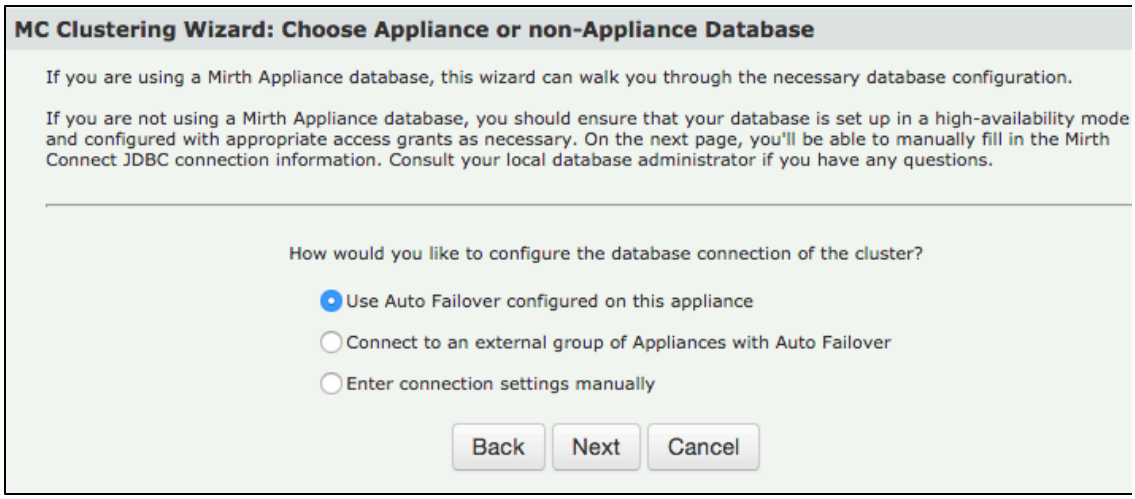
- Go to **Applications > Mirth Connect > Manage > Clustering > Wizard**

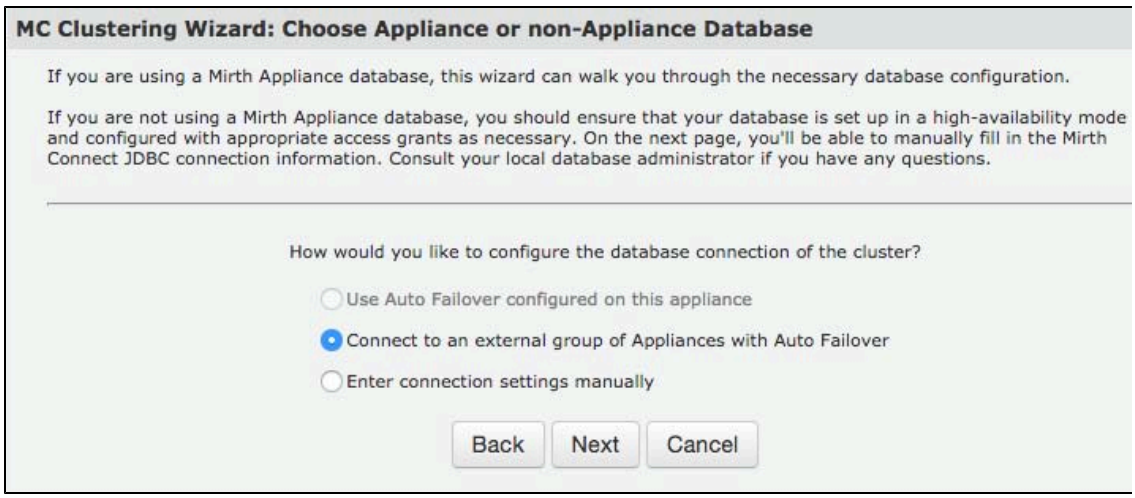


- Enter **Cluster Virtual IP Address**, **Active/Active Mode**, and **Participants** IP Addresses. (Three cluster nodes , 10.10.15.127, 10.10.15.18 and 10.10.14.54 are used in the example below.)
- Click **Next**.

Choose Appliance or non-Appliance Database steps

- Choose your database configuration.
- Be sure to check out Mirth Connect Cluster Database Connection Setup.
- If you chose one of the first two options, click **Next**, and continue with the following steps. Otherwise, skip down to the step for the Enter database connection settings manually selection.

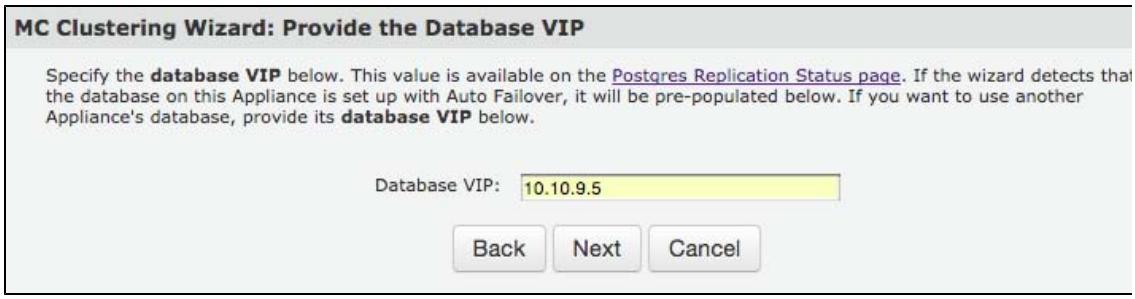




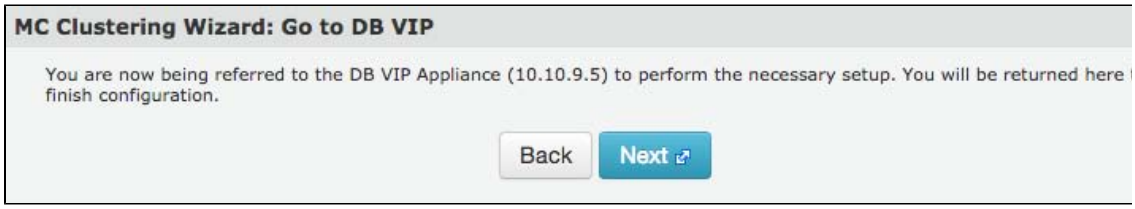
- Click **Next**.

- If you chose **Use Auto Failover configured on this appliance**, click **Next**.

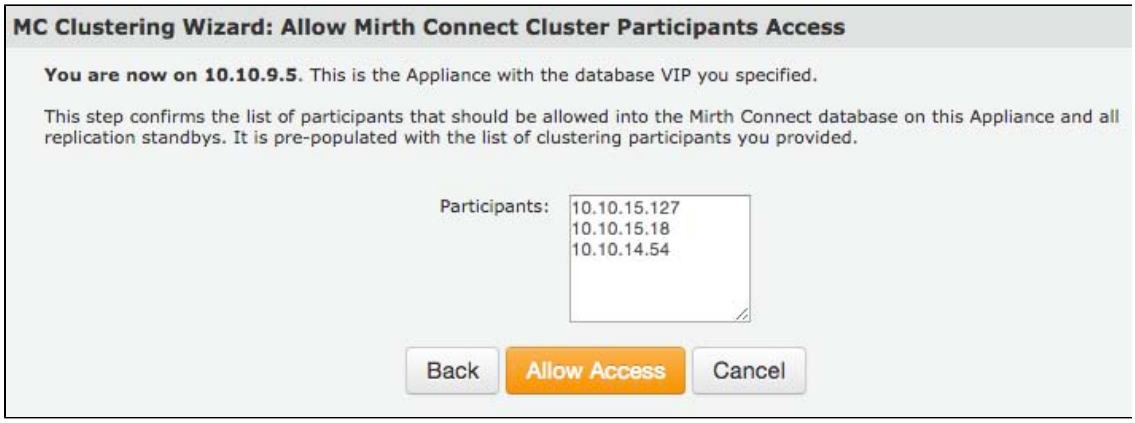
- If you chose **Connect to an external group of Appliances with Auto Failover**" enter the **Database VIP**, and then click **Next**.



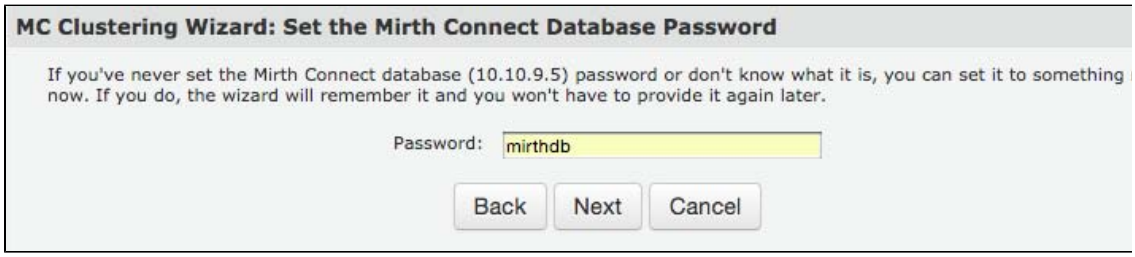
- Click **Next**. (You will be clicking through some transition pages to inform that you will be taken to another Appliance.)



- Click **Allow Access** to set ACLS. (This step gives all participants access to the database.)



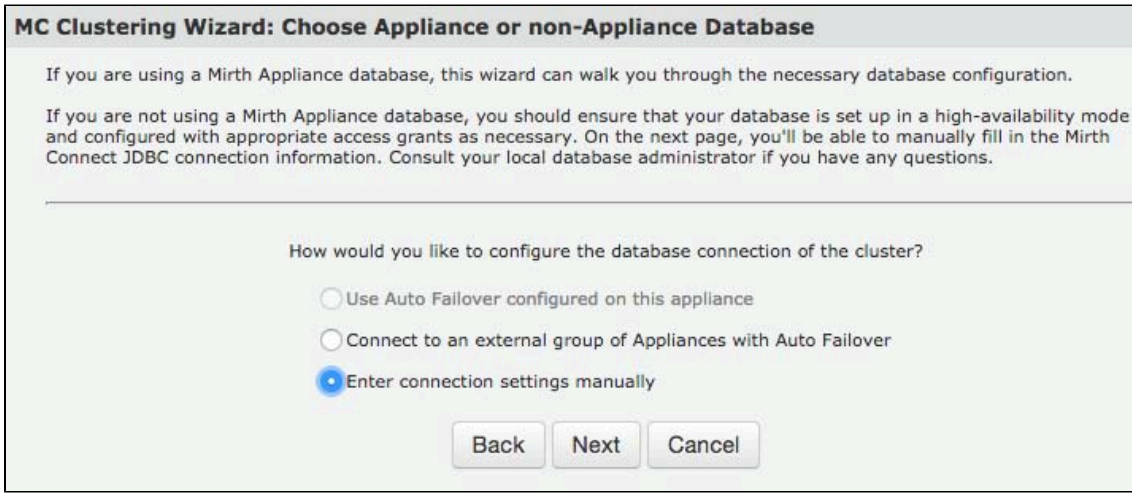
- Enter the database password. (Note: You may leave it blank if you do not wish to change the actual database password.)



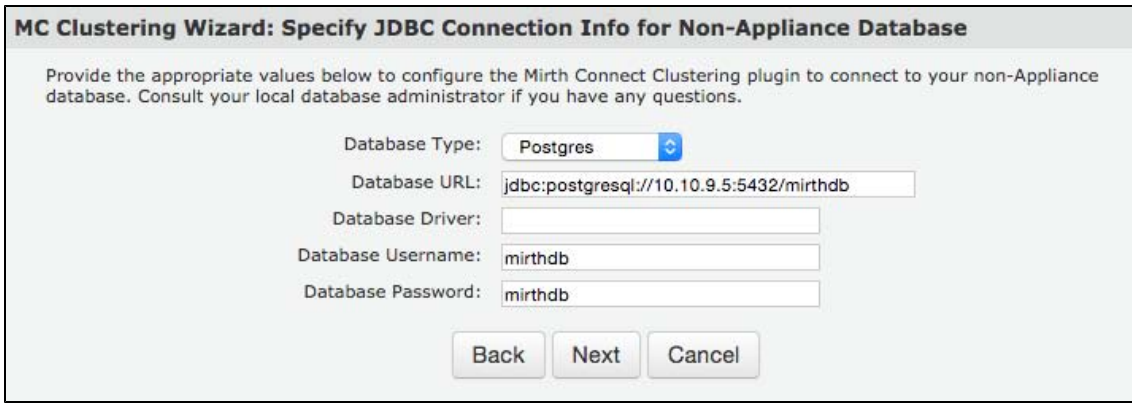
- Click **Next**.
- Click **Next** to be taken back to the initiating Appliance.

- If a database password was not provided earlier on the **Set the Mirth Connect Database Password** page, enter a password here so Mirth Connect will use this password to authenticate to the mirthdb database. You can leave it blank if the cluster nodes database credentials were already set.

- If you chose **Enter database connection settings manually**, click **Next.**



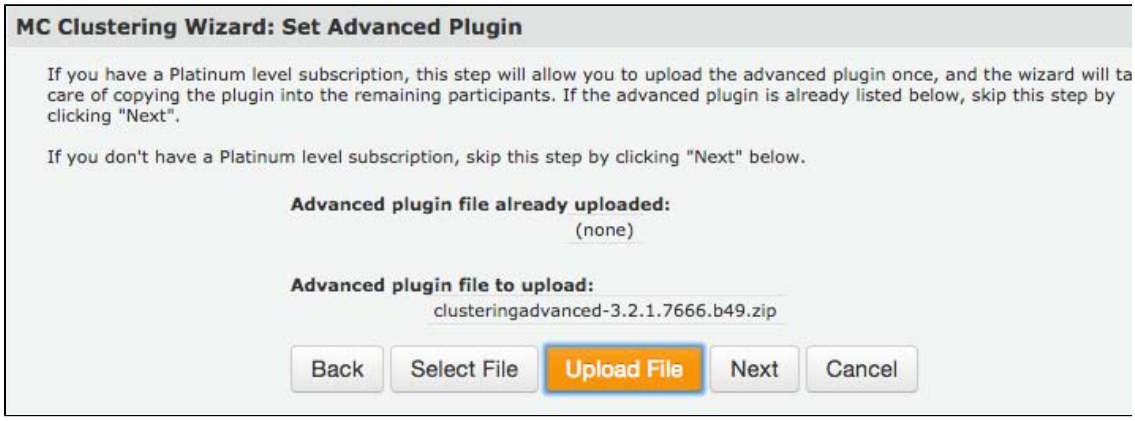
- Enter database settings



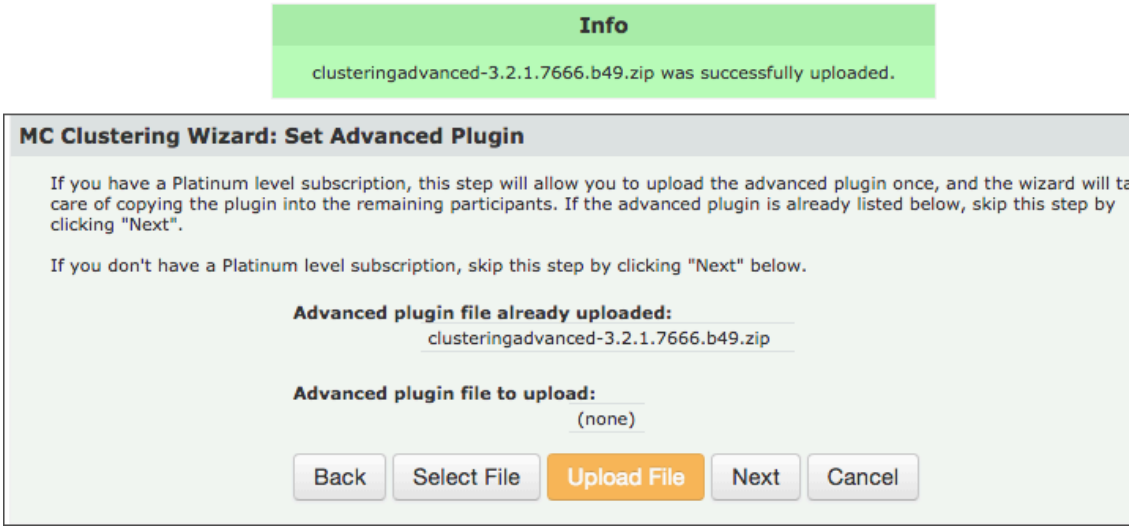
- Click **Next**.

Set Advance Plugin steps

- For users with Platinum level subscription, continue with the following steps to download the Advanced Clustering plugin from the customer portal. Otherwise, skip down to the step for users without a Platinum level subscription.
- Click **Select File** and choose plugin zip file.

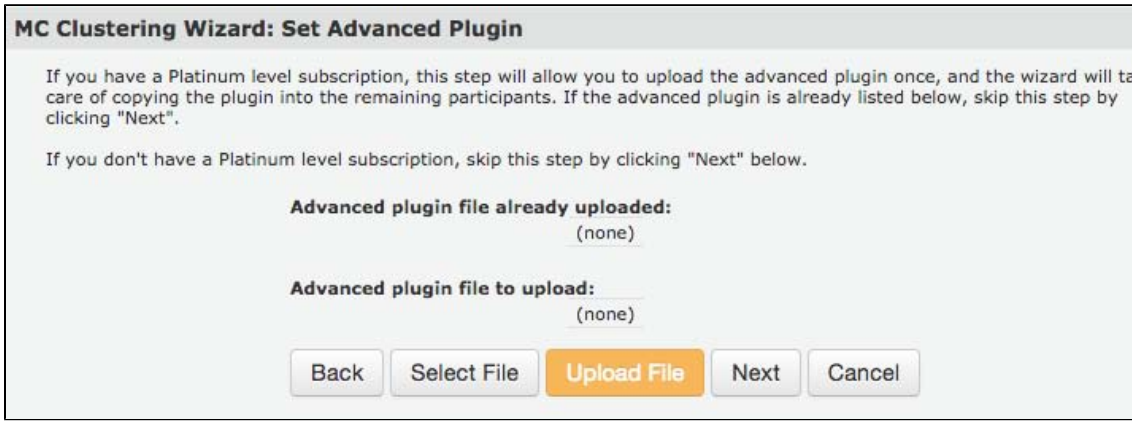


- Click **Upload File**



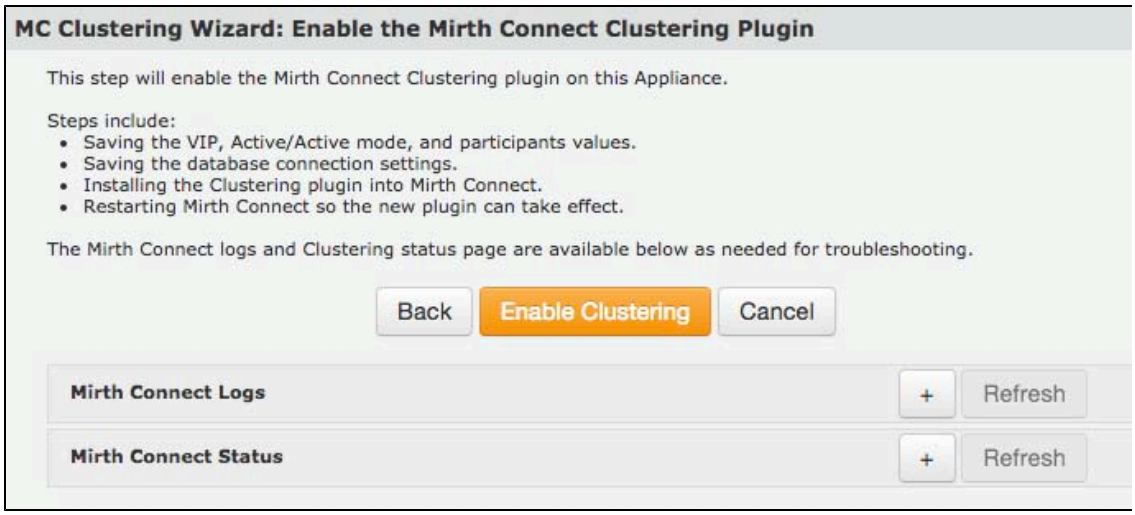
- Click **Next**.

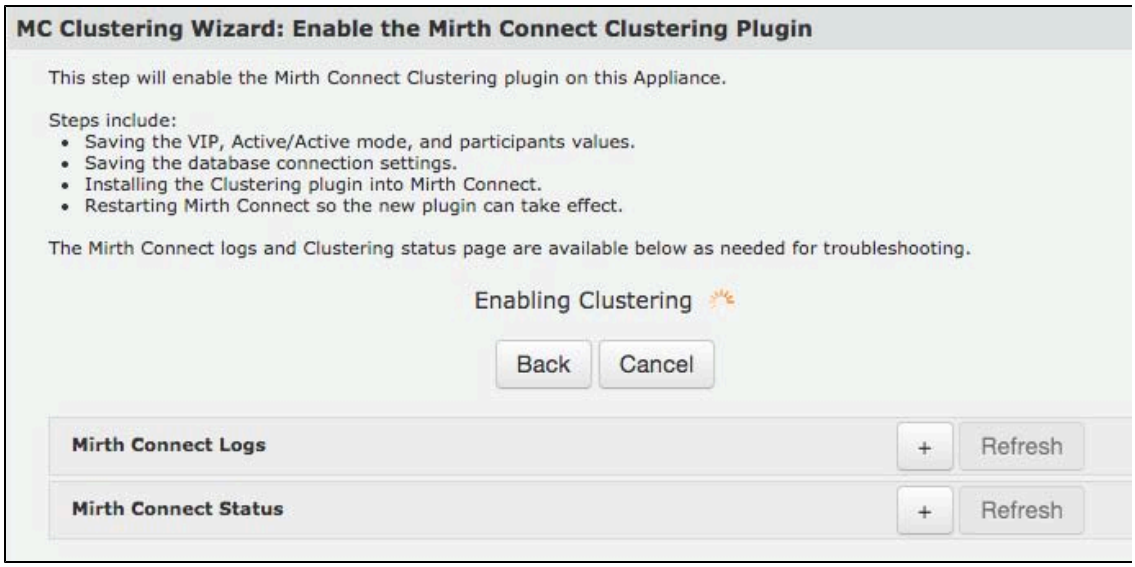
- For users without Platinum level subscription, click **Next**.



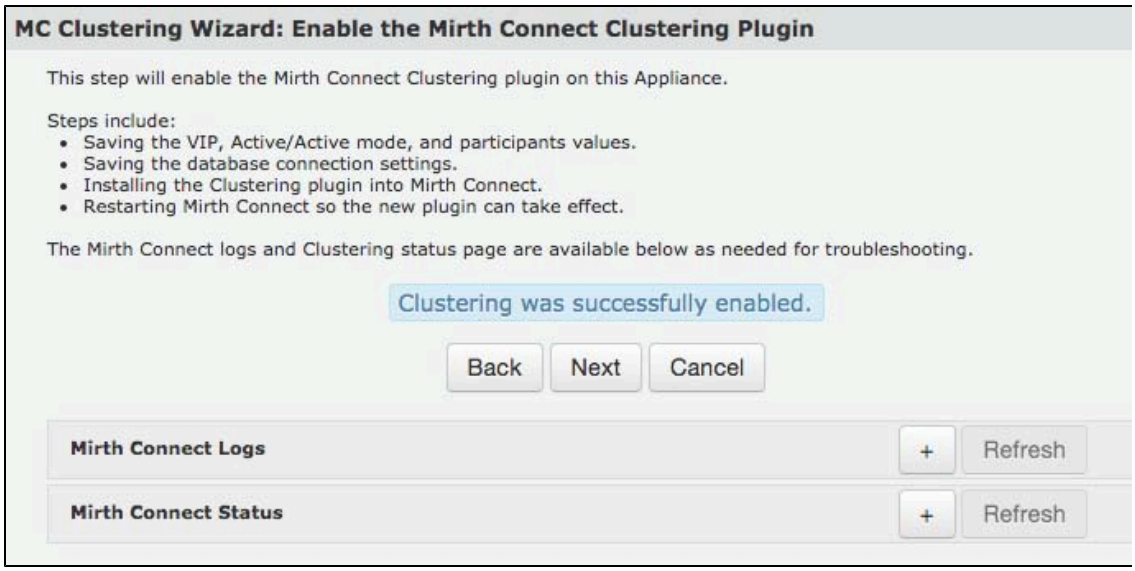
Enable Clustering steps

- Click **Enable Clustering**.

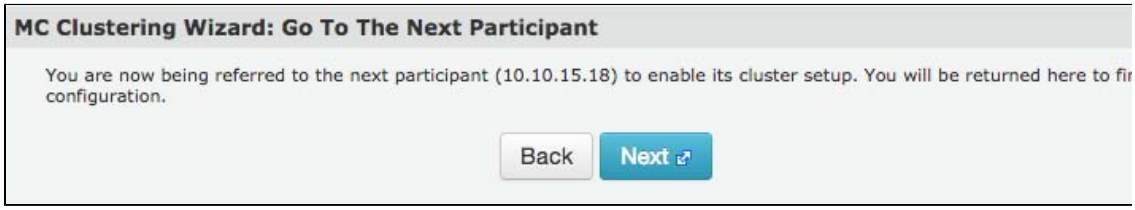




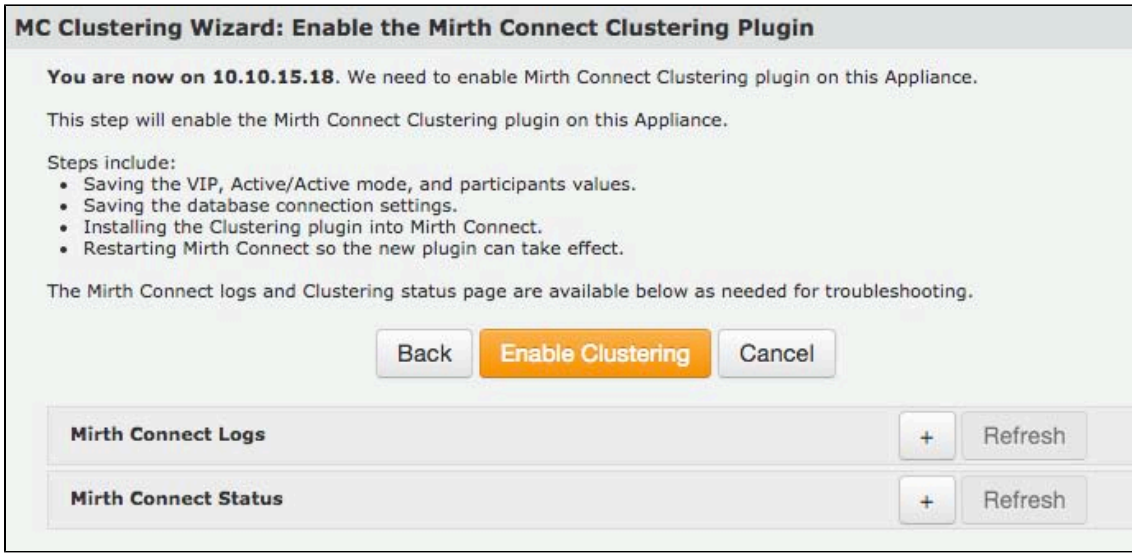
- Click **Next**.



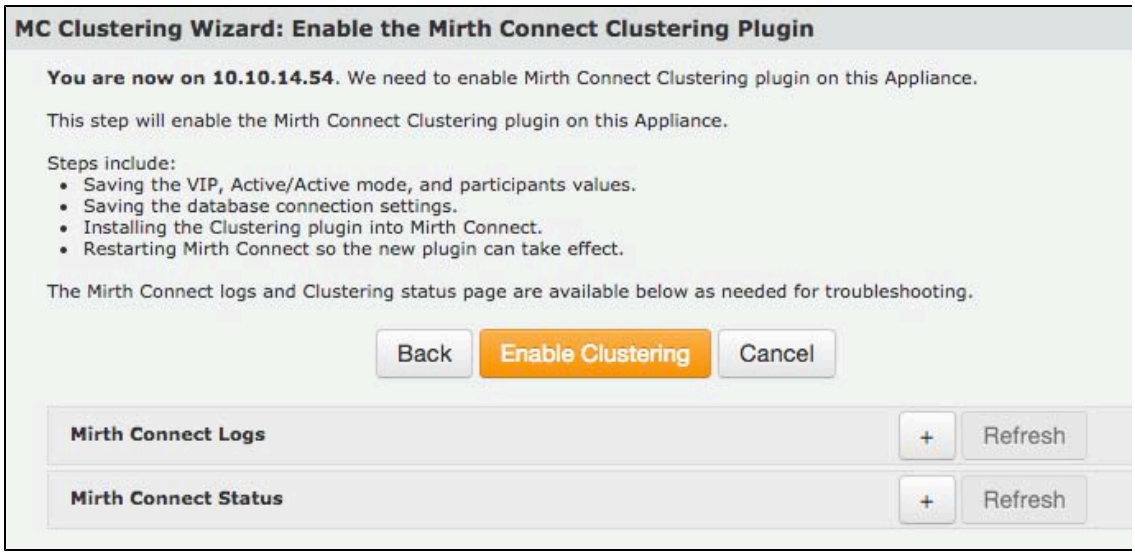
- Click **Next** to be taken to the next participant.



- Click **Enable Clustering**, Click **Next**, and Click **Next** on the transition page to be taken to the last participant.



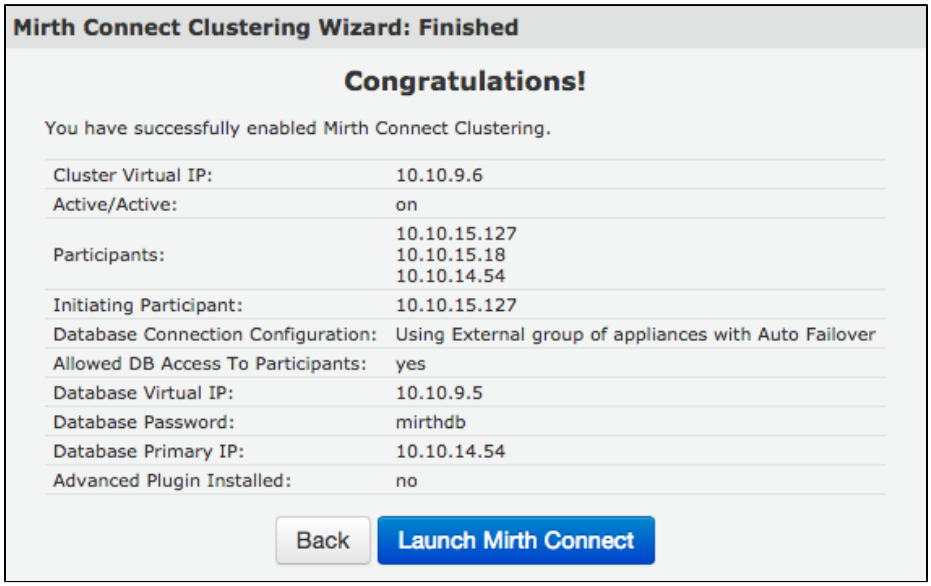
- Click **Enable Clustering**, and Click **Next**.

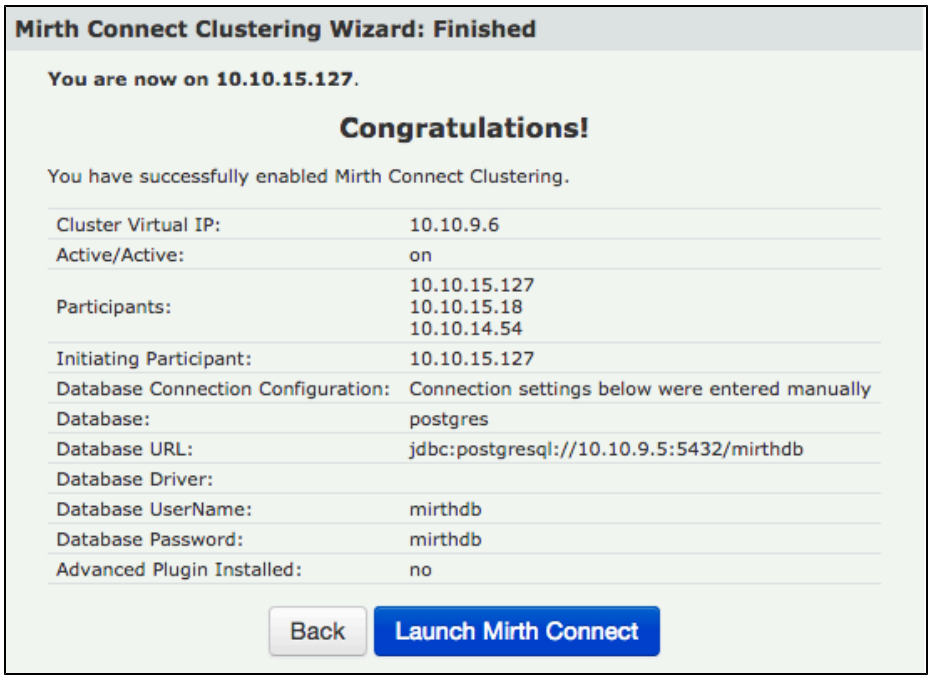


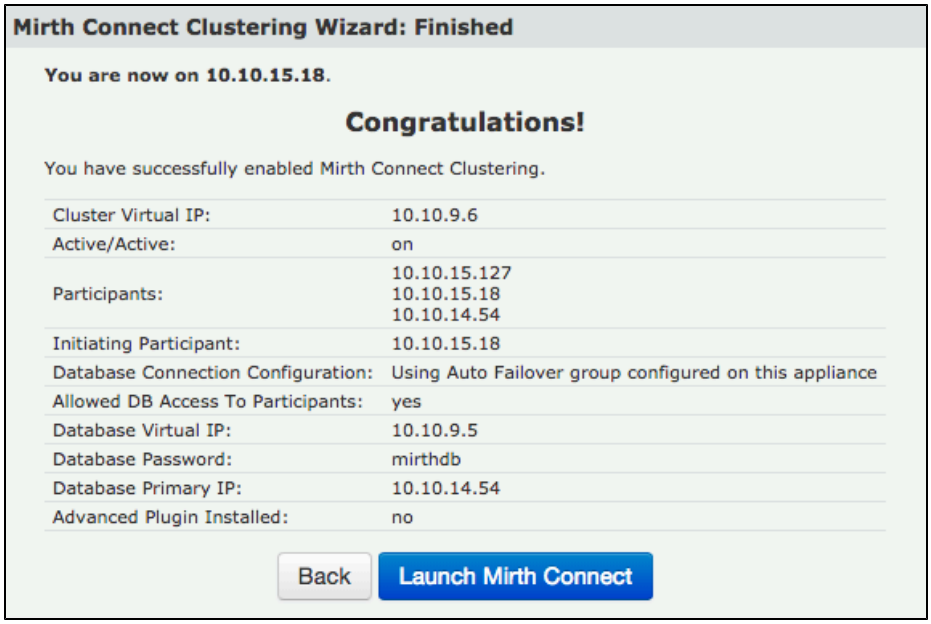
- Click **Next** to be taken back to the initiating participant.

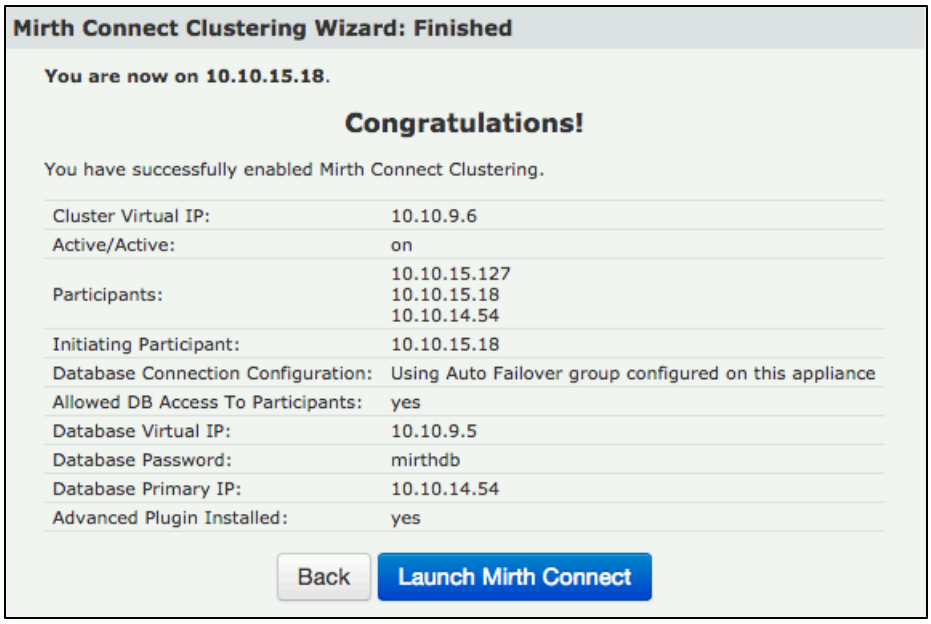
Finishing step

- Success! Completion page examples:









On each participant, restart Mirth Connect, and get the latest Java Webstart launcher file

- Go to **Applications > Applications Control**
- Click Mirth Connect's **Stop** button, wait for it to stop, then click **Start**
- Verify Mirth Connect started successfully:
  - Go to **Folders > Browse**, click **mirthconnect**, click **logs**, click **mirth.log**
  - Scroll to the bottom to make sure you see the normal Mirth Connect startup banner, and no exceptions.
- Go to **Applications > Mirth Connect > Launch** to download a new Webstart (JNLP) file
  - This is necessary because the Clustering plugin was added
- Launch Mirth Connect as you normally would.

You Have Completed Setup

At this point you have set up Mirth Connect Clustering using the Mirth Appliance's or the external highly-available database. Messages inbound to the Mirth Connect VIP address will be load balanced across all Mirth Connect instances, but all instances writes to the same underlying database resulting in a unified message store. In case one Appliance fails, the other Mirth Connect cluster nodes will handle all traffic.

The remaining steps in this document are optional reading and describe how to view diagnostic information and how to test a node failure.

View Diagnostic Information on all boxes

- Go to **Applications > Mirth Connect > Manage > Clustering > Status**
  - This page is for diagnostic purposes. It's rather low-level information but each of the four sections says what it should look like, and should be consulted in case of problems.
- Click **View Logs**
  - These messages are a log of what Mirth Connect told the Appliance to do and when.
  - You will see messages like the following at the appropriate times. They should be consulted and/or sent to Mirth Support for assistance when troubleshooting.
    - “Mirth Connect requested the following serverIds be made active”

Test a Node Failure

- Obtain the LLP to File - Filter Transformer ADT channel from Mirth Support.
- Add it to Mirth Connect one of the Appliance.
- After you deploy it, it should also automatically deploy on the rest of the Appliances (this is one of the features of the MC Clustering plugin).
- Set up a third Mirth Connect instance, the "Sender", either on your desktop, or in a third Appliance VM, to be used to send messages into the MC Clustering VIP.
  - Obtain the blast9104 channel from Mirth Support
  - Add it to the Sender's Mirth Connect.
  - Modify the channel's destination to send messages to your Mirth Connect VIP
  - Start it
- On the Sender, verify you see the Received and Sent counts increasing **every second**
- On each Appliances, verify you see the Received and Sent counts increasing **every 2 seconds**
- Through VMware, suspend an Appliance
- On the Sender, you will now see the Received and Sent counts have gone back to increasing, and the Error count is no longer increasing
- Through VMware, resume suspended Appliance.
  - Re-log into the MC Administrator
  - You will see it sharing the load now:
    - the Received/Sent counts increasing every 2 seconds

Manual Setup for Mirth Connect Clustering

Setting up clustering using the Appliance control panel

Before you start

1. Before starting to set up clustering, you will need to set up replication and auto failover for the Appliances that will be part of the cluster. See the **Replication** and **Auto Failover** sections of this guide for details of how to do this.
2. Take a snapshot of each VM before proceeding.
3. You will need an unused IP address to assign as the Mirth Connect Virtual IP (VIP) address:
    - This VIP must be different from and is in addition to the Database VIP.
    - This VIP must be in the same IP network as the Appliances.
    - You should ensure that it is not already in use on your network, for example by using the `ping` command and verifying you receive no responses.
    - Contact your network administrator or Mirth Support if you have any questions.

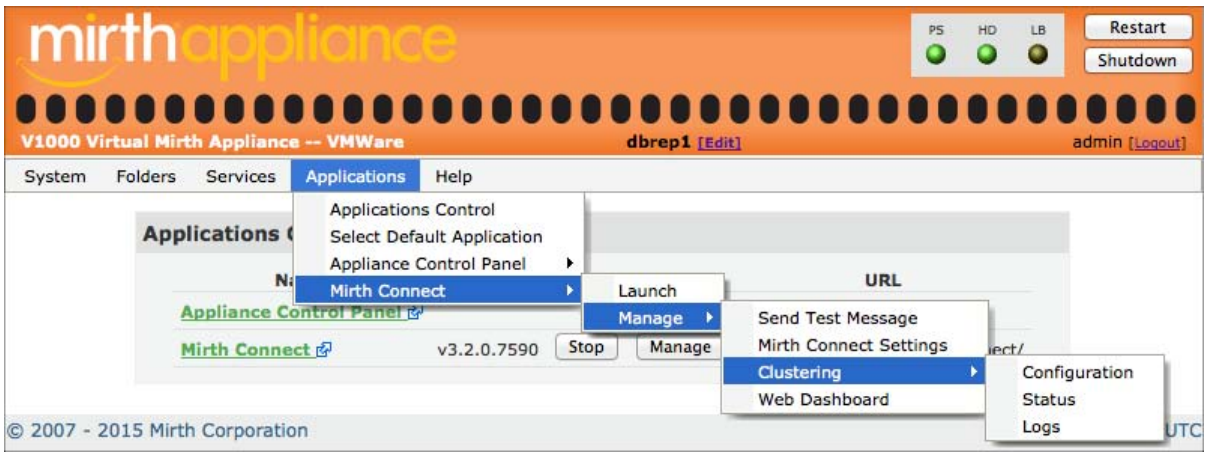
On the Primary:
Set mirthdb's password and IP access list

1. Go to **Services > Postgres > Database Management**
2. Click *mirthdb* to go to the **Edit Database** screen for mirthdb
3. Choose a password and enter it in the **New Password** and **Retype Password** fields. Remember it, you'll need it later.
4. Check **Enable External Access**
5. In the **Restrict connections to IP Address(es)** box, provide the following three IP addresses (ALL are required):
    - Appliance 1's IP
    - Appliance 2's IP
    - Your Database VIP
6. Click **Update**

On the Standby:
Set mirthdb's IP access list

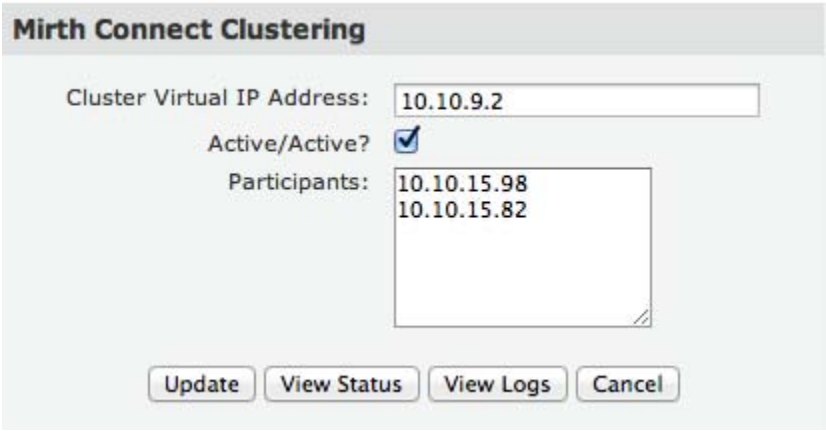
1. Go to **Services > Postgres > Database Management**
2. Click *mirthdb* to go to the **Edit Database** screen for mirthdb
3. Note: Do not try to set the password on this database. It has already been replicated from the Primary, and since this database is read-only, attempting to set it will fail.
4. Check **Enable External Access**
5. In the **Restrict connections to Ip Address(es)** box, provide the following three IP addresses (same as above, and ALL are required):
    - Appliance 1's IP
    - Appliance 2's IP
    - Your Database VIP
6. Click **Update**

When these preliminary steps have been completed, you can move on to the clustering settings.



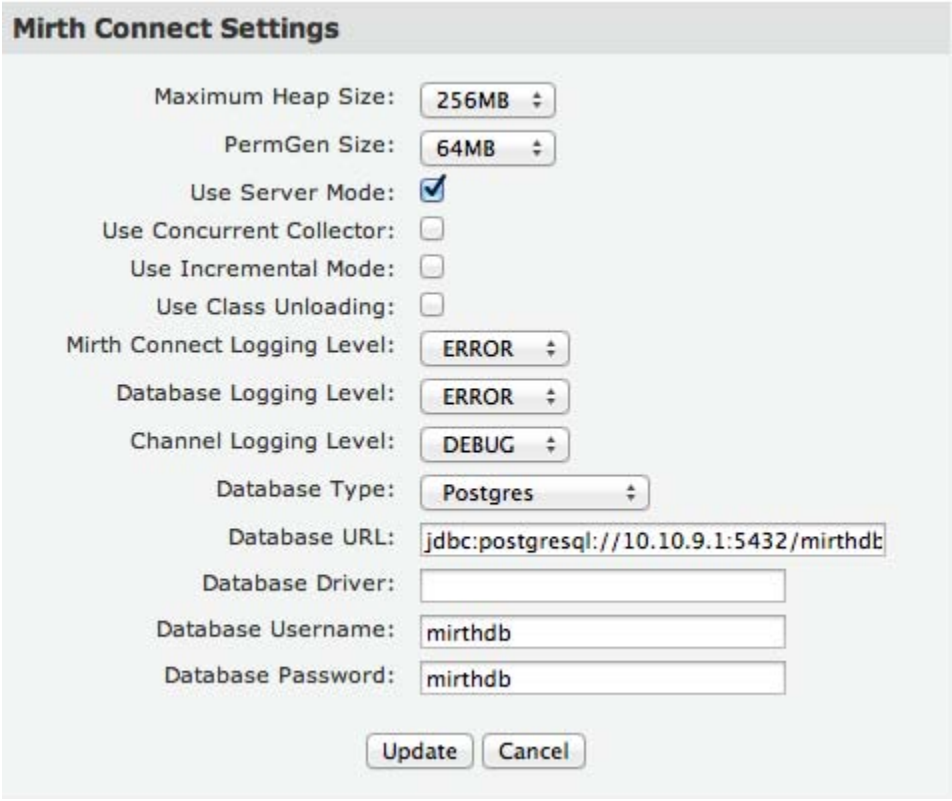
On both the Primary and the Standby:
Enable Mirth Connect clustering

1. Go to **Applications > Mirth Connect > Manage > Clustering > Configuration.**
2. Enter a VIP address for the cluster.
3. If active/active, check the **Active/Active?** box and enter the IP addresses of the participants in the cluster.



On both the Primary and the Standby:
Configure Mirth Connect's database URL to point to the Database VIP address

1. Go to **Applications > Mirth Connect > Manage > Mirth Connect Settings.**
2. Enter the database VIP address in the **Database URL.**
3. In the **Database Password** field, provide the mirthdb password you set earlier.



On both the Primary and the Standby:
Start Mirth Connect

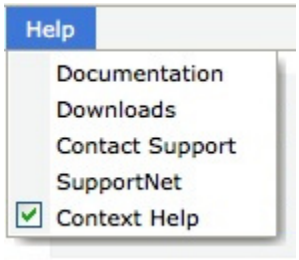
1. Navigate to **Applications > Applications Control**

2. Restart Mirth Connect

An alternate way to start Mirth Connect on each node is to use the **Applications > Mirth Connect > Launch** menu selection.

Help Menu

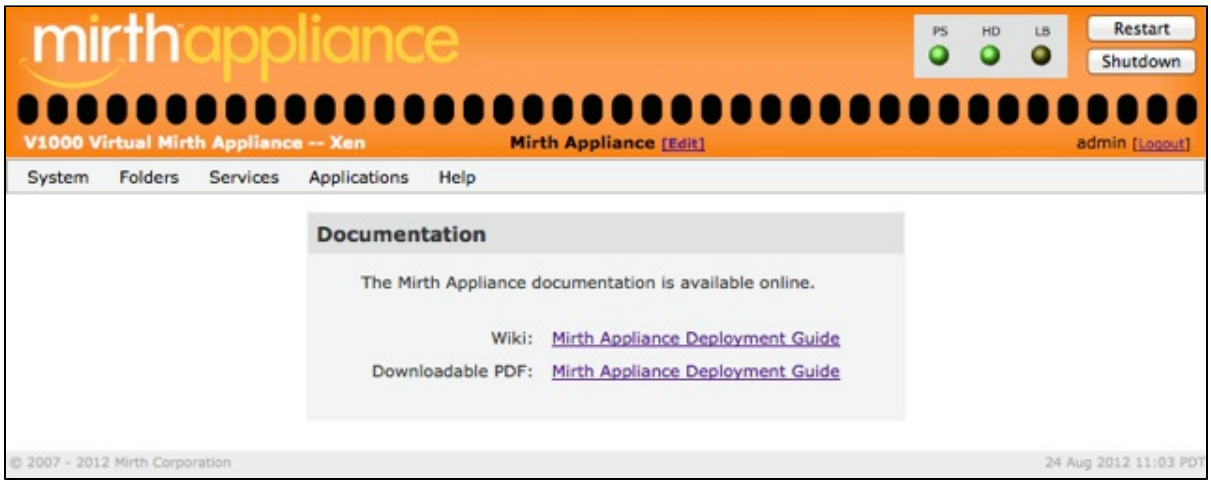
Click **Help** on the menu bar to open the **Help** menu.



The **Help** menu allows you to access a variety of help resources for using and managing the Mirth Appliance, as well as providing some support for Mirth Connect.

Documentation

To get to this page, click **Help** on the menu bar, and then select **Documentation** from the **Help** menu.



Documentation

The **Documentation** page has links to the documents related to the Appliance. The *Mirth Appliance Deployment Guide*, which you are reading now, is available both in online form and as a downloadable PDF file.

Downloads

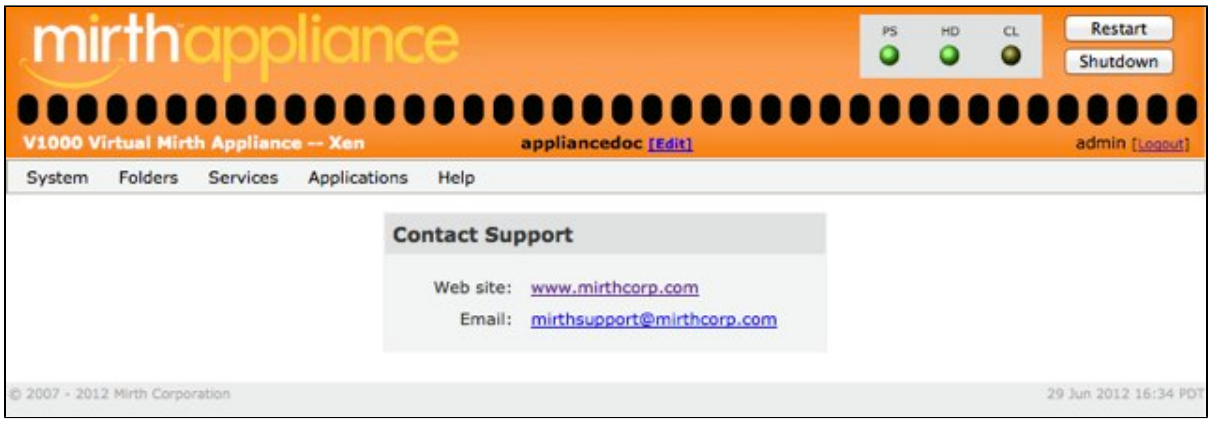
To get to this page, click **Help** on the menu bar, and then select **Downloads** from the **Help** menu.

Downloads

While you can access the standard documentation from the **Documentation** page, you can download other files related to the Mirth Appliance via the **Downloads** page. The *Mirth Appliance SNMP MIB* is the management information base for managing the Mirth Appliance via SNMP (Simple Network Management Protocol).

Contact Support

To get to this page, click **Help** on the menu bar, and then select **Contact Support** from the **Help** menu.



Contact Support

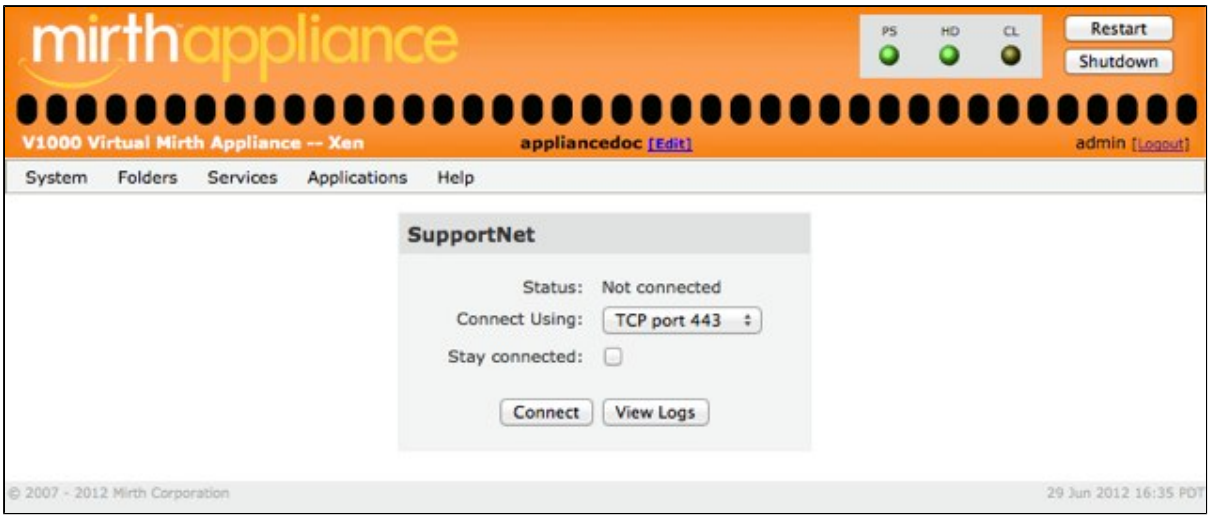
The **Contact Support** page provides links for Mirth Corporation. Use these links to quickly connect to Mirth Corporation's website or to email support personnel for assistance. When contacting Mirth Corporation for support on your Mirth Appliance, please have your Appliance serial number ready. The serial number is displayed in the **System Status** area on the **Mirth Appliance Dashboard** page, and on a sticker on the Appliance.

SupportNet

To get to this page, click **Help** on the menu bar, and then select **SupportNet** from the **Help** menu.

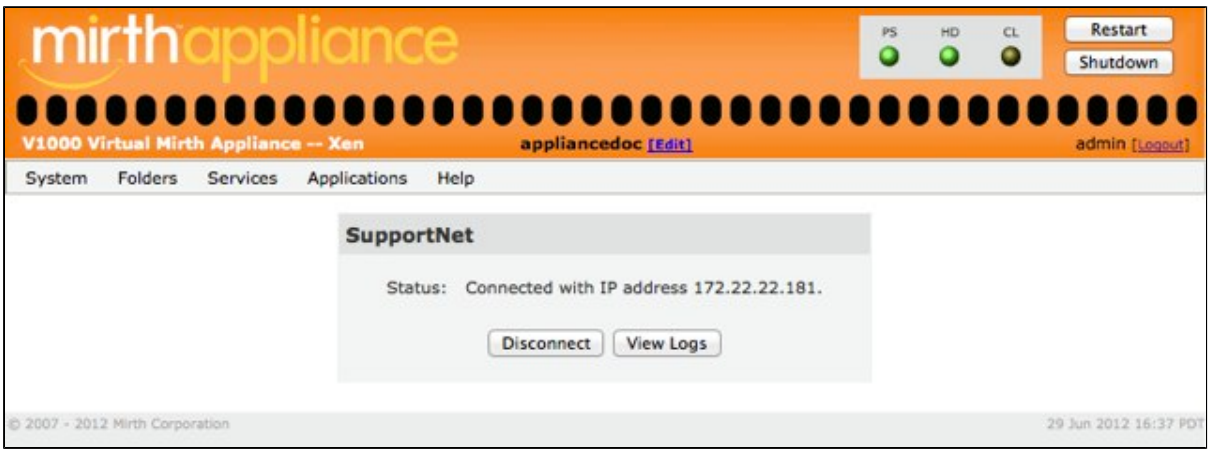
SupportNet is a Mirth Corporation customer support feature that allows your Mirth Appliance to be VPN'd into our support network. SupportNet is launched from the Mirth Appliance **Help** menu. Once connected, Mirth Corporation support staff and system administrators can connect directly to your Appliance, allowing us to debug Appliance issues or issues with applications running on the Appliance, such as Mirth Connect.

The only requirement to connect to SupportNet is that your Appliance must be able to make an outbound TCP connection on port 443 or an outbound UDP connection on port 1194, to connect to SupportNet. You may have better luck using TCP 443 as this is typically left open on corporate firewalls.



SupportNet

Under **Connect Using**, select either the *TCP* or *UDP* option and click the **Connect** button.

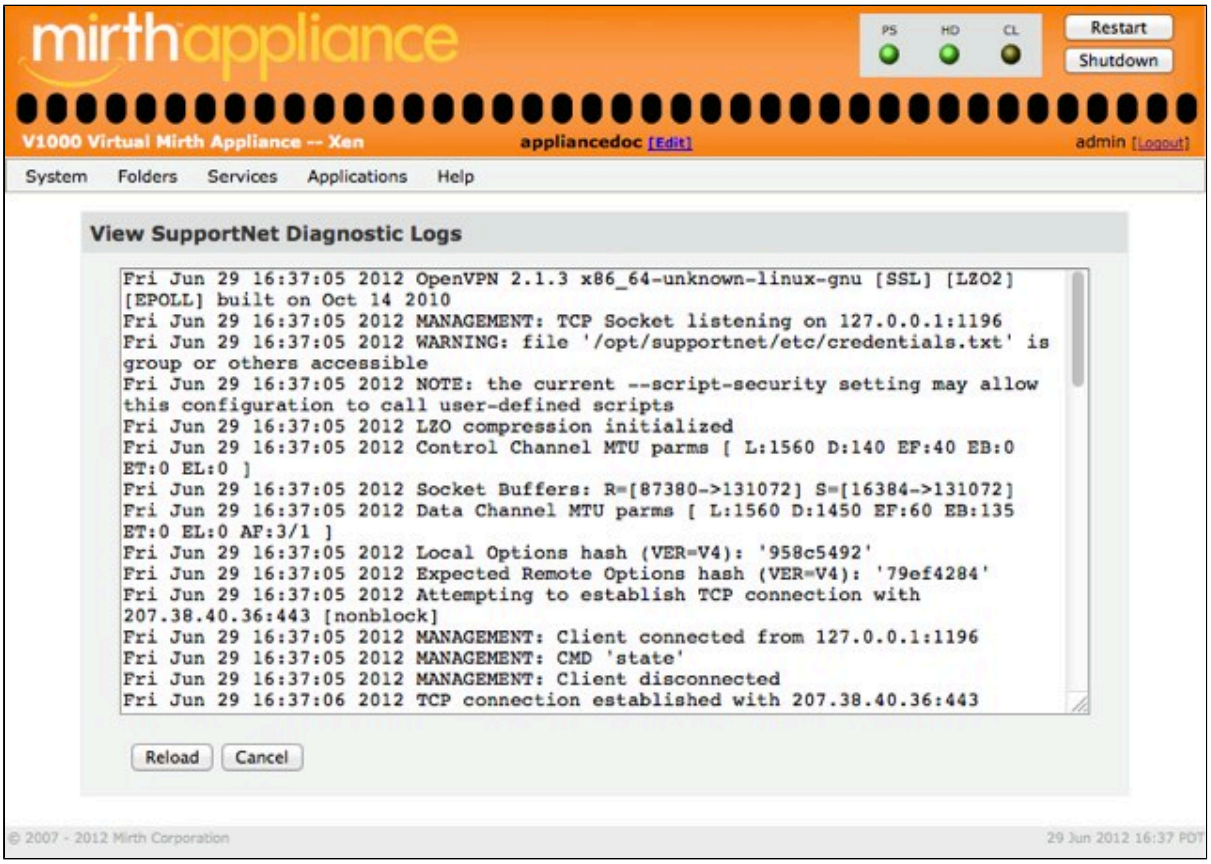


Connected to SupportNet

The web page will show the Connected status and display the Appliance's IP address on the VPN.

Diagnostic Logs

Click the **View Logs** button to view the SupportNet connection logs. This may be useful for diagnosing problems connecting to SupportNet.



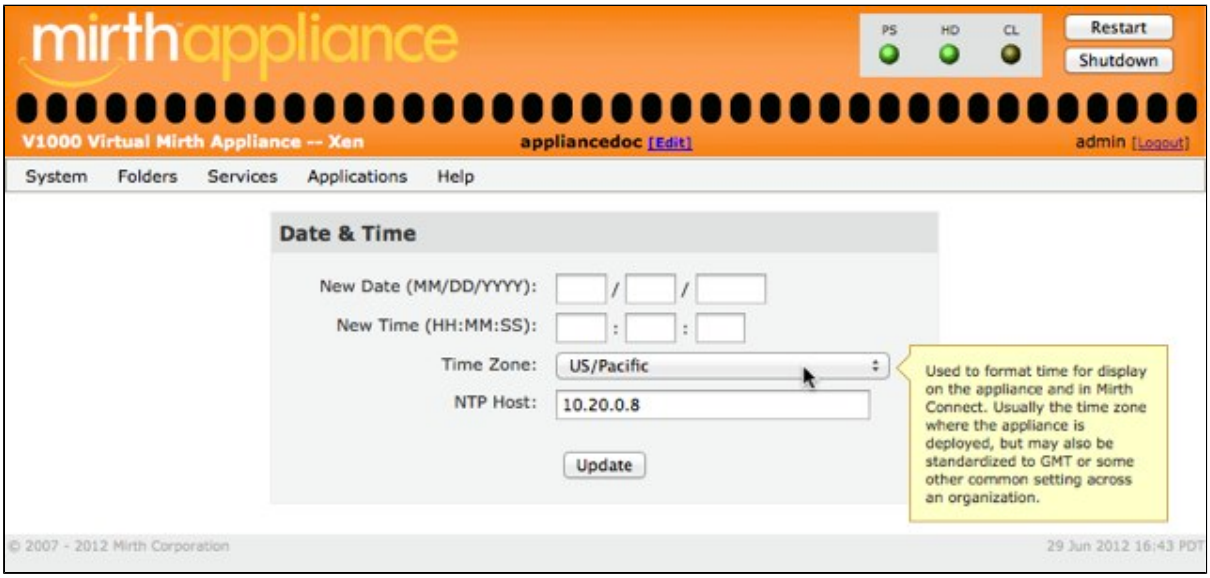
SupportNet Diagnostic Logs

Context Help

Context Help is a checkable menu item in the **Help** menu. Each time you select **Context Help** in the menu, you toggle the checkmark and the enabled/disabled status. A visible checkmark indicates that context help is enabled.

When context help is enabled, the Control Panel web pages will display context-sensitive help information when the cursor is moved over a web page control.

Here is an example for an item on the **Date & Time** page:



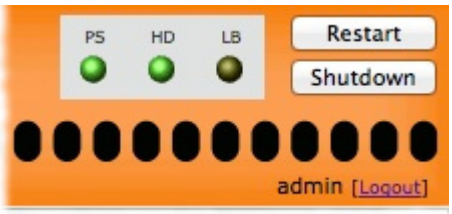
Context Help on the Date & Time Page

The description of using the **Time Zone** setting is an example of the context help built into the Mirth Application Control Panel.

Monitoring

At the top right of the Control Panel, next to the **Restart** and **Shutdown** buttons, there are three status indicators. These indicators represent **PS**=Power Supply, **HD**=Hard Drive, and **LB**=Load Balancing. (If Clustering is in use, a **CL** indicator will automatically be substituted for the **LB** indicator.) Green indicates the item is functioning normally. Yellow indicates the item is in a warning state that may require attention. Red indicates a failure. If an indicator is not green, click it to get more information on the problem.

A status Indicator that does not display green, yellow, or red simply means the item is not capable of being monitored. For example, the **LB** (Load Balancing) indicator will be dark if you only have one Mirth Appliance and thus are not running in a load balanced environment.



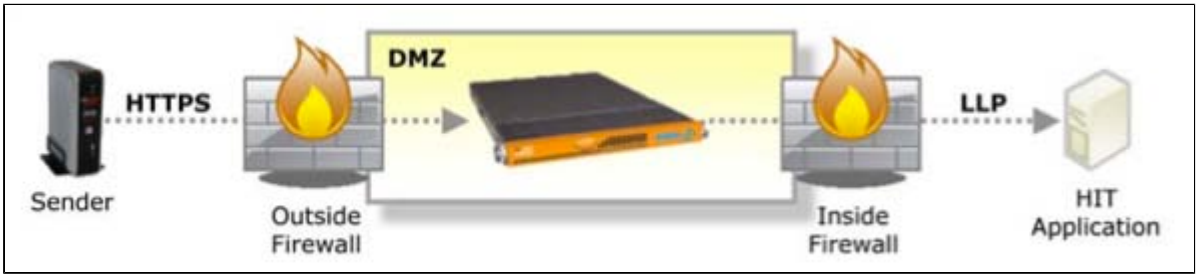
A Mirth Appliance can be integrated with your organization's monitoring infrastructure to take advantage of existing alerting and support systems. For more information on monitoring your Appliance, please see SNMP (**Services > SNMP**).

Deployment Considerations

The flexibility of the Mirth Appliance allows for a variety of deployment options. When planning the placement of your Appliance, consider the following recommendations.

DMZ for External Access

If the Appliance is to be used for connectivity to sources outside your organization's private network, it is recommended that the unit be placed into a DMZ network. A DMZ (derived from the military term *de-militarized zone*) is a network segment separated from both the public and private networks by a firewall.



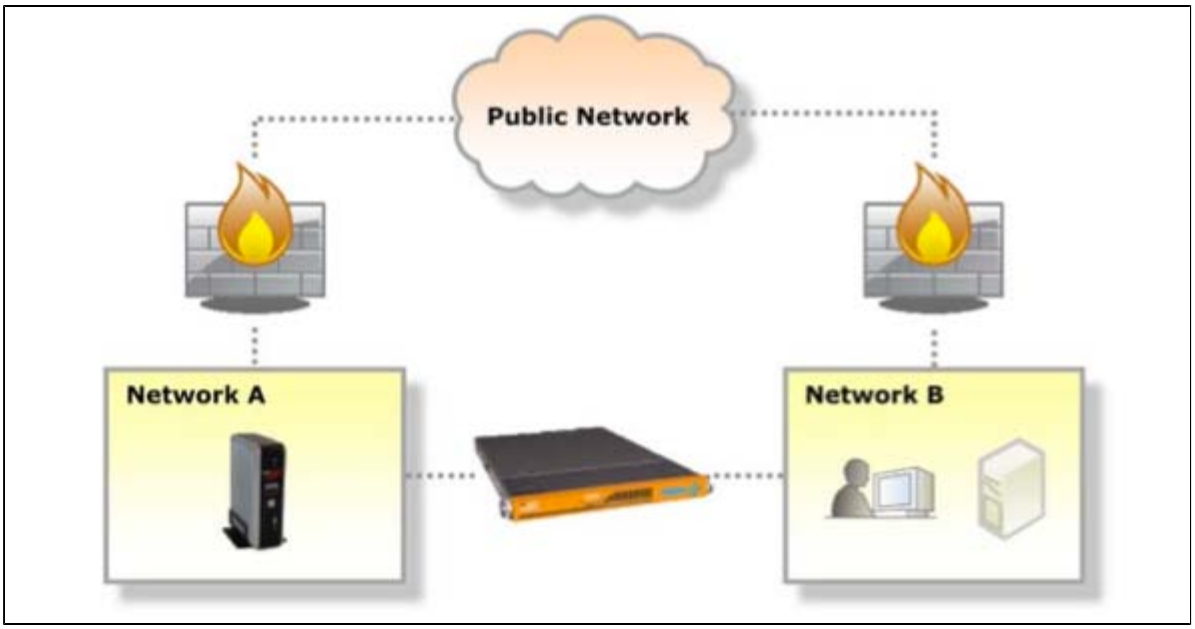
Example of a Mirth Appliance deployed in a DMZ network.

A typical security policy is that no network connection is allowed from the outside (public) network directly to the internal network. All devices accepting connections from public sources must reside in a DMZ network. Only connections originating from the DMZ network are allowed to penetrate the internal firewall.

This provides two levels of firewall protection between the public and private networks. For outside attackers to penetrate the internal network, they would first need to compromise a host on the DMZ.

Bridging Disconnected Network Segments

A Mirth Appliance with multiple Ethernet interfaces can be used as a message firewall to bridge otherwise disconnected networks. For security reasons, port forwarding is disabled, and network traffic will not automatically flow from one interface to the other. However, when a channel sends a message to an address that is in a network directly connected to a local interface of the Appliance, the preference will be for the Appliance to use that interface.



Using a Mirth Appliance to connect two networks.

This has the effect of using channels to granularly control the flow of message traffic between any two networks.

Opening Network Ports Through a Firewall

When operating a Mirth Appliance through a firewall (or other device performing access control), it is necessary to allow some network traffic to pass for certain features of the Appliance to function properly. The following tables list the ports used by the Mirth Appliance and by the various Mirth applications that might be installed on it.

MIRTH APPLIANCE

Port Number	Direction (In/Out)	Protocol	Most Common - Open/Closed to outside world	Notes
22	In	TCP		Used for SFTP, Console Access. Only necessary if using the SFTP Server or the Console Service.
25	Out	TCP		Used for Mail Delivery. Not necessary if using a mail relay behind the firewall.
53	Out	TCP		Used for DNS. Not necessary if using a local DNS server behind the firewall.
80	In	TCP	CLOSED	Used for the Control Panel and all installed web-based Mirth applications (e.g. Results, Match, Mail, Care). **Note:** Should be closed to the outside world. Only necessary to open if performing administration through the firewall. Alternative is to use VPN service for access.
80	Out	TCP		Used for VPN. Optional. Only used for detecting external IP address. Only necessary to open if performing administration through the firewall. An alternative is to use VPN service.
123	Out	UDP		Used for NTP (time). Not necessary if using a mail relay behind the firewall.
161	In	UDP		Used for SNMP. Only necessary if using SNMP.
389	In	TCP		Used for LDAP Directory. Only necessary if setting up Appliance-to-Appliance LDAP directory replication through the firewall.
443	In	TCP	CLOSED	Used for the Control Panel and all installed web-based Mirth applications (e.g. Results, Match, Mail, Care). **Note:** Should be closed to the outside world. Alternative is to use VPN service for access.
443	Out	TCP	Can be locked down to mirthhq.mirthcorp.com.	Used for Software Updates and self-registering.
443	Out	TCP	Can be locked down to supportnet.mirthcorp.com	Used for SupportNet. Only needed if SupportNet access is desired.
1194	Out	UDP	Can be locked down to supportnet.mirthcorp.com	Used for SupportNet. Only needed if SupportNet access is desired.
1194	In	UDP		Used for VPN. This is the default value. Can be changed. Only necessary if using the VPN Client Access service.
5432	In	TCP		Used for Database. Only necessary if using the Database Service and require access behind the firewall.

8009	In	TCP	CLOSED	Used by Apache.
8080, 8443	In	TCP		Used for Mirth. Only necessary to open if performing administration through the firewall. An alternative is to use VPN service.
9443	Out	TCP	Can be locked down to mirthhq.mirthcorp.com.	(Deprecated). Used for self-registering.

MIRTH CONNECT

Port Number	Direction (In/Out)	Protocol	Most Common - Open/Closed to outside world	Notes
8080	In	TCP	CLOSED	Used for Mirth Connect Java Web Start. Only necessary to open if administering through a firewall. Alternative is to use VPN service.
8443	In	TCP		Used for Mirth Connect. Only necessary to open if administering through a firewall. Alternative is to use VPN service.

MIRTH RESULTS

Port Number	Direction (In/Out)	Protocol	Most Common - Open/Closed to outside world	Notes
80	In	TCP		Used for access to the Mirth Results web UI, as well as access to web service and REST APIs.
443	In	TCP		Used to make calls to the Results APIs.
11037		TCP		
11038		TCP		
11039		TCP		
11048		TCP		
11076		TCP		
11080		TCP		
11086		TCP		
11200		TCP		Used for the Elasticsearch http.port
11300		TCP		Used for the Elasticsearch transport.tcp.port
11443		TCP		
11443	In	TCP		Used to send data to Mirth Results.

PIX/PDQ

Port Number	Direction (In/Out)	Protocol	Most Common - Open/Closed to outside world	Notes
443		TCP		Used for PIXPDQ XDS reverse proxy.

GLASSFISH 2

Port Number	Direction (In/Out)	Protocol	Most Common - Open/Closed to outside world	Notes
3700		TCP		
3820		TCP		
3920		TCP	CLOSED	Legacy Port
4848		TCP		
7676		TCP		
8181		TCP		
8686		TCP		

GLASSFISH 3

Port Number	Direction (In/Out)	Protocol	Most Common - Open/Closed to outside world	Notes
3037		TCP		
3038		TCP		
3039		TCP		
3076		TCP		
3080		TCP		
3086		TCP		
3443		TCP		
7676		TCP	CLOSED	Used by JMS.

AURION / CONNECT

Port Number	Direction (In/Out)	Protocol	Most Common - Open/Closed to outside world	Notes
4437	In	TCP	CLOSED	Used in CONNECT 4.3+, used for secured webservices
7048		TCP	CLOSED	
7080		TCP	CLOSED	
7037		TCP	CLOSED	
7076		TCP	CLOSED	
7038		TCP	CLOSED	
7039		TCP	CLOSED	
7086		TCP	CLOSED	
8443	In	TCP	OPEN	Used for secured webservices.
8181	In	TCP	CLOSED	Default port for secured webservices. Port should be closed, and webservices reconfigured to use port 8443.

MIRTH SIGNON

Port Number	Direction (In/Out)	Protocol	Most Common - Open/Closed to outside world	Notes
9200		TCP		Used for the Elasticsearch http.port
9300		TCP		Used for the Elasticsearch transport.tcp.port

MIRTH MATCH

Port Number	Direction (In/Out)	Protocol	Most Common - Open/Closed to outside world	Notes
14048		TCP		Used to access Mirth Match via Webservices client

MIRTH MAIL

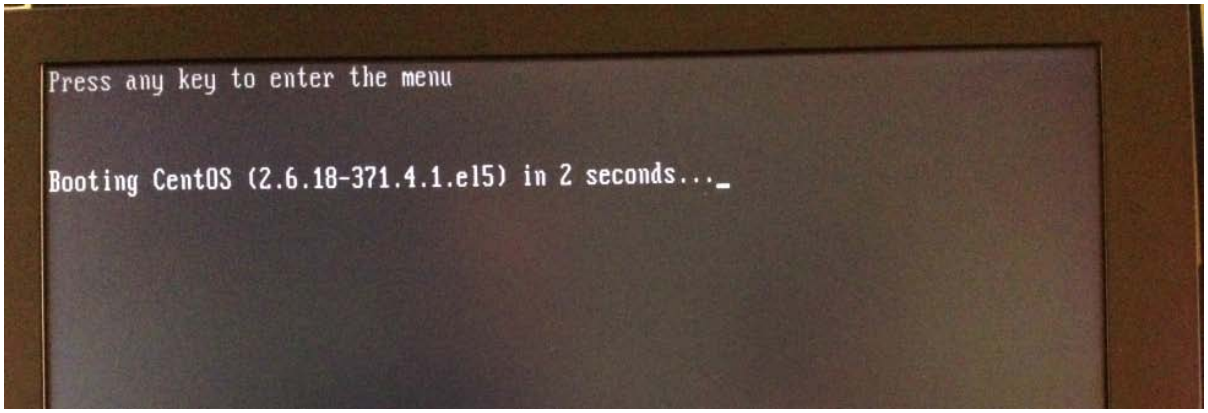
Port Number	Direction (In/Out)	Protocol	Most Common - Open/Closed to outside world	Notes
25	In	TCP	OPEN (External)	Used to accept SMTP traffic from other DIRECT providers.
53	In	TCP	OPEN (External)	Used to respond to DNS queries for DIRECT domains. This includes DNS CERT records, so you'll need to ensure that your firewall allows tcp + DNS responses greater than 512B in size (4k/8k limit recommended).
80	In	TCP	CLOSED	Used to access the Mirth Mail web UI and API endpoints.
443	In	TCP	OPEN (External)	Used to access the Mirth Mail web UI, and API endpoints.
465	Out	TCP	CLOSED	Legacy secure SMTP outbound.
587	In	TCP	CLOSED	Used by Roundcube for Secure SMTP. Can be opened only if needed. Internal.
993	In	TCP	CLOSED	Used by IMAP clients. Can be opened only if needed. Internal.
995		TCP	CLOSED	Used by Dovecot (POP3). Can be opened only if needed.
2000		TCP	CLOSED	Used by Dovecot.
3048		TCP	CLOSED	Glassfish Admin. Internal.
3080		TCP	CLOSED	Glassfish. Internal
7676		TCP	CLOSED	Used by JMS (Glassfish 3)
8181	In	TCP	OPEN (External)	Used for Mirth Mail XDR with TLS Mutual authentication. This is an optional port that only needs to be open if using XDR + TLS Mutual Auth.
10025	Out	TCP	CLOSED	Backend SMTP. Internal.
10026	Out	TCP	CLOSED	Internal. Used for all outbound non-DIRECT mail notifications (Postfix/SMTP). Internal.
10053		TCP	CLOSED	Mirth Mail DNS Server. Internal.
10389		TCP	CLOSED	LDAP (ApacheDS). Internal.

Factory Reset (hardware models only)

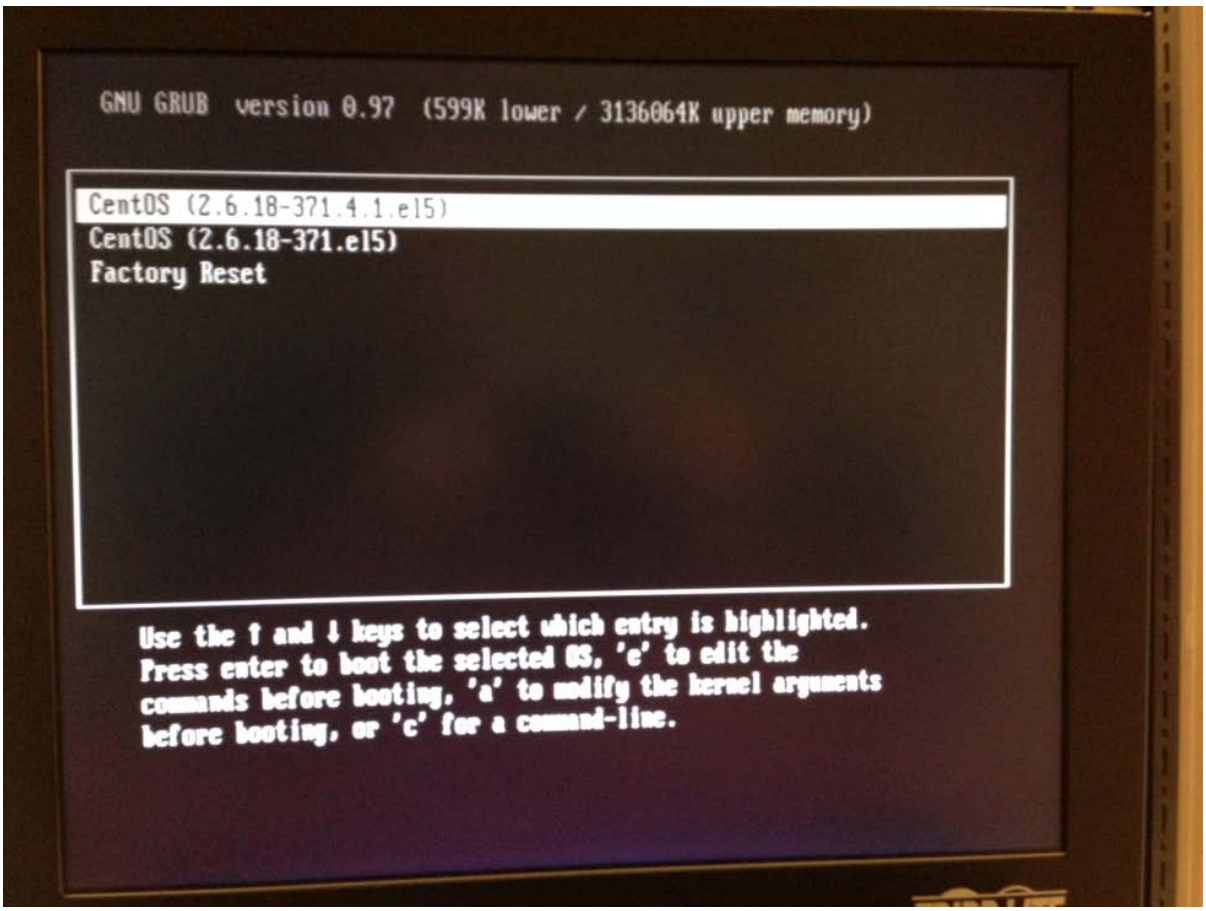
The Factory Reset feature allows you to return your hardware-based Mirth Appliance to its factory-shipped state. (This feature is not applicable for Appliances hosted on virtual machines.)

> ⚠ **Use this feature with caution**
> Performing a factory reset will delete all data, and cannot be undone. You will be presented with a number of confirmation prompts during the process to ensure that you are aware that all data will be lost, and that you really want to proceed.

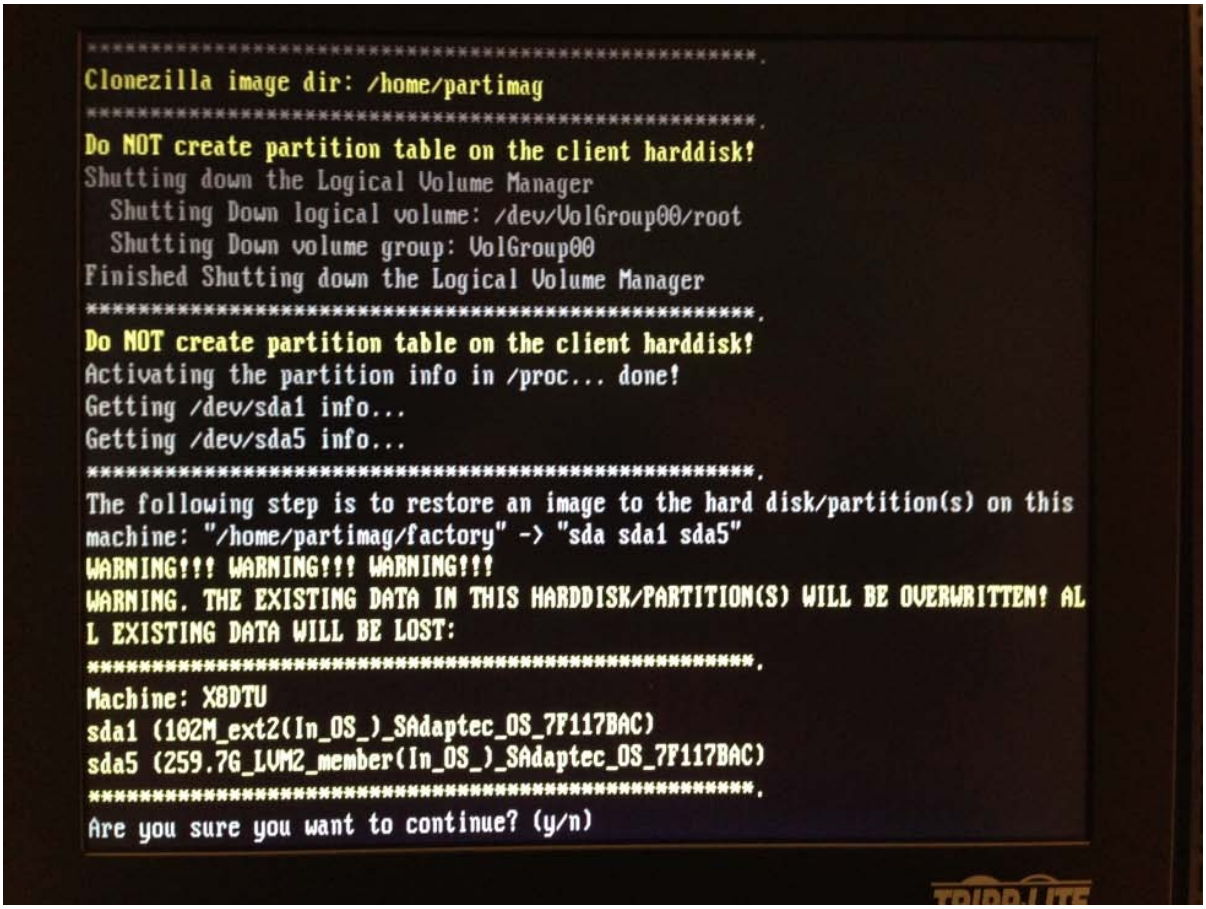
The Factory Reset feature is accessible by rebooting the Appliance and pressing the space bar while the Linux GRUB boot menu is prompting the user with "Press any key to enter the menu." **You have only three seconds to hit the space bar, so pay close attention and be ready.**



Upon hitting the space bar, you will be presented with the GRUB boot menu, with one or more choices of Linux kernels to boot, plus the **Factory Reset** option. Use the arrow keys to move the selection highlight down to **Factory Reset** and then press **Enter**.

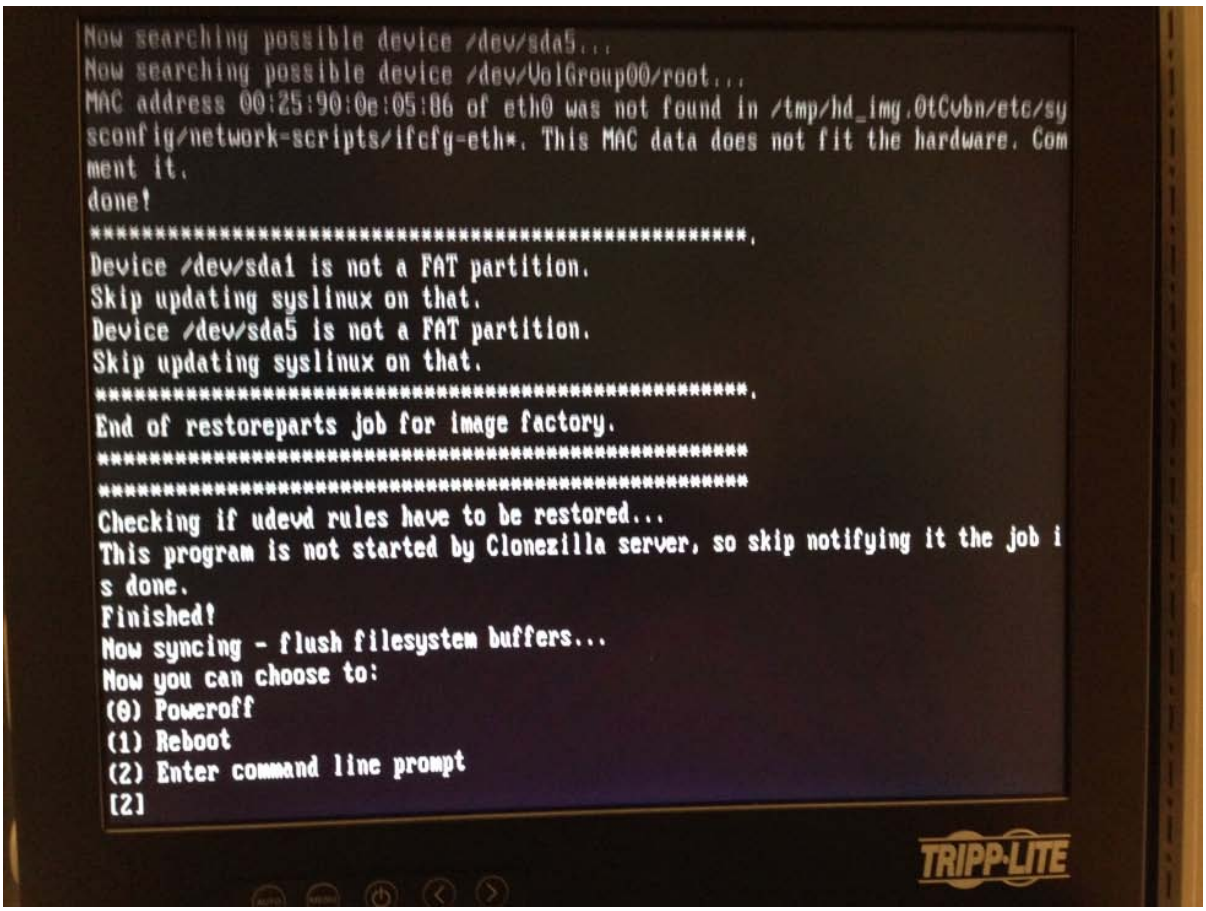


You will see lots of messages quickly scrolling as Linux boots up. Finally, you are presented with some warning text that all existing data will be lost:



If you are sure you wish to continue, type 'y' and press **Enter** to continue. You will be prompted to confirm once more.

The Factory Reset will take a few minutes. When it completes, you will be prompted on what to do next. Select **(1) Reboot** to continue.



Your Appliance has now been reset to its factory-shipped state. Allow it to boot it normally, and then proceed as described in the **Getting Started** section of this guide.