8 Example Websites
  8.1 Creating a WebFaction Site in 4 Minutes .................................................. 43
  8.2 Creating a Simple Website ................................................................. 44
  8.3 A Sophisticated Website Configuration ................................................. 44

9 Email
  9.1 Mailboxes and Addresses .......................................................... 47
  9.2 Accessing Email ........................................................................... 51
  9.3 Managing Email Automatically ...................................................... 107
  9.4 Mailing Lists ................................................................................. 113
  9.5 Email Limitations and Restrictions .................................................. 113
  9.6 Using Google Apps for Email ........................................................ 114

10 Databases
  10.1 Creating a New Database with the Control Panel ......................... 117
  10.2 Managing Database Users .......................................................... 118
  10.3 Connecting to a Database ............................................................ 119
  10.4 Accessing a Database from the Web ............................................ 119
  10.5 Accessing a Database from the Command Line ......................... 120
  10.6 Accessing a Database Remotely .................................................... 121
  10.7 Accessing a Database from a Script or Application .................... 124
  10.8 Import and Export Database Records ........................................... 125
  10.9 Backing Up a Database Automatically ....................................... 126
  10.10 Delete a Database ...................................................................... 128
  10.11 Enabling Procedural Languages for PostgreSQL ....................... 128

11 Usage Quotas
  11.1 Quotas on Shared Hosting .......................................................... 129
  11.2 Quotas on Cloud Hosting ............................................................ 129
  11.3 Types of Resources ...................................................................... 129

12 Getting Help
  12.1 Other Documentation ................................................................. 133
  12.2 Q&A Community ........................................................................ 133
  12.3 Support Tickets ........................................................................... 133

13 Special Topics
  13.1 Moving to WebFaction from Other Hosting Providers ................ 137
  13.2 Application Security .................................................................... 140
  13.3 Migrating Servers ....................................................................... 144
  13.4 Strengthening Passwords .............................................................. 160
  13.5 Payment Card Industry Data Security Standard (PCI DSS) Compliance .................................................. 161
  13.6 Using Multiple Servers .................................................................. 162

Index .................................................................................................................. 165
Contents:
Welcome to WebFaction! We’re delighted to have you aboard. This user guide will give you an in-depth tour of the great things you can do with our system and how to put them all together with the tools and support we provide.

1.1 Services

WebFaction provides a complete web hosting service, with everything you need to get up and running. This guide will show you how all of these services work and how you can use them.

1.1.1 Web Hosting

WebFaction provides you with reliable and flexible web hosting. You will have the power to run everything from basic blogs to e-commerce sites to sophisticated web applications load-balanced over multiple servers.

1.1.2 Email

We provide a comprehensive email system with unlimited addresses that you will be able to access via SMTP, POP, IMAP, and webmail. You will also be able to protect your time and attention with spam protection, server-side rules, and auto-responders.

1.1.3 Database Hosting

With WebFaction, you will be able to setup multiple databases—whether you like MySQL or PostgreSQL—in a few clicks.

1.1.4 Backups

WebFaction conducts a weekly backup of all home directories, email accounts, databases, and cron jobs. We retain the last two backup snapshots. While we take great care to protect each server from data loss, we cannot guarantee the existence or completeness of any backups. Customers are responsible for backing up their data.

1.1.5 Monitoring and System Administration

We monitor our servers 24 hours per day, seven days per week so you don’t need to. We also make sure our servers are up to date with latest security patches and newest software, so you will be able to sleep soundly knowing that your data is secure and you will be able to run the latest applications.
1.1.6 Support

With WebFaction, you’re not alone. You will be able to make use of our comprehensive documentation and active community to learn new skills, complete common tasks, and get new ideas. You will also be able to contact our customer support team at any time to fix any problems that might arise.

1.2 The Complete System

At WebFaction we bring everything together into one complete system composed of several key parts:

- our website, where we describe services and plans,
- our blog, our status blog, and our Twitter account, where you can keep up with WebFaction’s latest developments,
- our Q&A Community, where you can participate in the WebFaction community and review questions and answers from the past,
- our documentation, where you can browse our documentation or download it as PDF files,
- our support system, where you can ask our support team a question directly,
- our control panel, where you can control every aspect of your account with a few clicks,
- and, our servers, where your data is stored and your email is managed.

You get access to our system through one inclusive account which is organized into three main components:

- Plans and Machines
- Email
- Domains, Applications, and Websites

These components are tied together with a powerful tool, our custom control panel. In the rest of this user guide, you will learn more about how the parts of our system and your account are organized. You will be able to use each of your account’s components, and use the control panel to make everything work together.
The control panel is WebFaction’s tool which links all of the portions of your account together. Throughout this
guide, you will be presented with directions on how to use the control panel for various tasks. But before you can do
anything else with the control panel, you will need to learn how to log in, change your password, and what to do in
the event that you’ve forgotten your password.

2.1 Log in to the Control Panel

To log in to the control panel:

1. In a browser, open https://my.webfaction.com/.

   **Note:** If you’re using Microsoft Internet Explorer 7, Google Chrome, Chromium, or Opera, make sure your
system clock is set correctly. If your system clock is set incorrectly (for example, to the wrong time zone), your
login cookie may expire before you can access the control panel.

2. In the **Username** field, enter your account name.

3. In the **Password** field, enter your password.

   **See also:**  
   *What to Do About a Lost Password*

4. Click the **Sign-in** button.

If you have **two-step login** enabled, follow these additional steps:

1. In the field that appears, enter the code provided by your two-factor authentication app.

   Alternatively, if you want to use one of your emergency backup codes to log in, click **Use an emergency
backup code** and enter your emergency backup code in the field.

2. Click the **Sign In** button.

2.2 Change Your Control Panel Password

To change your control panel password:

1. Log in to the control panel.

2. Click your username in the upper right corner. A menu appears.

3. Click **Change passwords**. The **Change password** form appears.
4. In the Control Panel password section, click Change. Three password fields appear:

5. In the Current password field, enter your current password.

6. In the New password field, enter a new password.

See also:

See Strengthening Passwords for important information about choosing passwords.

7. In the Confirm new password field, reenter your password.

8. Click the Change password button.

The new password is saved.

2.3 What to Do About a Lost Password

If you cannot remember your password, request a password recovery email. To request a forgotten password email:

1. In a browser, open https://my.webfaction.com/password/reset.

2. In the Username field, enter your WebFaction account name.

3. In the Email field, enter your email address.

4. Click the Send button. A password reset message from support@webfaction.com is sent to your email address. The message may take several minutes to arrive.

5. Follow the directions in the password reset message.

2.4 Two-Step Login

Two-step login, also known as two-factor authentication, 2FA, or two-step verification, is a way to add extra security to your account. With two-step login, you must provide a one-time code, in addition to your username and password, when you log in to the WebFaction control panel.
2.4.1 Turn on Two-step Login

**Warning:** After you’ve turned on two-step login, you must have access to your two-factor authentication app or backup codes to log in to your account. You will be locked out of your account without the backup codes or app!

To activate two-step login:
1. If you don’t already have one, install a two-factor authentication app on your mobile device. Use a device you ordinarily carry with you and not one you share with others, such as your mobile phone.
   
   Two-factor authentication apps include:
   - Authy (Android, iOS)
   - Google Authenticator (Android, iOS)
2. Log in to the WebFaction control panel.
3. In the upper right corner of the page, click your username. A menu appears.
4. Click Change passwords. The Change password form appears.
5. In the Two Step login section, click Enable. An Are you sure? dialog appears.
6. In your two-factor authentication app, add a new account. When prompted to do so, scan the square QR code with your app or enter the letters and digits beneath the code.
7. Once the account is added to your app, enter the digits provided by the app into the field in the Enable Two Step Login dialog in your browser.
8. Click the Enable two step login button. An Emergency Backup Codes dialog appears.
9. Copy your emergency backup codes to a safe place.
10. Click the Dismiss button.

You have turned on two-step login. The next time you log in to the WebFaction control panel, you will be prompted to provide either a code from your app or an emergency backup code.

2.4.2 Turn off Two-step Login

To deactivate two-step login:
1. Log in to the WebFaction control panel.
2. In the upper right corner of the page, click your username. A menu appears.
3. Click Change passwords. The Change password form appears.
4. In the Two Step login section, click Disable. An Are you sure? dialog appears.
5. To turn off two-step login, click Yes, go ahead.

You have turned off two-step login. The next time you log in to the WebFaction control panel, you will not be prompted to provide either a code from your app or an emergency backup code.
There are many tasks that require you to know your server’s name (and domain name), operating system, or IP address. The following sections will help you find these important details.

### 3.1 Finding Your Server’s Name

Your server’s domain name identifies your server to others. Some commands or services may require your server’s name or your server’s domain name.

You server’s name takes one of the following forms:

- web\(x\), where \(x\) is a number, such as web321
- dweb\(y\), where \(y\) is a number, such as dweb123
- wf-a-b-c-d-e, where \(a-b-c-d-e\) is series of numbers separated by hyphens, such as wf-203-0-113-1

Your server’s domain name is always of the form `name.webfaction.com`. For example, web321’s domain name is `web321.webfaction.com` and wf-203-0-113-1’s domain name is `wf-203-0-113-1.webfaction.com`.

To find your server’s name:

1. Log in to the WebFaction control panel.
2. In the Dashboard, find the Web Server widget.

   **Note:** Can’t find the Web Server widget? Try these steps:

   (a) Click the Add a widget button. The Add a widget dialog appears.
   (b) In the Select a widget menu, choose Web Servers.
   (c) Click the Add Widget button.

3. Find your server’s name in the list. If you have more than one server associated with your account, all of your servers will be in the list.

### 3.2 Finding Your Server’s Operating System

WebFaction’s servers run the following operating systems:
### Operating System

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Servers Names</th>
</tr>
</thead>
<tbody>
<tr>
<td>CentOS 5 (32-bit)</td>
<td>&lt;= web299 and &lt;= dweb88</td>
</tr>
<tr>
<td>CentOS 6 (64-bit)</td>
<td>web300 to web499 and &gt;= dweb89</td>
</tr>
<tr>
<td>CentOS 7 (64-bit)</td>
<td>&gt;= web500 and servers starting with wf</td>
</tr>
</tbody>
</table>

You can also check a server’s operating system version directly. To find your server’s operating system:

1. Open an SSH session to your account.
2. Enter `cat /etc/redhat-release` and press Enter. The version number appears.

### 3.3 Finding Your Server’s IP Address

Each WebFaction server has two or more unique IP (Internet Protocol) addresses. To find your server’s IP addresses:

1. Log in to the WebFaction control panel.
2. In the Dashboard, find the Web Server widget.

**Note:** Can’t find the Web Server widget? Try these steps:

(a) Click the Add a widget button. The Add a widget dialog appears.

(b) In the Select a widget menu, choose Web Servers.

(c) Click the Add Widget button.

3. Find your server’s IP addresses in the list. If you have more than one server associated with your account, all of your servers and their IP addresses appear in the list.

   IPv4 addresses have four numbers separated by dots (like 203.0.113.1). IPv6 addresses contain digits and letters separated by colons (like 2001:db8:85a3::8a2e:370:7334).

   Primary IP addresses are indicated by a dagger symbol (†). Secondary IP addresses are indicated by a double-dagger symbol (‡).

You can also check a server’s primary IP address in a shell session. To find your server’s primary IP address:

1. Open an SSH session to your account.
2. Enter `hostname --ip-address` and press Enter. The server’s primary IP address appears.
Aside from the control panel, there are two other key ways to access your account and data. The first is by remotely working with each machine your account has access to with SSH (Secure Shell). The second is with FTP (File Transfer Protocol).

4.1 Connecting with SSH

SSH is short for Secure Shell. SSH allows you to use a command line on a remote computer securely. You can connect to your WebFaction server with SSH using an SSH client.

To connect with SSH, use the following connection information:

- **Host**: server_name.webfaction.com, where server_name is your server’s name.
- **Username**: your SSH username (your WebFaction account name), or the username of an additional SSH account you have created.
- **Password**: your SSH account’s password.

On Mac OS X and Linux systems, you can start an SSH session with the command line program ssh. At the command line, enter ssh username@server_name.webfaction.com and press Enter.

On Windows, you need an SSH client, like PuTTY. To start an SSH session with PuTTY:

1. Start the PuTTY application.
2. In the Host Name (or IP address) field, enter username@server_name.webfaction.com where username is your SSH username.
3. Click the Open button.
4. The first time you connect, a PuTTY Security Alert appears. Click the Yes button to add the server to the list of known hosts.
5. In the main PuTTY window, a password prompt appears. Enter your SSH account password and press Enter.

You’re now connected with SSH using PuTTY.

4.1.1 Using SSH Keys

You can use a password-less, key-based SSH authentication system with your WebFaction account.
Linux and Mac OS X

To create and deploy a key with Linux or Mac OS X:

1. Create a key on your local computer.
   (a) Open a terminal session.
   (b) Create ~/.ssh, if it does not already exist. Enter `mkdir -p $HOME/.ssh`.
   (c) Switch to the ~/.ssh directory. Enter `cd ~/.ssh` and press Enter.
   (d) Generate your keys. Enter `ssh-keygen -t rsa`.
   (e) A series of prompts appear. Press Enter for each to accept the defaults.

2. Deploy the key to your server.
   (a) Copy the key to your server. Enter `scp ~/.ssh/id_rsa.pub username@server_name.webfaction.com:temp_id_rsa_key.pub` and press Enter. When prompted, enter your password.
   (b) Open an SSH session to your account. Enter `ssh username@server_name.webfaction.com` and press Enter. When prompted, enter your password.
   (c) Create ~/.ssh, if it does not already exist. Enter `mkdir -p $HOME/.ssh`.
   (d) Add your key to the authorized_keys file. Enter `cat ~/temp_id_rsa_key.pub >> ~/.ssh/authorized_keys` and press Enter.
   (e) Remove the temporary key file. Enter `rm temp_id_rsa_key.pub` and press Enter.
   (f) Secure the SSH keys. Enter `chmod 600 ~/.ssh/authorized_keys` and press Enter.
   (g) Secure the SSH directory. Enter `chmod 700 ~/.ssh` and press Enter.
   (h) Secure your home directory. Enter `chmod go-w $HOME` and press Enter.
   (i) Close the SSH session.

3. Verify that your key works properly. Enter `ssh username@server_name.webfaction.com` and press Enter. The session should begin without a prompt for a password.

PuTTY

To create and deploy a key with PuTTY:

1. Create a key on your local computer.
   (a) Download puttygen.exe.
   (b) Run puttygen.exe. The PuTTY Key Generator window appears.
   (c) Click to select SSH-2 RSA.
   (d) Click the Generate button.
   (e) Generate randomness by moving your cursor around until the key is finished.
   (f) Click the Save private key button.
   (g) Click the Yes button.
(h) Save the file to \texttt{c:\ssh\id_rsa.ppk}.

(i) Click the \textit{Save public key} button.

(j) Save the file to \texttt{c:\ssh\id_rsa.pub}.

(k) In the \textit{Public key for pasting into OpenSSH authorized_keys file} field, select and copy the key text.

2. Deploy the key to your server.

(a) With PuTTY, open an SSH session to your account.

(b) Create the \texttt{~/.ssh} directory. Enter \texttt{mkdir -p ~/.ssh} and press Enter.

(c) Open \texttt{~/.ssh/authorized_keys} in a text editor. For example, enter \texttt{nano -w ~/.ssh/authorized_keys} and press Enter.

(d) Paste the key text such that the key is alone on a single line.

(e) Save and close the file.

(f) Secure the SSH keys. Enter \texttt{chmod 600 ~/.ssh/authorized_keys} and press Enter.

(g) Secure the SSH directory. Enter \texttt{chmod 700 ~/.ssh} and press Enter.

(h) Secure your home directory. Enter \texttt{chmod go-w $HOME} and press Enter.

(i) Close PuTTY.

3. Configure PuTTY to use key authentication.

(a) In the \textit{Host Name (or IP address)} field, enter \texttt{username@\textit{server_name}.webfaction.com}.

(b) In the \textit{Category} menu, click to expand \textit{SSH}.

(c) In the \textit{Category} menu, click to select \textit{Auth}.

(d) In the \textit{Private key file for authentication}, enter \texttt{c:\ssh\id_rsa.ppk}.

(e) In the \textit{Category} menu, click to select \textit{Session}.

(f) In the \textit{Saved Sessions} field, enter a name for the connection.

(g) Click the \textit{Save} button. The connection name appears in the list.

4. Verify that your key works properly. Double-click the connection name in the list. The session should begin without a prompt for a password.

### 4.1.2 Troubleshooting SSH Connections

If you’re having trouble connecting with SSH, try these troubleshooting strategies:

- If you encounter a \textit{Connection timed out} or \textit{Connection refused} error, check your network connection and try again. If your connection is working properly, please open a support ticket. As a security precaution, your IP address might have been temporarily banned after several consecutive failed connection attempts.

- If you encounter a \textit{Permission denied} error, make sure your SSH server details and credentials are correct. Confirm that you’re connecting to the correct hostname. Likewise, make sure you’re using the correct username and \textit{password}.

If you’re using \textit{key-based authentication}, verify that your private key is available on your local computer and that your public key is deployed to the remote WebFaction server.
4.2 Connecting with FTP

You can review, change, and create files in your home directory with the FTP protocol. WebFaction supports FTP and SFTP. SFTP is much more secure than FTP; SFTP is highly recommended.

To connect with SFTP you use the following connection information:

- **Server**: `server_name.webfaction.com`, where `server_name` is your server’s name.
- **Connection type**: SFTP
- **Port**: 22
- **Username**: your SFTP username (your WebFaction account name), or the username of an additional SFTP account you have created.
- **Password**: your SFTP account’s password.

To connect with FTP (for shell users only), substitute the connection type with FTP and the port number with 21.

You can use this configuration information in your FTP client. If you do not have an FTP client, there are many free clients available, such as FileZilla (cross-platform), Cyberduck (Mac OS X), and FireFTP (a Firefox extension).

4.3 Changing Your FTP or SSH Password

If you have forgotten your SSH or FTP password, then change your password with the control panel.

1. Log in to the control panel.
2. Click your username in the upper right corner. A menu appears.
3. Click **Change passwords**. The **Change password** form appears.
4. In the **Server password** section, click **Change**. A field for the new password and a confirmation field appear:

   ![Change password form](image)

5. In the **New password** field, enter a new password.

   **See also**: See *Strengthening Passwords* for important information about choosing passwords.

6. In the **Confirm new password** field, reenter your password.
7. Click the **Change password** button.

The new password is saved.
4.4 Additional Users

If you’re working with a team or need to grant limited access to someone else, you can create additional users. Extra users have their own (unique per machine) username, password, and home directory.

See also:

To learn how to grant additional users access to your applications, see *Granting Access to Specific Users*.

4.4.1 Creating Additional Users

You can create an extra user from the control panel. To create a user:

1. Log in to the WebFaction control panel.
2. Click *Account → SSH/SFTP users*. A list of users appears.
3. Click the *Add new user* button. The *Create a new user* form appears.
4. In the *Username* field, enter a username for the new user.
5. In the *Password* field, enter a password for the user.
   
   See also:

   See *Strengthening Passwords* for important information about choosing passwords.

6. In the *Confirm password* field, reenter the password.
7. If applicable, in the *Machine* menu, click to select a server for the user.
8. In the *Shell* menu, click to select the user’s shell type. Select */bin/bash* for the typical Bash shell. To limit the new user to SFTP connections only, click to select *No shell (sftp only)*. To allow the new user unsecured FTP access, you must choose a shell.
9. If needed, click to select the groups to add the user to. Use *Ctrl* or *Command* click to select more than one group.
10. Click the *Save* button.

The user is created and added to the list.

4.4.2 Granting Permissions to Additional Users

You can allow additional users read-only or read/write access to directories with the control panel. You can allow extra users to access directories in your home directory (such as application directories), or directories in your other additional users’ home directories.

To grant an additional user access to a directory:

1. Log in to the WebFaction control panel.
2. Click *Account → SSH/SFTP users*. A list of users appears.
3. Click on the user that you want to grant access to. The extra user’s details appear.
4. Click the *Grant permissions* button.
5. Choose the path to grant access to. In the *Grant access to section*, choose a base path, which is the home directory of your main account or one of your extra users. In the adjacent field, complete the path to the directory.
For example, to grant a user access to the directory for an application called myblog, click to select your main user’s home directory (/home/username/), then enter webapps/myblog.

6. Choose the user’s level of access to the directory. Click to select Read only or Read/write.

7. Click the Save button. A confirmation message appears.

The user now has access to the directory you chose.

### 4.4.3 Removing Additional Users

You can delete an extra user with the control panel. To delete a user:

1. Log in to the WebFaction control panel.
2. Click Account → SSH/SFTP users. A list of users appears.
3. Click the user to be deleted. The user’s details appear.
4. Click the Delete button. A prompt, *Are you sure you wish to delete the user*, appears.
5. To delete the user, click Yes, I’m sure. To preserve the user, click No, Cancel.

If you opted to delete the user, a confirmation message appears and the user disappears from the list.

### 4.5 Backups

WebFaction conducts a weekly backup of all home directories, email accounts, databases, and cron jobs. We retain the last two backup snapshots. While we take great care to protect each server from data loss, we cannot guarantee the existence or completeness of any backups. Customers are responsible for backing up their data.

If you would like to have something restored from our backups, please open a ticket and let the WebFaction support team know what data from what date you would like restored.
When you work with WebFaction, all of your activity is organized under the umbrella of an account, a unique username which identifies you on our machines and in the control panel. Your account is comprehensive: it’s used to manage which services you receive, how you interact with the WebFaction support team, how you make payments, and how you receive the benefits of our affiliate program.

Note: If you don’t have an account yet, sign up.

5.1 Plans and Services

Each account has services associated with it. When you signed up with WebFaction, you selected a plan. As your sites grow, you may change plans or add services which will be organized alongside your plan under your account.

Typically, you will need only one account for the services you use, since you can add plans and add-on services to your account at any time. That said, you’re free to open additional accounts, if desired (for example, one for personal use and another for your business), but they will be billed, managed, and supported separately.

5.1.1 Plans

Plans are a complete collection of services which include disk space, bandwidth, application memory, databases, email addresses and more. Each plan has varying amounts of disk space, bandwidth, and application memory.

An account can have multiple plans. Multiple shared plans aggregate disk space and bandwidth across servers (memory is not aggregated). Cloud server plan resources are not aggregated.

Plans are flexible and you are not bound to one particular plan for the lifetime of the account. To switch plans, click Account → Resize or migrate plan in the control panel.

5.1.2 Add-on Services

Some add-on services may be available for your plan, such as additional disk space or IP addresses. To add services, click Account → Upgrade / downgrade in the control panel.

Sometimes it’s wise to consider upgrading to a different plan instead. Upgrading can be easier and less expensive than adding services individually.

See also:

For our current services and prices, see Features & prices.
5.1.3 Monitoring and Managing Disk and Bandwidth Consumption

At any time you can use the control panel to see how much disk space and bandwidth has been used.

See also:

Monitoring Memory Usage

Disk

To see how much disk space has been consumed:
1. Log in to the control panel.
2. Click Usage → Disk usage. The disk usage summary appears.

The disk usage summary shows you how much disk has been consumed by home directories, MySQL databases, PostgreSQL databases, and mailboxes. It also indicates what percentage of your account’s disk allotment has been used.

Bandwidth

To see how much bandwidth has been consumed:
1. Log in to the control panel.
2. Click Usage → Bandwidth usage. The bandwidth usage summary appears.

The bandwidth usage summary provides two major reports: Last 14 days and Last 12 months. The Last 14 days report shows how much bandwidth was consumed and by which domain names per day for the last two weeks. The Last 12 months report shows how much bandwidth was consumed and by which domain names per month for the last year.

5.2 Communicating with WebFaction

Your account is used to manage your contact with the WebFaction support team. Even if you have multiple plans spread across many machines, all of your support requests are managed under your account name.

5.2.1 Contacting You

In the event that WebFaction needs to contact you regarding your account, you will be reached by the email address you have on file with us. For example, if you consume your allocated disk space, bandwidth, or memory, we send you an email to let you know. But you do need to make your current email address (as well as an email address which is not hosted by WebFaction, if the two are not the same) on file so that we can reach you.

5.2.2 Adding Contact Information with the Control Panel

To add a new point of contact with the control panel:
1. Log in to the control panel.
2. Click Account → Contacts. The list of contacts appears.
3. Click the Add new contact button. The New contact form appears.

4. Optional: In the Title field, enter the contact person’s title.

5. In the First name field, enter a first name.

6. In the Last name field, enter a last name.

7. In the Email address field, enter a valid email address.

8. In the Email usage list, click to select one or more message types for the point of contact to receive.

9. Optional: In the Twitter username section, enter your Twitter username.

10. Optional: If you provided your Twitter username and you wish to allow us to retweet you or quote your tweets about WebFaction, in the Twitter username section, click Yes.

11. Optional: To use the contact details on invoices:
   (a) In the Use on invoice section, click Yes. Company and address fields appear.
   (b) In the Company field, enter your company name.
   (c) In the Address, City, and Zipcode fields, enter your invoice address.
   (d) In the Country menu, click to select your country.

12. Click the Save button.

5.3 Payments

You can choose automatic monthly payments or make one-off prepayments.

If you choose to pay with automatic monthly payments, your payment source (a credit card or PayPal account) will be charged each month to pay for the next month of service (minus any balance credited to your account).
If you choose to pay with one-off prepayments, then you can pay one month, three months, six months, or one year in advance, or you can add any dollar amount to your account balance. When you choose to prepay, your account is paid for each month out of your account balance until it runs out.

If you choose to pay with one-off prepayments, then our system will send you a reminder when your next payment is due. These payments are not charged automatically. You can make prepayments using the control panel.

We accept these payment sources:

- American Express (long-term pre-payments only)
- Discover (long-term pre-payments only)
- MasterCard
- PayPal
- Visa

Unfortunately, we cannot accept checks or money orders.

**Missing Payments**

We understand that occasionally payments are not completed exactly as you imagined they would be. In the event that your payment source is declined or your annual payment is not received, WebFaction will always send a notification email. If you promptly update your payment source or make a payment, your service will continue as usual. You don’t even need to contact us.

If there’s some hurdle keeping you from making a payment (for example, you’re waiting for a replacement card), please contact us. If you’re in contact with us and we know you’re working to resolve the issue, we will not disable or cancel your account.

However, if it takes more than two weeks to make your account properly paid for and you have not contacted us, we may deactivate some of the services associated with your account. During this period, you can update a payment source, make a payment, and contact us; we’ll be happy to enable your services promptly.

If your account continues to be unpaid, your account will be canceled one month after we disable your account. WebFaction does not retain data for canceled accounts; if you want to be sure to have access to your sites and data, please make your payments promptly or make sure your payment sources are current in the control panel.

If you would like to close your account with us, you can use our no-hassle account cancellation form.

The WebFaction control panel allows you to make payments, add a payment source (for accounts paid month-to-month), select a payment source, and review your payment history.

### 5.3.1 Make a Payment with the Control Panel

To add money to the balance on your account:

1. **Log in to the WebFaction control panel.**
2. Click Billing → Make a one-off payment. The Make a payment form appears:
3. Choose an amount to pay. In the Payment period section, click to select a standard period or Other. If you selected Other, in the next field, enter the amount to pay.

4. In the Payment type field, click to select a payment type.

5. Click the Make Payment button and you’ll be redirected to the PayPal site. Please refer to the PayPal site to complete the transaction.

The amount specified is added to your account balance.

Note: If you do not want to use PayPal, to make an one-off payment, we have an alternative payment gateway that you can use instead. To do so, please open a support ticket and we can provide further instructions.

### 5.3.2 Add a Payment Source with the Control Panel

Note: If the expiration date has passed or another detail has changed for a payment source, you must create a new payment source to replace it. As a security measure, payment sources cannot be edited.

To create a new payment source (for automatic monthly payments only):

1. Log in to the control panel.

2. Click Billing → Payment sources. The list of payment sources appears.

3. Click the Add new payment source button. The Payment details form appears.

4. In the Payment type menu, click to select Visa/MasterCard or PayPal.

5. In the Label field, enter a description for the payment source. Use the label to remind you which card it is later.

6. Click the Save button and you’ll be redirected to the PayPal site. Please refer to the PayPal site to complete the process.

Note: A $0.10 verification charge will be made against any new payment source. Once verification of the payment source is complete, the charge will be canceled.

The new payment source is automatically set as the active payment source.
5.3.3 Change the Active Payment Source in the Control Panel

If you have stored more than one payment source in the control panel, you can change the active payment source from one to another. To make a payment source active:

1. Log in to the control panel.
2. Click *Billing → Payment sources*. The list of payment sources appears.
3. Click the row of the payment source to modify. The payment source’s details appear.
4. In the *Is active* section, click *Yes*.
5. Click the *Save* button.

The payment source is marked active. The previously active source is deactivated.

5.3.4 Remove a Payment Source in the Control Panel

If you have more than one payment source in the control panel, you can remove a payment source. If you only have one payment source set in your account, you must *create a new active payment source* before removing another.

1. Log in to the control panel.
2. Click *Billing → Payment sources*. The list of payment sources appears.
3. Click the row of the payment source to delete. The payment source’s details appear.
4. Click the *Delete* button. A prompt, *Are you sure you wish to delete the payment source*, appears.
5. To delete the payment source, click *Yes, I'm sure*. To keep the payment source, click *No, Cancel*.

If you opted to delete the payment source, it is deleted and a confirmation message appears.

5.3.5 Review Your Payment History with the Control Panel

To review payments you have made and services you have paid for with your account balance:

1. Log in to the control panel.
2. Click *Billing → Payment transaction history*. The list of transactions appears.

5.3.6 Get an Invoice for a Payment with the Control Panel

To see an invoice for a past payment:

1. Log in to the control panel.
2. Click *Billing → Payment transaction history*. The list of transactions appears.
3. Click the *Invoice* button next to a payment entry. The invoice appears. You may save or print the invoice for your records.

*Note:* If you require an invoice before making a payment or if the invoice button does not appear for one of your existing payments, please *open a support ticket*. 

5.4 Affiliate Program

Our affiliate program lets you earn money (via PayPal) or credit to your account for letting your friends, blog readers, and anyone else know about WebFaction. If someone signs up with WebFaction by following one of your affiliate links, you will receive 10% of that person’s spending on WebFaction services. Some restrictions do apply, however, so check out the program details.

5.4.1 Review Your Affiliates with the Control Panel

To see who has started a plan with your username as the referrer:

1. Log in to the control panel.
2. Click Affiliate program → Affiliates. The list of affiliates appears.

5.4.2 Review Your Affiliate Payments with the Control Panel

To see a list of payments made to you or credit to your account as a part of the affiliate program:

1. Log in to the control panel.
2. Click Affiliate program → Affiliates payments. The list of affiliates payments appears.

5.4.3 Change How You Receive Affiliate Payments with the Control Panel

To change how your receive your affiliate program payments:

1. Log in to the control panel.
2. Click Affiliate program → Affiliates settings. The Affiliate settings form appears:

   ![Affiliate settings form]

3. Click the Edit button.
4. Choose your preferred way to receive payments.
   - To receive affiliate payments as a credit toward WebFaction plans and services, click Account Credit.
   - To receive affiliate payments as money sent to your PayPal account, click PayPal. A text field appears.
5. If you selected PayPal, in the text field, enter the email address associated with your PayPal account.
6. Click the Save button.

Future affiliate payments are applied to the specified payment method.
5.4.4 Review Your Affiliate Click Statistics with the Control Panel

To review how many clicks you’ve received on affiliate links:

1. Log in to the control panel.
2. Click Affiliate program → Affiliate click stats. Your last two weeks and twelve month statistics appear.

5.5 Canceling Your Account

If you’re no longer interested in maintaining your account, we’ll be sorry to see you leave and hope you’ll be back soon. You can use the control panel to cancel your account, leave feedback, and, if applicable, request a refund under the terms of our 60-day money back guarantee.

5.5.1 Cancel Your Account with the Control Panel

**Warning:** This process cannot be undone. Your data will be immediately and irrevocably deleted and cannot be recovered.

To cancel your account:

1. Log in to the control panel.
2. Click Billing → Cancel account. The Cancel account form appears.
3. Click to select Please cancel my account effective immediately.
4. Optional: Enter your feedback in the text field.
5. Click the Cancel Account button.
A domain name is a unique and human-readable label, like google.com or bbc.co.uk. Your browser and other software tools can use that label to find a specific computer on the Internet. Configured correctly, a domain name under your control can be pointed to WebFaction’s servers.

6.1 Getting a Domain Name

Domain names are managed by registrars. You can purchase a domain name through a registrar; the Internet Corporation for Assigned Names and Numbers (ICANN) maintains a list of accredited registrars. You may already own a domain purchased through a registrar, reseller, or previous web host. If you don’t already own a domain name or you would like to purchase additional domain names, purchase one through a registrar or reseller. At this time, WebFaction is not a registrar and does not sell domains.

6.2 Pointing Your Domain to WebFaction’s Servers

Note: You can only point your domain to WebFaction’s name servers after adding it to the WebFaction Control Panel, not before.

We will reject addition of domains that are already pointed at WebFaction’s name servers.

This is one of the ways we protect our customers from DNS hijacking.

To use a domain name with WebFaction:

1. Log in to the WebFaction control panel.
2. Add your domain through the WebFaction Control Panel (see Adding a Domain to the Control Panel.) and then
3. Use your domain registrar’s website to set your domain’s name servers to WebFaction’s domain name servers.

WebFaction’s domain name servers are:

<table>
<thead>
<tr>
<th>Name Server</th>
<th>IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>ns1.webfaction.com</td>
<td>185.20.51.42</td>
</tr>
<tr>
<td>ns2.webfaction.com</td>
<td>103.44.220.74</td>
</tr>
<tr>
<td>ns3.webfaction.com</td>
<td>62.138.130.11</td>
</tr>
<tr>
<td>ns4.webfaction.com</td>
<td>148.72.160.4</td>
</tr>
</tbody>
</table>

Your registrar may not require all four domain name servers; enter as many as your registrar supports.

Note: After you configure domain to use WebFaction’s domain name servers, it may take up to 48 hours for all
requests for your domain to correctly resolve to WebFaction’s servers. The delay is often referred to as propagation. The delay is the result of caching, which is used heavily in the domain name system.

Setting your domain’s name servers to WebFaction’s name servers isn’t enough to get a working site, however.

### 6.2.1 Using External Name Servers

Optionally, you can use your own or third-party domain name servers instead of WebFaction’s name servers. Please follow your registrar’s instructions to configure your domain to use your preferred name server, then use the following DNS details to configure your name server to use WebFaction services.

#### A and AAAA

If your domain uses your WebFaction server to host a website, then configure your domain’s A and AAAA records to use your server’s IP address (such as 203.0.113.1 for IPv4 or 2001:db8:85a3::8a2e:370:7334 for IPv6). See Finding Your Server’s IP Address for details.

If you have multiple machines associated with your account, then check which machine is hosting the site you’re configuring:

1. Log in to the WebFaction control panel.
2. Click Domains / websites → Websites. The list of websites appears. For each site in the list, the server name and IP address for that site appears under the site’s name.

#### MX

If your domain uses WebFaction’s mail servers to receive mail, then configure your domain’s MX records to use the following servers and priority 10 for each server:

<table>
<thead>
<tr>
<th>Server</th>
<th>Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>mx7.webfaction.com</td>
<td>10</td>
</tr>
<tr>
<td>mx8.webfaction.com</td>
<td>10</td>
</tr>
<tr>
<td>mx9.webfaction.com</td>
<td>10</td>
</tr>
</tbody>
</table>

#### SPF

If your domain uses WebFaction’s mail servers exclusively, then configure your domain’s SPF record to

```
v=spf1 include:spf.webfaction.com ~all.
```

If your domain receives mail at WebFaction’s mail servers and you also use another SMTP server to send mail, then configure your domain’s SPF record to

```
v=spf1 include:spf.webfaction.com a:domain ~all.
```

where domain is the domain name of the other SMTP server you use.

### 6.3 Adding a Domain to the Control Panel

**Note:** You can only point your domain to WebFaction’s name servers after adding it to the WebFaction Control Panel, not before.

We will reject addition of domains that are already pointed at WebFaction’s name servers.
This is one of the ways we protect our customers from DNS hijacking.

**Before** you point your domain to WebFaction’s domain name servers, you must add your domain to the control panel. To add the domain with the control panel:

1. Log in to the control panel.
2. Click *Domains / websites → Domains*. The list of domains for your account appears.
3. Click the *Add new domain* button. The *Domain names to add* field appears.

   ![Domain names to add](image)

   Enter one or more domains or subdomains separated by whitespaces or newlines. For instance: `example.com www.example.com`.

4. In the *Domain names to add* field, enter one or more domain names separated by spaces or newlines (for example, `example.com` or `example.com www.example.com`).

   You may choose to enter wildcard subdomains with an asterisk, like `*.example.com`. Wildcard subdomains can be used to handle traffic for any and all matching subdomains. For example, a domain entry `*.example.com` handles `abc.example.com`, `xyz.example.com`, and any other subdomain of `example.com`.

   **Note:** If you’re adding a domain name that contains unicode characters, you must enter the domain name in Punycode. Punycode is a way of expressing unicode domain names using only ASCII characters. To simplify entering unicode domains, you may want to use a third-party Punycode converter such as:

   - charset.org Punycode converter
   - PunyCoder
   - Verisign IDN Conversion Tool

5. Click the *Save* button. The domain names are added to the list of domain names and a confirmation message appears.

   **Note:** If you are *using your own name server*, then create A records to point your subdomains at your WebFaction server’s IP address.

### 6.4 Managing DNS Records with the Control Panel

DNS, or Domain Name System, is the system that translates domain names (like `example.com`) to a server’s IP address (like `192.0.43.10`). If a domain is *added to the control panel* and then *pointed to WebFaction’s name servers*, WebFaction servers will handle Internet traffic directed to that domain. To use a domain with WebFaction websites and applications, special DNS configuration is not required. Changing DNS settings may be useful, however, for configuring a domain’s traffic to use external services.

The WebFaction control panel can make several common DNS changes, including creating:

- **A** and **AAAA** records, to use a domain with a third-party server
- **CNAME** records, to alias one domain to another
WebFaction User Guide

- **MX** records, to specify a domain’s mail provider
- **SPF** (Sender Policy Framework) records, to reduce some kinds of spam
- **SRV** records, to specify the hostname and port of a service
- **TXT** records, to specify other services associated with a domain

**Note:** Some DNS changes may take up to 48 hours to take effect, as the changes propagate through the entire Domain Name System.

### 6.4.1 Configuring A and AAAA Records

To configure a domain to use a third-party server to handle traffic:

1. Log in to the WebFaction control panel.
2. Click **Domains / websites → Domains**. The list of domains appears.

   **Note:** If you have not done so already, add the domain to your account.

3. Click on the domain name to reconfigure. The domain’s settings appear.
4. In the **Hosting** section, click to select **External**.
5. For each third-party server:
   a. Click **Add IP address**. A new field appears.
   b. In the field, enter the IP address of the third-party server.
      - To create an **A** record, enter an IPv4 address (for example, **192.0.2.5**).
      - To create an **AAAA** record, enter an IPv6 address (for example, **2001:0db8:85a3:0000:0000:8a2e:0370:7334**).
6. Click the **Save** button.

The **A** or **AAAA** records are created. Requests to the domain are directed to the specified IP address.

### 6.4.2 Configuring CNAME Records

To configure a domain to act as an alias for another domain:

1. Log in to the WebFaction control panel.
2. If you have not done so already, add the domain to your account.

   **Note:** If the CNAME domain is for a website hosted on WebFaction, also add the domain to a website. If the WebFaction-hosted domain isn’t part of a website record then your visitors will get an error message because your web server won’t know what to do with incoming traffic.

3. Click **Domains / websites → Domains**. The list of domains appears.
4. Click on the domain name to reconfigure. The domain’s settings appear.
5. In the **Hosting** section, click to select **CNAME**. A new field appears.
6. In the field, enter a domain name.
7. Click the **Save** button.

The **CNAME** record is created. Requests to the domain are handled by the **CNAME** domain’s server.
6.4.3 Configuring MX Records

**Note:** MX records cannot be created for domains with CNAME records.

To specify servers responsible for receiving mail for a domain:

1. Log in to the WebFaction control panel.
2. Click Domains / websites → Domains. The list of domains appears.
   
   **Note:** If you have not done so already, add the domain to your account.

3. Click on the domain name to reconfigure. The domain’s settings appear.
4. In the Email section, click to select External.
5. For each mail server:
   
   (a) Click Add Mail Server. Priority and Server fields appear.
   
   (b) In the Priority field, enter an integer priority value. Smaller numbers have higher priority.
   
   (c) In the Server field, enter the mail server’s domain name.
6. Click the Save button.

The MX records are created. Incoming mail to a domain is received by the named servers in priority order.

6.4.4 Configuring SPF Records

**See also:**

For more information about SPF and spam prevention, see Spam Protection.

To create a Sender Policy Framework record:

1. Log in to the WebFaction control panel.
2. Click Domains / websites → Domains. The list of domains appears.
   
   **Note:** If you have not done so already, add the domain to your account.

3. Click on the domain name to reconfigure. The domain’s settings appear.
4. In the Other DNS records section, in the Add DNS Record... menu, click to select SPF. A SPF Record field appears.
5. In the SPF field, enter an SPF value.

   If your domain uses WebFaction’s mail servers exclusively, then enter
   v=spf1 include:spf.webfaction.com ~all.

   If your domain receives at mail at WebFaction’s mail servers and you also use another SMTP server to send mail, then enter v=spf1 include:spf.webfaction.com a:domain ~all, where domain is the domain name of the other mail server.

   If your domain doesn’t use WebFaction’s mail servers at all, then check your mail provider’s documentation for the correct SPF record.

   If your domain uses Google Apps mail, then see Using Google Apps for Email for detailed instructions.
6. Click the Save button.
WebFaction User Guide

The SPF record is created. Email recipients that support SPF use the record to determine whether email received from the domain was sent from an authorized server.

### 6.4.5 Configuring SRV Records

To create a SRV record:

1. Log in to the WebFaction control panel.
2. Click Domains / websites → Domains. The list of domains appears.
3. If you have not done so already, add the service protocol subdomain to your account in the form of \_Service\_Proto.Name - for example, \_xmpp-server\_tcp.example.com.
4. Click on the service protocol subdomain name to reconfigure. The subdomain’s settings appear.

Note: SRV records may only be added to service protocol subdomains which are in the form of \_Service\_Proto.Name. For example, an SRV record may be added to \_xmpp-server\_tcp.example.com, but not www.example.com.

5. In the Other DNS records section, in the Add DNS Record… menu, click to select SRV. New Priority, Weight, Port, and Target fields appear.
6. In the fields, enter the SRV record data.
7. Click the Save button.

The SRV record is created.

### 6.4.6 Configuring TXT Records

To create a TXT record:

1. Log in to the WebFaction control panel.
2. Click Domains / websites → Domains. The list of domains appears.

Note: If you have not done so already, add the domain to your account.

3. Click on the domain name to reconfigure. The domain’s settings appear.
4. In the Other DNS records section, in the Add DNS Record… menu, click to select TXT. A TXT field appears.
5. In the TXT field, enter the TXT record value.
6. Click the Save button.

The TXT record is created.

### 6.5 Troubleshooting DNS Problems

Sometimes there are hurdles to getting a domain name working with a website. Check out these solutions to DNS problems.
6.5.1 You See an Error Message Regarding Pointing Name Servers

If you see this message when adding a new domain to the WebFaction Control Panel:

**For security reasons, you can only point your domain’s name servers to WebFaction *after* you have added it to our system.**

This is caused by pointing your domain at WebFaction’s name servers before adding it in the Control Panel (see *add a domain*).

To successfully add your domain and use WebFaction’s name servers: 

1. Use your domain registrar’s website to set your domain’s name servers to domain name servers other than WebFaction’s name servers.
2. Once your change has propagated, you will be able to *add the domain to your account.*
3. If you wish to use WebFaction’s name servers, you can *set this up* now.

6.5.2 A Domain Still Resolves to a Previous Host

If your domain name is still resolving to your old hosting service there are a few steps you can take to get everything working:

- **Wait up to 48 hours.** If you recently changed domain name servers, please wait while the change to your domain information circulates throughout the domain name system.

- **Flush your DNS cache.** In much the same way your browser caches web pages and images to speed up page loads, your system may cache DNS requests to open connections faster. This is most obvious when one computer accesses your site correctly on WebFaction, while another still loads your site on your previous host. You can also detect DNS caching when the IP address of your domain (for example, when using **ping**) is still your previous host’s server’s IP address.

To clear your DNS cache on **Mac OS X:** see Apple’s document *Reset the DNS cache in OS X* for instructions that apply to your specific version of OS X.

To clear your DNS cache on **Windows 8** or **Windows 8.1:**

1. Open the Start screen. Click the Windows Start button or press the Windows key.
2. Type **cmd**. **Command Prompt** appears in the search results.
3. Right-click on **Command Prompt**. A menu appears.
4. Click **Run as administrator**. A **User Account Control** dialog appears.
5. Click **Yes**. The command prompt appears.
6. Enter **ipconfig /flushdns** and press **Enter**.

To clear your DNS cache on **Windows Vista** or **Windows 7:**

1. Click **Start → All Programs → Accessories.**
2. Right-click on **Command Prompt**. A menu appears.
3. Click **Run as administrator**. A **User Account Control** dialog appears.
4. Click **Continue**. The command prompt appears.
5. Enter **ipconfig /flushdns** and press **Enter**.

To clear your DNS cache on **Windows XP:**

1. Press **Windows + R**. The **Run** dialog appears.
2. Enter **cmd** in the **Open** field.
3. Press Enter. The command prompt appears.

4. Enter ipconfig /flushdns.

5. Press Enter.
CHAPTER SEVEN

APPLICATIONS AND WEBSITES

The WebFaction web hosting system works by keeping track of three important components of your account:

• **domains** – domain names, like *example.com* (see Domains)
• **applications** – a collection of directories, files, and processes used to serve data
• **websites** – a record used in our system to determine which URLs should be served by which applications (see A Sophisticated Website Configuration)

In this section of the user guide, you will learn how to assemble domain names, applications, and your files into a complete website that your visitors can reach and use.

**See also:**
The next chapter of the user guide, *Example Websites*, demonstrates common use cases.

### 7.1 Applications

To serve content, run code, and interact with databases, you need **applications**. Applications are collections of directories, files, and system settings which allow media to be served and code to be executed by the web server.

For example, an application could be as simple as a *Static-only* application storing a handful of HTML files and some JPEG images. In contrast, however, applications can be sophisticated software tools, like a *Django* application or the *WordPress* blogging engine. You can even run a *Custom app (listening on port)* to use software not covered by one of WebFaction’s one-click installers.

The control panel allows you to manage applications installed on your account. You can install a wide variety of applications, including:

• AWStats
• CherryPy
• Django
• Drupal
• Passenger
• Python (Apache with mod_wsgi)
• Ruby on Rails
• Static-only
• Static/CGI/PHP
• Subversion
You can also create a custom application, which lets you listen on a specified port.

When you create an application with the control panel, a directory is created in your home
directory—$HOME/webapps/app, where app is the application name you entered on the control panel—along
with any required files, like .htaccess or included scripts. If the application is a long-running process, the
control panel installer also adds a cron job which periodically restarts the process if it stops running.

Note: An application cannot be reached from outside a WebFaction server without being configured in a website
entry with the control panel. You’ll learn more about configuring website entries in the Websites section.

7.1.1 Create an Application with the Control Panel

See also:

These directions show you how to create a new application unconnected to a website record. If you’re creating a
website too, see Create a Website with the Control Panel for instructions to create websites and applications at the
same time. If you’re creating an application that won’t be attached to a particular website record (such as a MongoDB
installation), follow these directions.

To create an application with the control panel:

1. Log in to the control panel.
2. Click Domains / websites → Applications. The list of applications appears.
3. Click the Add new application button. The Create a new application form appears.
4. In the Name field, enter a name for the application.
5. In the App Category menu, click to select an application category.
6. In the App Type menu, click to select a specific application version.
7. If applicable, in the Machine menu, click to select a web server.
8. Review the application description. The description contains important details, cautions, and links to
documentation.
9. If applicable, in the Extra info field, enter any required information. See the application description for details.
10. If applicable, choose whether to open this application’s port. In most cases, opening a port is not necessary;
only open a port if you know you require it. If selected, the port is opened on a shared IP address and, if
applicable, your dedicated IP address.

To open the port, click to select Open a port in the server firewall for the application.
11. Click the Save button.

The application is installed and added to the list of applications. If a port was opened, the applicable IP addresses
appear beneath the list of installed applications.
7.1.2 Installing Applications Not Listed in the Control Panel

If an application or a version of an application you want to use is not listed in the control panel, don’t despair. First, check out WebFaction Software Documentation, in which we provide instructions for additional software packages not covered by a control panel installer. You can also install custom applications using one of the three “generic” application types:

- **Static/CGI/PHP**: If the software you want to use can run directly from the document root directory, like many PHP software packages, use a Static/CGI/PHP application. Once you’ve installed the application, upload files to `~/webapps/static_app`, where `static_app` is the name of the application.

  See also:

  Static Files, CGI Scripts, and PHP Pages

- **Symbolic link to static/cgi/php**: If the software you want to use needs only a subset of its files exposed to the web, use a Symbolic link to static/cgi/php application. When creating the application, enter the absolute path to the directory you want to expose to the web in the `extra_info` field. In all other respects, it works like a Static/CGI/PHP application.

- **Custom app (listening on port)**: If the software you want to use listens on a network port, use a Custom app (listening on port). A Custom app assigns a specific port number where incoming traffic will be directed. Install the software and configure it to listen to the specified port.

  See also:

  Custom Applications

If you need to repeatedly install an application not provided by the WebFaction control panel, see the WebFaction API Documentation.

7.2 Websites

Usually, an application by itself isn’t particularly useful: it needs a web address—a domain name and a path—so it can be reached by a web browser. A website entry in the control panel connects an application to a domain and path. A website entry instructs your WebFaction web server to forward requests for a specific URL path to an application, and then return the application’s response.

The Life Cycle of a Request and Response

Requests to a URL path are received by a WebFaction server’s front end process (an instance of the nginx web server). Such requests are proxied to a specific application’s process, such as a Django application’s instance of the Apache web server. The front end process waits for a response from the application and forwards that response to the source of the original request.

Please see the diagram below for a closer look at how requests are received and replied to in a WebFaction server.
For example, suppose you have a Drupal application, `my_drupal`, and a domain, `mysite.example`. A website lets you configure `mysite.example` to point to your application, `my_drupal`. When a visitor opens `http://mysite.example/` in their browser, your Drupal application will load at that URL. Behind the scenes, the web server proxies requests for `mysite.example` to the application stored at `~/webapps/my_drupal`.

**Hint:** Creating a new site, but haven’t decided on a domain name yet? Or maybe you want to test the latest version of your site before taking it live on your existing domain name? Create subdomains of your `username.webfactional.com` domain to connect to your applications instead (like `testsite.username.webfactional.com`). See *Adding a Domain to the Control Panel* for more information.

Websites permit much more sophisticated configurations, however. You can configure a specific path (or *mount point*) at a domain to point to an application, allowing you to run multiple applications under a single domain. For example, suppose you have a pair of applications, a Drupal application called `my_drupal` and a Static/PHP/CGI application containing phpBB called `forum`, and a domain, `mysite.example`. You can configure a website to serve `my_drupal` from the root path (`/`) of `mysite.example` and `forum` from `/forum`:

```
mysite.example
/   -> my_drupal
/forum -> forum
```

Domain and path combinations and applications may have a many-to-one relationship. While a particular domain and path combination can only point to one application, numerous domain and path combinations can point to the same application.

### 7.2.1 Create a Website with the Control Panel

To create a Website record (and any needed applications) with the control panel:

1. Log in to the control panel.
2. Click *Domains / websites* → *Websites*. The list of websites appears.
3. Click the *Add new website* button. The *Create a new website* form appears.
4. In the *Name* field, enter a website name.
5. If applicable, in the *Machine* menu, click to select the server to host the website.
6. If applicable, in the IP address menu, click to select the IP address to serve the site.

7. If you want your site served over an HTTPS connection:
   (a) Click to select Encrypted website (https).
   (b) In the Choose a certificate menu, click to select a certificate.

   The Shared certificate is WebFaction’s shared certificate. If you use the shared certificate, most browsers will warn that your domain doesn’t match the certificate (though the connection will still be encrypted).

   To add your own certificate, see Secure Sites (HTTPS).

   **Note:** A website’s HTTPS setting is either on or off. Connections to the website are over the specified protocol only.

   If you want your site to be served over HTTPS exclusively, then create a redirect from HTTP to HTTPS.

   If you need your site to be available over both HTTP and HTTPS, then create two website records, one HTTP and the other HTTPS, and ensure that both sites are assigned to the same IP address.

8. For each domain name you want to use with the website, add it to the list of domains. In the Domains field, enter the domain name. Enter one or more domain names. If the domain has not yet been added to the control panel, click the Create link that appears at the bottom of the list of domains to add it.

   **Note:** Don’t forget to point new domains to the WebFaction name servers after you have added them.

9. Add one or more applications to the website.

   To add a new application:
   (a) Click Add an application → Create a new application. The Create a new web app form appears.
   (b) In the Name field, enter a name for the application.
   (c) In the App category menu, click to select an application category.
   (d) In the App type menu, click to select a specific application version.
   (e) If applicable, in the Extra info field, enter any required information. See the application description for details.
   (f) If applicable, choose whether to open this application’s port. In most cases, opening a port is not necessary; only open a port if you know you require it. If selected, the port is opened on a shared IP address and, if applicable, your dedicated IP address.

   To open the port, click to select Open a port in the server firewall for the application.
   (g) In the URL field, enter the URL path (for example, /blog).

   **Note:** The first application added to a website is assigned to the root URL path (/).
   (h) Click the Save button. The application is installed and added to website’s list of applications.

   To add an existing application:
   (a) Click Add an application → Reuse an existing application. The Reuse an existing web app form appears.
   (b) Select the existing application on the website’s server to add to the website.
   (c) In the URL field, enter the URL path (for example, /blog).

   **Note:** The first application added to a website is assigned to the root URL path (/).
(d) Click the *Save* button. The application is added to the website’s list of applications.

10. Click the *Save* button. The website is created and added to the list of websites.

Changes to website entries can take up to two minutes to take effect. As soon as the changes take effect, you can access each application at the URLs you picked. If at first a new or modified website is not working as expected, please wait at least two minutes and try again.

### 7.2.2 Secure Sites (HTTPS)

You can configure any website record to use HTTPS (Hypertext Transfer Protocol Secure), an encrypted alternative to an ordinary HTTP connection.

**Note:** A website’s HTTPS setting is either on or off. Connections to the website are over the specified protocol only.

If you want your site to be served over HTTPS exclusively, then create a redirect from HTTP to HTTPS.

If you need your site to be available over both HTTP and HTTPS, then create two website records, one HTTP and the other HTTPS, and ensure that both sites are assigned to the same IP address.

An HTTPS website requires an SSL/TLS certificate. By default, HTTPS websites will use WebFaction’s shared certificate. Alternately, you can use our control panel to generate a free certificate using Let’s Encrypt or even bring your own, issued by another SSL certificate issuer.

If you use WebFaction’s shared certificate, most browsers will warn that your domain doesn’t match the certificate (though the connection will still be encrypted). To set up your website to use HTTPS with WebFaction’s certificate, see *Use a Certificate with a Website*.

If you want to automatically provision a a free SSL certificate, using Let’s Encrypt as your Certificate Authority, you can select that option when you add or edit an HTTPS enabled website, see *Use a Certificate with a Website*. Our panel will renew such a certificate when it is near its expiration date.

**Note:** Please note that it is currently not possible to issue Let’s Encrypt certificates for websites that contain a wildcard domain or a webfactional.com subdomain. If you have one in your https websites, you will need to remove it before issuing a certificate.

Finally, if you want to use your own certificate that matches your domain, then follow these steps:

1. Get a certificate through a certificate authority. Your domain registrar may provide this additional service or you can get a free certificate from Let’s Encrypt. Depending on how your provider issues certificates, then you may need to **generate a CSR** first.

2. **Add the certificate** with the WebFaction control panel.

3. **Use the certificate with a website**.

4. Whenever your certificate is soon to expire, **renew your certificate**.

### Generating a Certificate Signing Request

If you are requesting a security certificate, you may be asked to provide a Certificate Signing Request (CSR). To generate a CSR:

1. **Log in to the WebFaction control panel**.

2. Click *Domains / websites* → *SSL certificates*. The list of certificates appears.

3. Click *Generate a CSR*. The **CSR generator** form appears.
4. In the Country field, enter your country’s two-letter country code, such as US.

5. In the State field, enter your state or province, such as California.

6. In the Locality field, enter your city name, such as Los Angeles.

7. In the Organisation field, enter your name, such as your company’s legal name or your personal name.

8. In the Organisational unit field, enter your department, such as Marketing or IT.

9. In the Common name field, enter the domain or subdomain name for use with the certificate, such as example.com or www.example.com.

10. Optional In the Additional domains field, enter any additional domain names covered by the certificate, separated by spaces.

11. Click Generate CSR. A Generated CSR dialog appears.

12. Click Download CSR to download a zip file which contains both your CSR file and key file.

You now have a certificate signing request that you can give to your certificate provider.

**Warning:** Please do not delete the zip before you have installed the certificate on our panel. The zip file also contains the certificate’s key, that is needed in order to complete the installation later on.

### Add a Certificate

A certificate authority (CA) typically issues a certificate and some CAs may also issue an intermediate certificate or bundle. You can recognize your certificate and keys by their distinctive PEM format, which looks like this:

```plaintext
-----BEGIN CERTIFICATE-----
MIIFIjCCBAqgAwIBAgISA+B6sUMFu2K6oYwShXBLYjtMA0GCSqGSIb3DQEBCwUA
<more characters>
CIPIs5IBywAw6wGgCdxtOvTDJMVv==
-----END CERTIFICATE-----

-----BEGIN PRIVATE KEY-----
MIIFIjCCBAqgAwIBAgISA+B6sUMFu2K6oYwShXBLYjtMA0GCSqGSIb3DQEBCwUA
<more characters>
CIPIs5IBywAw6wGgCdxtOvTDJMVv==
-----END PRIVATE KEY-----
```

To add your certificate, private key, and, if applicable, intermediate certificate or bundle, follow the directions for the method you’d like to use: uploading files or copying and pasting the certificate and key text.

#### Upload files:

1. *Log in to the WebFaction control panel.*
2. Click **Domains / websites** → **SSL certificates**. The list of certificates appears.
3. Click **Add SSL certificate** → **Upload certificate**. The **Upload certificate** form appears.
4. In the **Name** field, enter a name for the certificate, such as the name of the website or domain you plan to use the certificate with.
5. In the **Certificate** section, click the **Choose File** button and select your certificate file.
6. In the **Private key** section, click the **Choose File** button and select your private key file.
7. If your CA provided you with an intermediate certificate or bundle, then, in the **Intermediates/bundle** section, click the **Choose File** button and select your intermediate certificate or bundle file.
8. Click the Save button.

Your certificate is added to the list of certificates. You can now use your certificate with a website.

**Copy and paste:**

1. Log in to the WebFaction control panel.
2. Click Domains / websites → SSL certificates. The list of certificates appears.
3. Click Add SSL certificate → Copy & paste certificate. The Create a new SSL certificate form appears.
4. In the Name field, enter a name for the certificate, such as the name of the website or domain you plan to use the certificate with.
5. In the Certificate field, paste the text of your certificate, including the BEGIN and END lines.
6. In the Private key field, paste the text of your private key, including the BEGIN and END lines.
7. If your CA provided you with an intermediate certificate or bundle, then, in the Intermediates/bundle field, paste the text of the intermediate certificate or bundle, including the BEGIN and END lines.
8. Click the Save button.

Your certificate is added to the list of certificates. You can now use your certificate with a website

**Use a Certificate with a Website**

Once you’ve added a certificate to your account, you can configure a website to use the certificate.

To set up a new website record to use a certificate, see Create a Website with the Control Panel.

To modify an existing website record to use a certificate, follow these steps:

1. Log in to the WebFaction control panel.
2. Click Domains / websites → Websites. The list of websites appears.
3. Click the name of the website that you want to modify to use a certificate. The website’s details appear.
4. In the Security section, click to select Encrypted website (https).

**Note:** A website’s HTTPS setting is either on or off. Connections to the website are over the specified protocol only.

If you want your site to be served over HTTPS exclusively, then create a redirect from HTTP to HTTPS.

If you need your site to be available over both HTTP and HTTPS, then create two website records, one HTTP and the other HTTPS, and ensure that both sites are assigned to the same IP address.

5. In the Choose a certificate menu, click to select a certificate.

   The Shared certificate is WebFaction’s shared certificate. If you use the shared certificate, most browsers will warn that your domain doesn’t match the certificate (though the connection will still be encrypted).

   The Let’s Encrypt certificate we will request a certificate from Let’s Encrypt on your behalf and install it on this site. Please note we can only provision a Let’s Encrypt certificate for a domain name once it is resolving to your WebFaction machine.

6. Click the Save button.

The website is now configured to use the certificate you selected.
Renew a Certificate

Periodically, your certificates will expire. To keep your sites secure and spare your visitors security error messages, you must renew your certificate with your certificate authority (CA) and then update your certificate with the control panel.

Note: Let’s Encrypt certificates issued by our control panel are renewed automatically. If your website’s certificate is managed by our control panel then you do not need to renew it.

Once you’ve received the updated certificate from your CA, follow these steps:

1. Log in to the WebFaction control panel.
2. Click Domains / websites → SSL certificates. The list of certificates appears.
3. Click the name of the certificate that you want to update. The certificate’s details appear.
4. In the Certificate field, paste the text of your certificate (replacing the existing text), including the \texttt{BEGIN} and \texttt{END} lines.
5. In the Private key field, paste the text of your private key (replacing the existing text), including the \texttt{BEGIN} and \texttt{END} lines.
6. If your CA provided you with an intermediate certificate or bundle, then, in the \texttt{Intermediates/bundle} field, paste the text of the intermediate certificate or bundle (replacing the existing text), including the \texttt{BEGIN} and \texttt{END} lines.
7. Click the Save button.

The certificate is now updated.

7.3 Reviewing Logs

You have complete access to your websites’ and applications’ logs in your home directory. You will find logs in your \texttt{$HOME/logs} directory, named according to the websites’ names in the control panel.

See also:

To learn more about logs, please see \textit{Accessing Logs}.

To generate statistics based on log files, see \textit{Webstats}.
CHAPTER
EIGHT

EXAMPLE WEBSITES

What Our Users Say
“Forgot how neat WebFaction’s hosting panel was. The concept of app plus domain equals site is nice.”
— wheelermichael

In this section of the user guide, you can see how Website records bring Applications and Domains together to create something accessible from a browser in a few clicks.

8.1 Creating a WebFaction Site in 4 Minutes

Follow these steps to create a new website, with a new subdomain and WordPress blog application, in a few minutes.

1. Log in to the WebFaction control panel.
2. Click Domains / websites → Websites. The list of websites appears.
3. Click the Add new website button. The Create a new website form appears.
4. In the Name field, enter myfirstsite.
5. Add a new domain.
   (a) In the Domains field, enter mynewsite.username.webfactional.com, where username is your WebFaction username.
   (b) Click Create mynewsite.username.webfactional.com.
6. Add a new application.
   (a) Click Add an application → Create a new application. The Create a new web app form appears.
   (b) In the Name field, enter myfirstapp.
   (c) In the App category menu, click to select WordPress.
   (d) Click the Save button. The application is installed and added to website’s list of applications.
7. Click the Save button. The website is created and added to the list of websites.
8. Wait two minutes while your changes go into effect. Now might be a good time to check your email or refill that cup of coffee.
### 8.2 Creating a Simple Website

While applications and website records allow for complex arrangements of domains and applications, the most common use-case is a collection of files—HTML, PHP, and images—connected to a single domain. To create a simple website:

1. Log in to the WebFaction control panel.
2. Click `Domains / websites` → `Websites`. The list of websites appears.
3. Click the `Add new website` button. The `Create a new website` form appears.
4. In the `Name` field, enter a name for the website.
5. For each domain name you want to use with the website, add it to the list of domains. In the `Domains` field, enter the domain name. Enter one or more domain names. If the domain has not yet been added to the control panel, click the `Create` link that appears at the bottom of the list of domains to add it.
   For example, you might enter a base domain (like `example.com`) and a subdomain (like `www.example.com`).
6. Add a new Static/CGI/PHP application.
   (a) Click `Add an application` → `Create a new application`. The `Create a new web app` form appears.
   (b) In the `Name` field, enter a name for the application.
   (c) In the `App category` menu, click to select `Static`.
   (d) In the `App type` menu, click to select `Static/CGI/PHP-X.Y`, substituting X.Y with the version of PHP that you wish to use.
   (e) Click the `Save` button. The application is installed and added to website’s list of applications.
7. Click the `Save` button. The website is created and added to the list of websites.
8. Upload files and images to the `Static/CGI/PHP` application’s directory, `~/webapps/application`, where `application` is the name of the `Static/CGI/PHP` application.

See also:

See [Connecting with FTP](#) for detailed directions on using FTP with your account.

After the changes have taken effect in about two minutes, the pages and images in the `Static/CGI/PHP` application can be reached at the domain selected.

### 8.3 A Sophisticated Website Configuration

While a WordPress blog or static site may be all you need, it’s possible to use domains, applications, and websites to reuse content across domains and segment content for different audiences. Consider this example for the hypothetical Widget Company.

Widget company can use a collection of domains and applications to target business and individual customers separately, without unnecessarily duplicating resources.

Widget Company has three domains:

- `widgetco.example`
- `widgetsforbiz.example`
- `widgetsforfun.example`
and four applications:

- **static_corp**, a Static/PHP/CGI application
- **django_biz**, a Django application
- **django_consumer**, a Django application
- **wordpress_blog**, a WordPress blog.

With three website entries in the control panel, Widget Company can reuse applications under each of the three domains:

```plaintext
widgetco.example
 /   -> static_corp
 /biz -> django_biz
 /blog -> wordpress_blog
 /consumer -> django_consumer

widgetsforbiz.example
 /   -> django_biz
 /blog -> wordpress_blog

widgetsforfun.example
 /   -> django_consumer
 /blog -> wordpress_blog
```
On WebFaction, you can use the control panel to create email addresses, access your mail in a variety of ways, and make use of advanced features, like auto-responders, forwarders, spam protection, and mailing lists.

9.1 Mailboxes and Addresses

The WebFaction mail system works with two basic units, email addresses and mailboxes. An email address is a public identifier where others can direct mail (for example, me@example.com). A mailbox is a place on the WebFaction mail servers where email received by one or more addresses is stored.

A mailbox has a single username and password and with them you can access all the mail received by any email address which points to that mailbox. While mailboxes generally correspond to one person, email addresses can point to, or target many mailboxes. In other words, email addresses can be thought of as aliases for mailboxes.

Note: Mail stored in a WebFaction mailbox counts toward disk usage limits.

For example, suppose there are two people using the email system, Jane and Sam. Jane has a mailbox called jane and Sam has a mailbox called sam. While sam@example.net and jane@example.net point to sam and jane, respectively, team@example.net points to both sam and jane, so that both of them receive email messages directed to their team.

Additionally, our mail system supports mail extensions, also known as “sub-addressing,” “tag addressing”, and “plus addressing.” This type of addressing allows you to insert into a valid email address the plus (+) symbol followed by arbitrary characters between the local part of the email address and the domain. For example, consider the email address joe@example.net: mail addressed to joe+extratext@example.net will be correctly routed to Joe’s mailbox, where Joe can use the text between the plus (+) symbol and the at (@) symbol to filter email.

9.1.1 Create an Email Mailbox with the Control Panel

To create an email mailbox with the control panel:

1. Log in to the control panel.
2. Click E-mails → Mailboxes. The list of mailboxes appears.
3. Click the Add new mailbox button. The Create a new mailbox form appears.
4. In the Mailbox name field, enter the mailbox name. Mailbox names must be unique. If the message Mailbox with this Name already exists appears, choose a different name for your mailbox.

5. In the Password field, enter a password for the mailbox.

See also:
See Strengthening Passwords for important information about choosing passwords.

6. In the Confirm password field, reenter the password for the mailbox.

7. Click to select a mail filtering mode.

   • To skip server-side spam filtering, choose None. Use this option to rely on your mail client’s junk mail filters only. Note that messages coming from a blacklisted or misconfigured mail server are rejected, and an error code is returned to the sending mail server. This error code is typically reported to the original sender as a bounced message.

   • To redirect junk mail to an IMAP folder, choose Redirect junk mail. A field appears. In the field, enter a folder name (such as spam).

     Note: Mail stored in IMAP folders is not accessible to POP clients. Don’t choose this option for mailboxes that are to be accessed primarily by POP clients.

   • To delete incoming junk mail, choose Discard junk email.

   • To use advanced mail filtering rules, choose Advanced. A field appears. Enter procmail rules into the field that appears.

     See also:
     Automatically Filtering Email

8. Click the Save button. The mailbox is created and added to the list.

9.1.2 Change an Email Mailbox Password

There are two ways to change an email mailbox password: a web form and the control panel.

**Change an Email Mailbox Password without the Control Panel**

You can use a form to change email mailbox passwords without logging into the WebFaction control panel. This method is the preferred way to allow your users to change their own mailbox password, because it does not require
giving them access to your account.

To change an email mailbox password with the form:

1. In a web browser, open https://my.webfaction.com/change_mail_password/create.
2. In the Mailbox name field, enter the mailbox name.
3. In the Current password field, enter the preexisting password.
4. In the New password field, enter the new password.

   See also:

   See Strengthening Passwords for important information about choosing passwords.

5. In the Confirm new password field, reenter the new password.
6. Click the Change password button. The password is changed.

You can use the new password to log in to the mailbox.

**Change an Email Mailbox Password with the Control Panel**

To change an email mailbox password with the control panel:

1. Log in to the control panel.
2. Click E-mails → Mailboxes. The list of mailboxes appears.
3. Click the name of the mailbox to change the password of.
4. In the Password section, click Change.
5. In the Password field, enter the new password.

   See also:

   See Strengthening Passwords for important information about choosing passwords.

6. In the Confirm password field, reenter the new password.
7. Click the Save button. The password is updated.

You can use the new password to log in to the mailbox.

**9.1.3 Create an Email Address with the Control Panel**

To create an email address with the control panel:

1. Log in to the WebFaction control panel.
2. Click E-mails → E-mail addresses. The Email list appears.
3. Click the Add new email button. The Create a new email address form appears.
4. In the Email fields, enter the local part and the domain name of the email address. For example, to create no-reply@example.com, enter no-reply and example.com. If the address is for a new domain, click Create in the list when it appears. The domain name will be automatically added to your list of domains.

You may also create catchall email addresses. To create a catchall email address, enter an asterisk in the local part of the email address. For example, *@example.com handles all mail addressed to the example.com domain. Catchall addresses are especially susceptible to spam. Use them sparingly.

5. To save incoming email to a mailbox, in the Save to local mailboxes section, click Yes. A field appears.

To save incoming email to an existing mailbox:
(a) In the field, enter the name of the mailbox until the mailbox appears in the list below.
(b) In the list, click the name of the mailbox.

To save incoming email to a new mailbox:
(a) In the field, enter the name of the mailbox. A Create link appears in the list below.
(b) In the list, click the Create link. Two password fields appear.
(c) In the Password field, enter a password.

See also:
See Strengthening Passwords for important information about choosing passwords.
(d) In the Confirm password field, reenter the password.
(e) Click the Save button. The mailbox is created.

To save incoming email to additional mailboxes, repeat the steps for a new or existing mailbox.

6. To forward incoming email to another address, in the Forward to other email addresses section, click Yes. A field appears. In the field, enter an email address.

To forward incoming email to additional addresses, enter more addresses.

See also:
Automatically Forwarding Email
7. To send an automatic response to incoming email, in the Send automatic response, click Yes. A form appears.

See also:

Automatically Responding to Email

(a) In the From fields, enter an outgoing email address and display name for the automatic response.
(b) In the Subject field, enter a subject line for the automatic response.
(c) In the Message field, enter a message body for the automatic response.
(d) (Optional) In the Reply To fields, enter an email address and display name for the automatic response’s Reply-To address.

8. To send incoming email to a program, in the Send to a program section, click Yes. A Path field appears. If you have plans on more than one server, a Server field appears.

If applicable, in the Server field, click to select a server. In the Path field, enter an absolute path to the program.

See also:

Sending Mail to a Script

9. Click the Save button. The address is created. A confirmation message appears.

You can receive mail at the new address.

9.2 Accessing Email

There are several ways to access your email stored on WebFaction’s mail servers. You can access your mail using an email client, such as a desktop or mobile application, or using our webmail access.

9.2.1 Configuring an Email Client

IMAP, POP, and SMTP

IMAP (Internet Mail Access Protocol) and POP (Post Office Protocol) are two ways of accessing mail servers. WebFaction supports both protocols, but IMAP is recommended. By default, IMAP leaves messages stored on the mail server, allowing you to access your mail from different computers and devices, while POP typically does not.

For POP configuration details, please see Configuring Other Mail Clients.

SMTP (Simple Mail Transfer Protocol) is used to send email messages.

WebFaction’s mail servers support clients that use IMAP or POP to access received mail. You can also access your mail on the web. The SMTP protocol is required for outgoing email.

To setup your client to access your WebFaction mailbox, choose your client from the list:

Configuring Mail Delivery and Transfer Agents

fetchmail

Note: WebFaction supports IMAP and POP mail protocols, but IMAP is recommended. By default, IMAP leaves messages stored on the mail server, allowing you to access your mail from different computers and devices, while
POP typically does not. If you still want to configure your email client to use POP, please see *Configuring Other Mail Clients* for details.

You can use fetchmail to retrieve mail from WebFaction’s mail servers. To configure fetchmail:

1. Open your `$HOME/.fetchmailrc` file in a text editor.
2. Add the following lines to the file:

   ```
   poll mail.webfaction.com with proto IMAP
   user mailbox_name there with password mysecret is username here
   ```

   where
   - `mailbox_name` is the name of the mailbox you configured in the WebFaction control panel,
   - `mysecret` is the password for the mailbox,
   - and `username` is your local (not WebFaction) username.

   **Note:** For more information about configuring fetchmail, please see the fetchmail documentation. It contains important information about how mail is handled after being retrieved from the server.

3. Save and close `.fetchmailrc`.

Now, if you enter `fetchmail` and press Enter, your mail is downloaded.

getmail

**Note:** WebFaction supports IMAP and POP mail protocols, but IMAP is recommended. By default, IMAP leaves messages stored on the mail server, allowing you to access your mail from different computers and devices, while POP typically does not. If you still want to configure your email client to use POP, please see *Configuring Other Mail Clients* for details.

You can use getmail to fetch mail from WebFaction’s mail servers. To configure getmail:

1. Create a `.getmail` directory in your HOME directory. Enter `mkdir -m 0700 $HOME/.getmail` and press Enter.
2. Open a new file, `$HOME/.getmail/getmailrc`, in a text editor.
3. Add the following lines to the file:

   ```
   [retriever]
   type = SimpleIMAPSSLRetriever
   server = mail.webfaction.com
   username = mailbox_name
   port = 993

   [destination]
   type = Maildir
   path = maildir_path
   ```

   where `mailbox_name` is the name of the mailbox you configured in the WebFaction control panel and `maildir_path` is the location where you would like the incoming messages to be stored.

   **Note:** For more information about configuring getmail, please see the getmail documentation. It contains important information about mail file formats and other settings.
4. Save and close `getmailrc`.

Now, if you enter `getmail` and press Enter, you are prompted for your password and your mail is downloaded to the specified destination.

**msmtp**

`msmtp` is a tool for sending mail. By default, it sends email messages provided by standard input. It can be used to send email with scripts or some mail clients, such as mutt.

To set up `msmtp`:

1. **Open an SSH session to your account.**
2. Download the `msmtp` source tar file. Enter `wget url`, where `url` is the URL for the source archive (see the `msmtp files` page for the latest version), and press Enter. The source file (typically of the form `msmtp-version.tar.bz2`) is created in the current directory.
3. Unpack the archive. Enter `tar -xf archive`, where `archive` is the name of the tar file containing the `msmtp` source, and press Enter. A directory containing the `msmtp` source is created in the current directory.
4. Switch to the `msmtp` source directory. Enter `cd source`, where `source` is the path to the directory containing the source files, and press Enter.
5. Configure the installation. Enter `./configure --prefix=$HOME` and press Enter.
7. Install `msmtp`. Enter `make install` and press Enter.
8. Create a `$HOME/.msmtprc` configuration file, if it does not already exist. Enter `touch $HOME/.msmtprc` and press Enter. The file is created.
9. Set user-only read and write permissions on the configuration file. Enter `chmod 600 $HOME/.msmtprc` and press Enter.
10. Open the `$HOME/.msmtprc` file in a text editor.
11. Add the following lines to the file:

```
account default
host smtp.webfaction.com
port 587
from email_address
auth on
user mailbox_name
password mysecret
tls on
tls_trust_file certificate_file
```

where `email_address` is the email address you configured in the WebFaction control panel, `mailbox_name` is the name of a WebFaction mailbox, `mysecret` is the mailbox password, and `certificate_file` is the path to your certificate authority file. Alternatively, you may substitute the `tls_trust_file` setting with `tls_certcheck off` to disable the verification of certificates.

12. Save and close the file.

You have configured `msmtp`. To verify your settings work, enter `msmtp -S` and press Enter.
Configuring Mac OS X Mail Clients

Mail for Mac OS 10.9 (Mavericks)

Note: WebFaction supports IMAP and POP mail protocols, but IMAP is recommended. By default, IMAP leaves messages stored on the mail server, allowing you to access your mail from different computers and devices, while POP typically does not. If you still want to configure your email client to use POP, please see Configuring Other Mail Clients for details.

To set up a WebFaction-hosted mailbox with Mail for Mac OS 10.9 (Mavericks):

1. Start the Mail application.
2. Click Mail → Preferences. ... Mail’s preferences window appears.
3. Click Accounts. The list of mail accounts appears.
4. Click the + (plus) button. The Choose mail account to add dialog appears:
5. Click to select *Add Other Mail Account*.

6. Click *Continue*. The *Add a mail account* dialog appears:
7. In the **Full Name** field, enter your name as you would like it to appear to recipients of your messages.

8. In the **Email Address** field, enter your email address.

9. In the **Password** field, enter your mailbox password.

10. Click the **Create** button. A message, **Account must be manually configured**, appears.

11. Click the **Next** button. The **Incoming Mail Server Info** dialog appears.
12. In the Account Type menu, click to select IMAP.

13. In the Mail Server field, enter mail.webfaction.com.

14. In the User Name field, enter your mailbox name.

15. In the Password field, enter your mailbox password.

16. Click the Next button. The Outgoing Mail Server Info dialog appears:
17. In the **SMTP Server** field, enter `smtp.webfaction.com`.

18. In the **User Name** field, enter your mailbox name.

19. In the **Password** field, enter your mailbox password.

20. Click the **Create** button. The mailbox is added to Mail’s list of accounts.

21. In the **Outgoing Mail Server (SMTP)** list, click to select *Edit SMTP Server List...*. The list of SMTP servers appears.

22. In the list, click to select `smtp.webfaction.com`.

23. Click the **Advanced** tab.

24. Click to select *Use Secure Sockets Layer (SSL)*.

25. In the **Authentication** menu, click to select *Password*.

26. Click **OK**.
The account is now configured.

Mail for Mac OS 10.11 (El Capitan)

Note: WebFaction supports IMAP and POP mail protocols, but IMAP is recommended. By default, IMAP leaves messages stored on the mail server, allowing you to access your mail from different computers and devices, while POP typically does not. If you still want to configure your email client to use POP, please see Configuring Other Mail Clients for details.

To set up a WebFaction-hosted mailbox with Mail for Mac OS 10.9 (El Capitan):

1. Start the Mail application.
2. Click Mail → Preferences…. Mail’s preferences window appears.
3. Click Accounts. The list of mail accounts appears.
4. Click the + (plus) button. The Choose a Mail account provider dialog appears.
5. Click to select Add Other Mail Account…
6. Click Continue.
7. In the Name field, enter your name as you would like it to appear to recipients of your messages.
8. In the Email Address field, enter your email address.
9. In the Password field, enter your mailbox password.
10. Click the Sign In button. A message, Unable to verify account name or password, and additional fields appear.
11. In the User Name field, enter your mailbox name.
12. In the Account Type menu, click to select IMAP.
13. In the Incoming Mail Server field, enter mail.webfaction.com.
15. Click the Sign In button. A Select the apps you want to use with this account menu appears.
16. Click to select Mail.
17. Click the Done button. An Account Information window appears.
18. In the Outgoing Mail Server (SMTP) menu, click to select Edit SMTP Server List. An Account Information window appears.
19. Click the Advanced tab. Additional options appear.
20. In the **Port** field, enter **587**.

21. Click to select **Use SSL**.

22. In the **Authentication** menu, click to select **Password**.

23. In the **User Name** field, enter your mailbox name.

24. Click the **OK** button.

The account is now configured.

**Mozilla Thunderbird (Mac OS X)**

**Note:** WebFaction supports IMAP and POP mail protocols, but IMAP is recommended. By default, IMAP leaves messages stored on the mail server, allowing you to access your mail from different computers and devices, while
POP typically does not. If you still want to configure your email client to use POP, please see Configuring Other Mail Clients for details.

To add an email address and mailbox to Mozilla Thunderbird:

1. Start the Thunderbird application.
2. Click Tools → Account Settings. The account settings dialog appears.
3. Click Account Actions → Add Mail Account. . . A prompt appears:

4. In the Your name field, enter your name as you would like it to appear for recipients of your messages.
5. In the Email address field, enter your email address.
6. In the Password field, enter your mailbox password.
7. Click the Continue button. Thunderbird attempts to automatically determine the mail server settings, and fails. A table of settings appears:
8. In the table’s *Incoming* row, configure the incoming mail (IMAP) server.
   (a) In the *Server hostname* field, enter `mail.webfaction.com`.
   (b) In the *Port* field, enter `993`.
   (c) In the *SSL* menu, click to select *SSL/TLS*.
   (d) In the *Authentication* menu, click to select *Autodetect*.

9. In the table’s *Outgoing* row, configure the outgoing (SMTP) server.
   (a) In the *Server hostname* field, enter `smtp.webfaction.com`.
   (b) In the *Port* field, enter `465`.
   (c) In the *SSL* menu, click to select *SSL/TLS*.
   (d) In the *Authentication* menu, click to select *Autodetect*.

10. In the *Username* field, enter your mailbox name.

11. Click the *Re-test* button.

12. Click the *Done* button.

The account is added to Thunderbird.

**Configuring Mobile Mail Clients**

**Mail app for Android 4.3 (Jelly Bean)**

**Note:** WebFaction supports IMAP and POP mail protocols, but IMAP is recommended. By default, IMAP leaves messages stored on the mail server, allowing you to access your mail from different computers and devices, while POP typically does not. If you still want to configure your email client to use POP, please see *Configuring Other Mail Clients* for details.

To set up a WebFaction-hosted mailbox with Android 4.3 (Jelly Bean):

1. Launch the *Settings* app.
2. Touch + Add Account. A list of possible account types to add appears.

3. Touch Email. Account setup appears.

4. In the Email address field, enter your email address.

5. In the Password field, enter your mailbox password.


7. Touch IMAP. Incoming server settings appears.

8. In the Username field, enter your mailbox name.

9. In the Password field, enter your mailbox password.

10. In the IMAP server field, enter mail.webfaction.com.

11. In the Security type menu, touch SSL/TLS.

12. In the Port field, enter 993.


15. In the Security type menu, touch SSL/TLS.

16. In the Port field, enter 465.

17. Touch to select Require sign-in.

18. In the Username field, enter your mailbox name.

19. In the Password field, enter your mailbox password.


21. Touch Next. Your account is set up appears.

22. In the Your name field, enter your name as you want it to appear to recipients.

23. Touch Next. Your account is added.

**Mail app for Android 4.4 (KitKat)**

**Note:** WebFaction supports IMAP and POP mail protocols, but IMAP is recommended. By default, IMAP leaves messages stored on the mail server, allowing you to access your mail from different computers and devices, while POP typically does not. If you still want to configure your email client to use POP, please see *Configuring Other Mail Clients* for details.

To set up a WebFaction-hosted mailbox with Android 4.4 (KitKat):

1. Launch the Settings app.

2. Touch + Add Account. A list of possible account types to add appears.

3. Touch IMAP. Account setup appears.
4. In the *Email address* field, enter your email address.

5. In the *Password* field, enter your mailbox password.


8. In the Username field, enter your mailbox name.

9. In the Password field, enter your mailbox password.

10. In the IMAP server field, enter mail.webfaction.com.

11. In the Security type menu, touch SSL/TLS.

12. In the Port field, enter 993.


15. In the **Security type** menu, touch **SSL/TLS**.

16. In the **Port** field, enter `465`.

17. Touch to select **Require sign-in**.

18. In the **Username** field, enter your mailbox name.

19. In the **Password** field, enter your mailbox password.


21. Touch Next. Your account is set up appears.
22. In the *Your name* field, enter your name as you want it to appear to recipients.

23. Touch *Next*.

The email account is added. You can send and receive the account’s mail with the *Email* app.

**Mail app for Android 5.0 and 5.1 (Lollipop)**

**Note:** WebFaction supports IMAP and POP mail protocols, but IMAP is recommended. By default, IMAP leaves messages stored on the mail server, allowing you to access your mail from different computers and devices, while POP typically does not. If you still want to configure your email client to use POP, please see *Configuring Other Mail Clients* for details.

To set up a WebFaction-hosted mailbox with Android 5.0 and 5.1 (Lollipop):
1. Launch the **Settings** app.
2. Touch **Accounts**.
3. Touch + **Add Account**. A list of possible account types to add appears.
4. Touch **Personal (IMAP)**. Add your email address appears.
5. In the Enter your email address field, enter your email address.
6. Tap **Next**.
7. In the Password field, enter your mailbox password.
8. Tap Next. **Incoming server settings** appears.
9. In the Username field, enter your mailbox name.
10. In the Server field, enter mail.webfaction.com.
11. In the Port field, enter 993.
12. In the Security type menu, touch SSL/TLS.
13. Tap **Next**. **Outgoing server settings** appears.
15. In the Port field, enter 465.
16. In the Security type menu, touch SSL/TLS.
17. Touch to select Require signin.
18. In the Username field, enter your mailbox name.
19. In the Password field, enter your mailbox password.
20. Touch Next. **Account options** appears.
21. Touch Next. **Your account is set up** appears.
22. In the Your name field, enter your name as you want it to appear to recipients.
23. Touch Next.

The email account is added. You can send and receive the account’s mail with the **Gmail** app.

**iOS 7 (iPhone, iPad, and iPod Touch)**

**Note**: WebFaction supports IMAP and POP mail protocols, but IMAP is recommended. By default, IMAP leaves messages stored on the mail server, allowing you to access your mail from different computers and devices, while POP typically does not. If you still want to configure your email client to use POP, please see Configuring Other Mail Clients for details.

To add an email address and mailbox to an iPhone, iPad, or iPod Touch running iOS 7:
1. From the home screen, tap the **Settings** app.
2. Tap Mail, Contacts, Calendars.
3. Tap **Add Account**. A list of mail providers appears.
4. Tap **Other**.
5. Tap **Add Mail Account**.
6. In the Name field, enter your name as you would like it to appear to others.

7. In the Email field, enter your email address.

8. In the Password field, enter your mailbox password.

9. Tap Next.

10. Complete the Incoming Mail Server settings:
    (a) In the Host Name field, enter mail.webfaction.com.
    (b) In the User Name field, enter your mailbox name.
    (c) In the Password field, enter your mailbox password.

11. Complete the Outgoing Mail Server settings:
    (a) In the Host Name field, enter smtp.webfaction.com.
    (b) In the User Name field, enter your mailbox name.
    (c) In the Password field, enter your mailbox password.

12. Tap Next. The account settings are verified.

13. Tap Save.

The account is added to the device.

**iOS 8 (iPhone, iPad, and iPod Touch)**

**Note:** WebFaction supports IMAP and POP mail protocols, but IMAP is recommended. By default, IMAP leaves messages stored on the mail server, allowing you to access your mail from different computers and devices, while POP typically does not. If you still want to configure your email client to use POP, please see Configuring Other Mail Clients for details.

To add an email address and mailbox to an iPhone, iPad, or iPod Touch running iOS 8:

1. From the home screen, tap the Settings app.
2. Tap Mail, Contacts, Calendars.
3. Tap Add Account. A list of mail providers appears.
4. Tap Other.
5. Tap Add Mail Account.
6. In the Name field, enter your name as you would like it to appear to others.
7. In the Email field, enter your email address.
8. In the Password field, enter your mailbox password.
9. Tap Next.
10. Complete the Incoming Mail Server settings:
    (a) In the Host Name field, enter mail.webfaction.com.
    (b) In the User Name field, enter your mailbox name.
    (c) In the Password field, enter your mailbox password.
11. Complete the Outgoing Mail Server settings:
(a) In the Host Name field, enter smtp.webfaction.com.
(b) In the User Name field, enter your mailbox name.
(c) In the Password field, enter your mailbox password.

12. Tap Next. The account settings are verified.
13. Tap Save.

The account is added to the device.

**iOS 9 (iPhone, iPad, and iPod Touch)**

**Note:** WebFaction supports IMAP and POP mail protocols, but IMAP is recommended. By default, IMAP leaves messages stored on the mail server, allowing you to access your mail from different computers and devices, while POP typically does not. If you still want to configure your email client to use POP, please see Configuring Other Mail Clients for details.

To add an email address and mailbox to an iPhone, iPad, or iPod Touch running iOS 9:

1. From the home screen, tap the Settings app.
2. Tap Mail, Contacts, Calendars.
3. Tap Add Account. A list of mail providers appears.
4. Tap Other.
5. Tap Add Mail Account.
6. In the Name field, enter your name as you would like it to appear to others.
7. In the Email field, enter your email address.
8. In the Password field, enter your mailbox password.
9. Tap Next.
10. Complete the Incoming Mail Server settings:
   (a) In the Host Name field, enter mail.webfaction.com.
   (b) In the User Name field, enter your mailbox name.
   (c) In the Password field, enter your mailbox password.
11. Complete the Outgoing Mail Server settings:
   (a) In the Host Name field, enter smtp.webfaction.com.
   (b) In the User Name field, enter your mailbox name.
   (c) In the Password field, enter your mailbox password.
12. Tap Next. The account settings are verified.
13. Tap Save.

The account is added to the device.
Configuring Web Mail Clients

Gmail

To add a WebFaction-hosted mailbox and email address to Gmail:

1. Log in to Gmail.

2. Click the settings gear button. A menu appears:

3. Click **Settings**.

4. Click **Accounts and Import**.

5. Click **Add a mail account you own**. A pop up window appears:

6. In the *Email address* field, enter your email address.

7. Click the *Next Step* button. Several mail configuration fields appear:
8. In the **Username** field, enter your mailbox name.

9. In the **Password** field, enter your password.

10. In the **POP Server** field, enter `mail.webfaction.com`.

11. In the **Port** menu, click to select 995.

12. Click to select *Leave a copy of retrieved message on the server.*

13. Click to select *Always use a secure connection (SSL) when retrieving mail.*

14. Click the **Add Account** button.

15. Click to select *Yes, I want to be able to send mail as demo@demo.webfactional.com.*

16. Click the **Next Step** button.

17. In the **Name** field, enter your name as it you want it to appear to message recipients.

18. Click the **Next Step** button. Several mail configuration fields appear:
19. In the **SMTP Server** field, enter `smtp.webfaction.com`.

20. In the **Port** menu, click to select **587**.

21. In the **Username** field, enter your mailbox name.

22. In the **Password** field, enter your mailbox password.

23. Click to select **Secured connection using TLS (recommended)**.

24. Click the **Add Account** button. A **Confirm verification and add your email address** message appears.

25. Wait for an email message, **Gmail Confirmation**, to arrive in your inbox.

26. When the email message arrives, click the confirmation link in the body of the message. Your mailbox is added to Gmail and you can send mail from the address.

**Outlook.com**

To add a WebFaction-hosted email address and mailbox to your Outlook.com account:

1. Log in to your Outlook.com account.

2. Click the settings gear. A menu appears:
3. Click *More mail settings*. The *Options* page appears.

4. Click *Your email accounts*. The *Your email accounts* page appears.

5. Click the *Add a send-and-receive account* button. The *Add a send-and-receive account* form appears:
Add a send-and-receive account

You can use Outlook.com to send and receive email from other accounts. To get started, enter your name, email address, and password below. The name you enter will be used when you send an email from this account.

Name:

**Demo WebFactioneer**

Email address:

**demo@demo.webfactional.com**

Password:

************

Advanced options

Privacy

6. In the Name field, enter your name as you’d like it to appear to message recipients.
7. In the Email address field, enter your WebFaction-hosted email address.
8. In the Password field, enter your mailbox password.
9. Click the Next button. The Account info form appears.
10. In the Name field, enter your name as you’d like it to appear to message recipients.
11. In the Email address field, enter your WebFaction-hosted email address.
12. Complete the Incoming (POP3) server information section:
   (a) In the Server address field, enter `mail.webfaction.com`.
   (b) In the Port menu, click to select 995.
   (c) Click to select Requires a secure connection (SSL).
   (d) In the Username field, enter your mailbox name.
   (e) In the Password field, enter your mailbox password.
13. Complete the Outgoing (SMTP) server information section:
   (a) Click to select Send email using your provider’s server.
   (b) In the Server address field, enter `smtp.webfaction.com`.
   (c) In the Port menu, click to select 465.
   (d) Click to select Requires a secure connection (SSL/TLS).
   (e) Click to select Use the same username and password to send and receive mail.
14. Click the Next button. The Your email accounts page appears.

15. Choose where to save incoming mail from your mailbox.

   - To save incoming mail to a new folder, click to select A new folder called, then enter a folder name in the field adjacent.
   - To save incoming mail to an existing folder, click to select An existing folder, then click to select a folder name in the menu adjacent. For example, you can choose your Outlook.com inbox as the destination folder.

16. Click the Save button. A confirmation page appears.

Your email address and mailbox is added to your Outlook.com account.

**Configuring Windows Mail Clients**

**Microsoft Outlook 2007**

*Note:* WebFaction supports IMAP and POP mail protocols, but IMAP is recommended. By default, IMAP leaves messages stored on the mail server, allowing you to access your mail from different computers and devices, while POP typically does not. If you still want to configure your email client to use POP, please see *Configuring Other Mail Clients* for details.

To add an email address and mailbox account to Microsoft Outlook 2007:

1. Click Tools → Account Settings:
2. Click the Email tab. The Account settings dialog appears:
3. Click the New... button. The Add New E-mail Account wizard begins:
4. Click to select *Manually configure server settings or additional server types*.

5. Click *Next*. The *Choose E-mail Service* dialog appears:
6. Click to select *Internet E-mail*.

7. Click the *Next* button. The *Internet E-mail Settings* dialog appears:
8. In the *Your Name* field, enter your name.

9. In the *E-mail Address* field, enter your email address.

10. In the *Account Type* menu, click to select *IMAP*.

11. In the *Incoming mail server* field, enter *mail.webfaction.com*.

12. In the *Outgoing mail server (SMTP)* field, enter *smtp.webfaction.com*.

13. In the *User Name* field, enter your mailbox name.

14. In the *Password* field, enter your mailbox password.

15. Click the *More Settings*... button. The *Internet E-mail Settings* dialog appears.

16. Click the *Outgoing Server* tab.

17. Click to select *My outgoing server (SMTP) requires authentication*.

18. Click to select *Use same settings as my incoming mail server*.

19. Click the *Advanced* tab:
20. In the **Incoming server (IMAP)** field, enter 993.

21. Beneath **Incoming server (IMAP)**, click to select SSL from the **Use the following type of encrypted connection** menu.

22. In the **Outgoing server (SMTP)** field, enter 465.

23. Beneath **Outgoing server (SMTP)**, click to select SSL from the **Use the following type of encrypted connection** menu.

24. Click the **OK** button.

25. Click the **Next** button.

26. Click the **Finish** button.

27. Click the **Close** button.

28. Click the **OK** button.

The email address and mailbox is added to Microsoft Outlook 2007.
Microsoft Outlook 2010

**Note:** WebFaction supports IMAP and POP mail protocols, but IMAP is recommended. By default, IMAP leaves messages stored on the mail server, allowing you to access your mail from different computers and devices, while POP typically does not. If you still want to configure your email client to use POP, please see *Configuring Other Mail Clients* for details.

1. Start the Outlook 2010 application.

2. Click *File* → *Info* → *Account Settings* → *Account Settings*… The *Account Settings* window appears.

3. Click the *E-mail* tab. The list of mail accounts appears.
4. Click the New... button. The Add New Account wizard appears.

5. Click to select Manually configure server settings or additional server settings or additional server types.
6. Click the Next button.

7. Click to select Internet E-mail.
8. Click the Next button.

9. In the Your Name field, enter your name as you’d like it to appear to recipients.

10. In the E-mail Address field, enter your email address.

11. In the Account Type field, click to select IMAP.

12. In the Incoming mail server field, enter mail.webfaction.com.

13. In the Outgoing mail server (SMTP) field, enter smtp.webfaction.com.

14. In the User Name field, enter your mailbox name.

15. In the Password field, enter your mailbox password.

16. Click the More Settings... button. The Internet E-Mail Settings window appears.

17. Click the Outgoing Server tab.
18. Click to select *My outgoing server (SMTP) requires authentication.*
19. Click to select *Use same settings as my incoming mail server.*
20. Click the *Advanced* tab.
21. In the *Incoming server (IMAP)* field, enter 993.

22. Under *Incoming server (IMAP)*, in the *Use the following type of encrypted connection* menu, click to select SSL.

23. In the *Outgoing server (SMTP)* field, enter 465.

24. Under *Outgoing server (SMTP)*, in the *Use the following type of encrypted connection* menu, click to select SSL.

25. Click the *OK* button.
26. Click the Next button.
27. Click the Finish button.
28. Click the Close button.
29. Click the OK button.

The account is added to Outlook.

Mozilla Thunderbird (Windows)

**Note:** WebFaction supports IMAP and POP mail protocols, but IMAP is recommended. By default, IMAP leaves messages stored on the mail server, allowing you to access your mail from different computers and devices, while POP typically does not. If you still want to configure your email client to use POP, please see *Configuring Other Mail Clients* for details.

To add an email address and mailbox account to Mozilla Thunderbird:

1. Start the Thunderbird application.

2. Click *Thunderbird menu → Options… → Account Settings…*.

   ![Thunderbird menu settings](image)

   The Account Settings window appears.

3. Click *Account Actions → Add Mail Account…*.
The Mail Account Setup window appears.

4. In the Your name field, enter your name as you would like it to appear for recipients of your messages.

5. In the Email address field, enter your email address.

6. In the Password field, enter your mailbox password.

7. Click the Continue button. Thunderbird attempts to automatically determine the mail server settings, and fails. A table of settings appears:

8. In the table’s Incoming row, configure the incoming mail (IMAP) server.
   (a) In the Server hostname field, enter `mail.webfaction.com`.
   (b) In the Port field, enter `993`.
   (c) In the SSL menu, click to select SSL/TLS.
   (d) In the Authentication menu, click to select Autodetect.

9. In the table’s Outgoing row, configure the outgoing (SMTP) server.
(a) In the Server hostname field, enter smtp.webfaction.com.
(b) In the Port field, enter 465.
(c) In the SSL menu, click to select SSL/TLS.
(d) In the Authentication menu, click to select Autodetect.

10. In the Username field, enter your mailbox name.
11. Click the Re-test button.
12. Click the Done button.

The account is added to Thunderbird.

Windows Live Mail

**Note:** WebFaction supports IMAP and POP mail protocols, but IMAP is recommended. By default, IMAP leaves messages stored on the mail server, allowing you to access your mail from different computers and devices, while POP typically does not. If you still want to configure your email client to use POP, please see Configuring Other Mail Clients for details.

To add an address and mailbox to Windows Live Mail:

1. Start the Windows Live Mail application.
2. Click the Windows Live Mail menu button. The menu appears:

3. Click Options -> Email accounts... The Accounts dialog appears:
4. Click the Add button. The Select Account Type dialog appears:
5. Click to select *Email Account*.

6. Click the *Next* button. The *Add your email accounts* dialog appears.
7. In the Email address field, enter your email address.

8. In the Password field, enter your password.

9. In the Display name for your sent messages field, enter your name as you would like it to appear to message recipients.

10. Click to select Manually configure server settings.

11. Click the Next button. The Configure server settings dialog appears:
12. Configure the *Incoming server* settings.
   
   (a) In the *Server type* menu, click to select *IMAP*.
   
   (b) In the *Server address* field, enter *mail.webfaction.com*.
   
   (c) In the *Port* field, enter *993*.
   
   (d) Click to select *Requires a secure connection (SSL)*.
   
   (e) In the *Authenticate using* menu, click to select *Clear text*.
   
   (f) In the *Logon user name*, enter your mailbox name.

13. Configure the *Outgoing server* settings.

   (a) In the *Server address* field, enter *smtp.webfaction.com*.
   
   (b) In the *Port* field, enter *465*.
   
   (c) Click to select *Requires a secure connection (SSL)*.
   
   (d) Click to select *Requires authentication*.

14. Click the *Next* button.

15. Click the *Finish* button.
16. Click the *Close* button.

Your address and mailbox is added to Windows Live Mail.

**Windows Mail (Windows Vista)**

*Note:* WebFaction supports IMAP and POP mail protocols, but IMAP is recommended. By default, IMAP leaves messages stored on the mail server, allowing you to access your mail from different computers and devices, while POP typically does not. If you still want to configure your email client to use POP, please see *Configuring Other Mail Clients* for details.

To add an email address and mailbox account to Windows Mail:

1. Start the Windows Mail application.
2. Click *Tools → Accounts:*

   ![Internet Accounts list](image)

   The *Internet Accounts* list appears:
3. Click the *Add* button. The account wizard appears:
4. Click to select E-mail Account.

5. Click the Next button. The Your Name dialog appears:
6. In the *Display name* field, enter your name.

7. Click the *Next* button. The *Internet E-mail Address* dialog appears.
8. In the *E-mail address* field, enter your email address.

9. Click the *Next* button. The *Set up e-mail servers* dialog appears:
10. In the *Incoming e-mail server type* menu, click to select **IMAP**.

11. In the *Incoming mail (POP3 or IMAP) server* field, enter `mail.webfaction.com`.

12. In the *Outgoing e-mail (SMTP) server name* field, enter `smtp.webfaction.com`.

13. Click to select *Outgoing server requires authentication*.

14. Click the *Next* button. The *Internet Mail Logon* dialog appears.
15. In the *E-mail username* field, enter your mailbox name.
16. In the *Password* field, enter your mailbox password.
17. Click the *Next* button.
18. Click to select *Do not download my email and folders at this time*.
19. Click the *Finish* button.
20. Click to select *mail.webfaction.com account*.
21. Click the *Properties* button.
22. Click the *Advanced* tab. The *Advanced* tab appears:
23. In the *Outgoing mail (SMTP)* field, enter **465**.

24. Beneath the *Outgoing mail (SMTP)* field, click to select *This server requires a secure connection (SSL)*.

25. In the *Incoming mail (IMAP)* field, enter **993**.

26. Beneath the *Incoming mail (IMAP)* field, click to select *This server requires a secure connection (SSL)*.

27. Click the *OK* button.

28. Click the *Close* button.

The email address and mailbox are added to Windows Mail.

**Windows 8 Mail**

To add an email address and mailbox account to Windows 8:

1. On the Start screen, click *Mail*.
2. Move the cursor to the lower-right corner of the screen, then click *Settings*.
3. Click *Accounts*.
4. Click *Add an account*. 

5. Click Other account.
6. Click to select IMAP.
7. Click the Connect button. Add your Other account appears.
8. Click Show more details.
9. In the Email address field, enter your WebFaction-hosted email address.
10. In the Username field, enter your mailbox name.
11. In the Password field, enter your mailbox password.
12. In the Incoming (IMAP) email server field, enter mail.webfaction.com.
13. In the adjacent Port field, enter 993.
14. Click to select Incoming server requires SSL.
15. In the Outgoing (SMTP) email server field, enter smtp.webfaction.com.
16. In the adjacent Port field, enter 465.
17. Click to select Outgoing server requires SSL.
18. Click to select Outgoing server requires authentication.
19. Click to select Use the same username and password to send and receive mail.
20. Click the Connect button.

Your account is added.

Configuring Other Mail Clients

While we do not provide directions for other clients, we do offer the these configuration details, which should get you started with your mail client of choice.

IMAP, POP, and SMTP

IMAP (Internet Mail Access Protocol) and POP (Post Office Protocol) are two ways of retrieving mail from a server. WebFaction supports both protocols, but IMAP is recommended. By default, IMAP leaves messages stored on the mail server, which allows you to access your mail from different computers and devices, while POP typically does not.

SMTP (Simple Mail Transfer Protocol) is used to send email messages.

Our mail servers require authentication, including SMTP.

Account Settings:

- Username — mailbox name as it appears in the WebFaction control panel
- Password — mailbox password
- “From” Email Address — an email address registered in the WebFaction control panel which includes the mailbox used to authenticate with the SMTP server as a target

Servers:

- POP (for receiving) — mail.webfaction.com
- IMAP (for receiving) — mail.webfaction.com
• SMTP (for sending) — smtp.webfaction.com

Ports:

<table>
<thead>
<tr>
<th></th>
<th>Standard</th>
<th>Secure (SSL)</th>
<th>Secure (TLS)</th>
</tr>
</thead>
<tbody>
<tr>
<td>POP</td>
<td>110</td>
<td>995</td>
<td></td>
</tr>
<tr>
<td>IMAP</td>
<td>143</td>
<td>993</td>
<td></td>
</tr>
<tr>
<td>SMTP</td>
<td>25</td>
<td>465</td>
<td>587</td>
</tr>
</tbody>
</table>

### 9.2.2 Webmail

You can access your email at any time using Roundcube, a webmail interface. Roundcube is available at [https://webmail.webfaction.com/](https://webmail.webfaction.com/). Roundcube requires no configuration to read email: log in with your mailbox name and password to get started.

To send mail with the webmail interface, you must assign an outgoing email address.

To set your outgoing address with Roundcube:

1. Log in to Roundcube.

   **Note:** If it’s your first time logging in to Roundcube, a *Please complete your sender identity* dialog appears. If the dialog appears, then follow these steps:
   
   (a) In the *Display Name* field, enter your name as you would like it to appear to mail recipients.
   
   (b) In the *Email* field, enter an address you want to send mail from (for example, demo@example.com).
   
   (c) Click the *Save* button.

   The email address is added to the *From* menu when composing messages with Roundcube. If you want to add more outgoing email addresses, then continue to the next step.

2. Click *Settings*.
3. Click *Identities*.
4. At the bottom of the *Identities* column, click the + (plus) button. The *New identity* form appears.
5. In the *Display Name* field, enter your name as you would like it to appear to mail recipients.
6. In the *Email* field, enter an address you want to send mail from (for example, demo@example.com).
7. Click the *Save* button.

   The email address is added to the *From* menu when composing messages with Roundcube.

### 9.2.3 Using Roundcube on a Mobile Device

By selecting a difference appearance, Roundcube can be easier to use with some mobile touchscreen devices. To change Roundcube’s appearance:

1. Log in to Roundcube.
2. Click *Settings*. The menu of settings sections appears.
3. In the *Section* menu, click *User Interface*. A settings form appears.
4. In the *Interface skin* menu, select w21_mobile.
5. Click the *Save* button.
9.3 Managing Email Automatically

WebFaction offers you several ways of managing email programmatically, with automatic forwarding and responders, spam protection, and integration with scripts or applications.

9.3.1 Automatically Filtering Email

You can enable server-side filtering rules to help you manage mail. Unlike filtering rules set in your email client, server-side filters are applied to all incoming mail, regardless of which email client you use.

Note: Mail stored in IMAP folders is not accessible to POP clients. Server-side mail filters are not recommended for mailboxes primarily accessed by POP clients.

To add a mail filter:

1. Log in to the control panel.
2. Click E-mails → Mailboxes. The list of mailboxes appears.
3. Click the mailbox you want to add mail rules to. The mailbox’s details appear.
4. Click to select Advanced. A text field appears.
5. In the text field, enter your filtering rules.

Note: Rules are processed in order. Enter the most important rules first.

See also:

• Filtering by Sender
• Filtering by Subject
• Filtering Spam
• procmail tips and recipes

6. Click the Save button.

Filtering by Sender

To filter email based on the sender, use this mail rule:

```c
:0:
  * ^From:<regex>
  ./<folder>/
```

where:

• `<regex>` is a regular expression. For example, to filter on a sender’s domain, use a regular expression like `.*@example.com`
• `<folder>` is the name of the destination folder.
Filtering by Subject

To filter email based on the contents of the subject line, use this mail rule:

```
:^Subject:<regex>.<folder>/
```

where:

- `<regex>` is a regular expression. For example, to filter on a word appearing in the subject line, use a regular expression like `.*\sword.*`.
- `<folder>` is the name of the destination folder.

Filtering Spam

You can filter incoming mail based on its spam score. To filter mail which has a spam score greater than or equal to 3, use this mail rule:

```
:^X-Spam-Level: \*\*\*<spam>/
```

where `<spam>` is the name of the spam destination folder (for example, `spam` or `junk`).

You can filter on higher spam levels by adding more asterisks to the rule (don’t forget to escape the asterisk with a backslash, like this: `\*`).

9.3.2 Automatically Forwarding Email

Any email address set up in the WebFaction control panel can be configured to automatically forward email to another email address (or several email addresses).

**Note:** Obvious spam email will not be automatically forwarded. If you wish to retain email which is not forwarded to other addresses, be sure to save incoming email to a mailbox.

**See also:**

Mail forwarded to a Google Gmail account will not appear in the Gmail inbox if the sender is the same Gmail account. Such incoming messages are ignored. Only the original, sent message will appear in Sent Mail.

To automatically forward email:

1. Log in to the WebFaction control panel.
2. Click E-mails → E-mail addresses. The list of addresses appears.
3. Click on the email address to automatically forward email.
4. In the Forward to other email addressees section, click Yes. A field appears. In the field, enter the destination address. To forward to additional addresses, enter more addresses in the field.
5. Save your changes. Click the Save. A confirmation message appears.

New incoming messages are forwarded to the specified addresses. You can also configure forwarding destinations while creating a new email address in the control panel. For more information, see Create an Email Address with the Control Panel.
9.3.3 Automatically Responding to Email

Any email address set up in the control panel can be configured to automatically respond to incoming email. To setup an autoresponder:

1. Log in to the WebFaction control panel.
2. Click E-mails → E-mail addresses. The list of email addresses appears.
3. Click on the email address to automatically respond to email. In the Send automatic response section, click Yes. Fields for customizing the autoresponder messages appear.
4. In the From fields, enter an outgoing email address and display name for the automatic response.
5. In the Subject field, enter a subject line for the automatic response.
6. In the Message field, enter a message body for the automatic response.
7. (Optional) In the Reply To fields, enter an email address and display name for the automatic response’s Reply-To address.
8. Click the Save button to save your changes. A confirmation message appears.

New incoming messages receive an automatic response. You can also configure autoresponders while creating a new email address in the control panel. For more information, see Create an Email Address with the Control Panel.

9.3.4 Automatically Emptying a Folder

To delete all of the email in a folder automatically, run this Python script:

```python
#!/usr/local/bin/python2.7

import imaplib

M = imaplib.IMAP4('mail.webfaction.com')
M.login('<mailbox_name>', '<mailbox_password>')
M.select('<folder>')
typ, data = M.search(None, 'ALL')
for msgid in data[0].split():
    M.store(msgid, '+FLAGS', '("Deleted")')
M.expunge()
M.close()
M.logout()
```

where:

- `<mailbox_name>` is the name of a WebFaction mailbox as it appears on the control panel,
- `<mailbox_password>` is the mailbox password,
- and `<folder>` is the name of the folder to be emptied (for example, Spam or Junk).

If you want to schedule a folder to emptied on a regular basis, run the script as a cron job.

9.3.5 Spam Protection

You can filter incoming spam messages on any of your mailboxes. Our spam protection strategy uses greylisting, blacklists, and SpamAssassin, an effective, open source spam filter. You can automatically direct junk messages to a folder, delete junk messages, or use custom filtering. To configure a mailbox’s spam handling, see Create an Email Mailbox with the Control Panel for details.
Backscatter Spam

Does it look like your email account has been hacked? If you’ve suddenly received many notifications of bounced email—email messages with phrases like *delivery failed*, *no such user*, or *mailbox not found*—in response to messages you don’t recall sending, your account probably wasn’t hacked. Instead, you may be the victim of backscatter spam.

Backscatter spam is the result of spammers sending email with forged *From* addresses. When the faked sender address happens to be your mail account, the various bounce responses are sent to your address, rather than the actual sender.

Typically, backscatter spam appears in batches. You may receive many backscatter spam messages over the course of several hours and then go weeks, months, or even years without seeing more. In such cases, it’s easiest to delete the offending messages and move on. But if you find yourself the frequent victim of backscatter spam, try these solutions:

- Where possible, remove catchall email addresses. With a catchall address, all email addresses on a domain are considered valid. Because spammers often use random sender addresses, this increases the likelihood that your address will receive the backscatter spam messages.
- Consider creating an SPF record for your domain. SPF records, or *Sender Policy Framework* records, inform receiving mail servers of servers permitted to send on behalf of your domain, allowing recipients to silently reject mail sent from unauthorized sources. Not all mail servers verify incoming mail against SPF records, however, so this method may only reduce, not eliminate, the volume of backscatter spam you receive. See *Configuring SPF Records* for step-by-step instructions.

For more details on what an SPF records are and how to use them, see Wikipedia’s *Sender Policy Framework* article and the *Sender Policy Framework* project.

9.3.6 Sending Mail from an Application

WebFaction web servers provide a sendmail interface via `/usr/bin/sendmail` or `/usr/sbin/sendmail`. Mail can be sent directly with sendmail or through a programming language’s wrapper around sendmail, like like PHP’s `mail()` function.

**Note:** By default, mail sent through sendmail is from a `user@host.webfaction.com` address, where *user* is your username and *host* is the name of the server. Our mail system will not allow messages to be sent from such addresses, so be sure to set a valid sender address in your application.

You also have the option of connecting to an outside SMTP server, such as the WebFaction SMTP server. Many languages have libraries to simplify this process.

For example, this Python script will send the contents of `email_msg.txt` to `team@example.com`.

```python
from smtplib import SMTP
from_addr = 'my_email_address@example.com'
to_addrs = ['team@example.com']
msg = open('email_msg.txt', 'r').read()
s = SMTP()
s.connect('smtp.webfaction.com')
s.login('my_mailbox_name', 'password1')
s.sendmail(from_addr, to_addrs, msg)
```

This PHP script sends a message using the built-in `mail()` function:
This PHP script uses the PEAR mail package to send a message without the built-in `mail()` function:

```php
<?php
require_once "Mail.php";
$from_addr = "Me <my_email_address@example.com>";
$to = "Team <team@example.com>";
$subject = "Hello!";
$body = "Dear Team, here is my message text.";
$headers = array("From" => $from_addr,
                 "To" => $to,
                 "Subject" => $subject);
$smtp = Mail::factory("smtp", array("host" => "smtp.webfaction.com",
                                       'auth' => true,
                                       'username' => "my_mailbox_name",
                                       'password' => "password1"));
$mail = $smtp->send($to, $headers, $body);
?>
```

Here is a Perl script that demonstrates sending an email:

```
#!/usr/bin/perl -w
use Net::SMTP;
use MIME::Base64;

$smtphost = "smtp.webfaction.com";
$username = '<username>';  
$password = '<password>';  
$TZoffset = '<tz_offset>';  
$emailto = '<recipient>';  
$subject = '<subject>';  
$message = '<message>';  

sub date_r  {
    my ($monthday, $mon, $yr, $time, $hour, $str);
    $str = $mon . "/" . $monthday . "/" . $yr . ":" . $time;
    return $str;
}

$mail = Net::SMTP->new($smtphost, Debug => 1, Timeout => 5);
$mail->datasend("AUTH LOGIN
");
```
Warning: Please note that your script or application must comply with WebFaction’s Acceptable Use Policy (AUP). Do not send unsolicited bulk email messages. All mass mailings must be opt-in and provide a means for subscribers to easily opt-out. Violation of the AUP may result in suspension or termination of your account. See also: Email Limitations and Restrictions

9.3.7 Sending Mail to a Script

Our mail system features mail2script, which allows you to send email to a script in your home directory. When an email message is received by our mail server, mail2script executes the specified script with the email message (including any headers and attachments) provided via standard input.

Some caution is required before handling incoming mail with a program. Failures in the script occur silently. If something goes wrong with the program that’s processing incoming mail, then you will not be notified. If you want to retain a copy of all messages, then choose to save to local mailboxes or forward to another destination, in addition to sending mail to a script.

To use mail2script with an existing address:
1. Log in to the WebFaction control panel.
2. Click E-mails → E-mail addresses. The list of email addresses appears.
3. Click on the email address to send email to a script.
4. In the Send to a program section, click Yes. A Path field appears. If you have plans on more than one server, a Machine field appears.
5. If applicable, in the Server field, click to select the program’s server.
6. In the Path field, enter an absolute path to the program (for example, /home/username/myscript.py).
7. Click the Save button to save your changes. A confirmation message appears.

For example, this Python script writes all incoming email to example-script.out in user123’s home directory:

```python
#!/usr/bin/env python
import sys
```
output = open('/home/user123/example-script.out', 'a')
output.write(sys.stdin.read())
output.close()

Note: *mail2script* scripts are run as your user and must be executable by your user. To make your script executable:
1. Open an SSH session to your account.
2. Enter `chmod u+x path`, where *path* is the path to the script, and press Enter.

### 9.4 Mailing Lists

Each WebFaction account comes with an unlimited number of *Mailman* mailing lists, with web-based administration tools and user-driven opt-in and unsubscribe actions.

To create a mailing list, you will need to request it by creating a support ticket with the following information:

- an email address for the mailing list itself, where incoming and outgoing mail will be sent and received, like `project-discuss@example.com`,
- another email address for the person responsible for administering the mailing list, and
- optionally, a administration password (if unspecified, one will be generated for you).

**Warning:** Common list names such as `members`, `discuss`, or `news` are not available. The list’s name is the portion of the address before the `@` symbol. Please choose a name which uniquely identifies your mailing list (for example, `myorg-discuss`).

**Note:** Mailing lists are only available to domains and subdomains that use WebFaction’s mail servers to manage email. If a domain’s MX record is pointing to a third-party mail server, such as Google Apps for Domains’s mail server, then that domain cannot be used with a WebFaction mailing list.

To use a WebFaction mailing list with a domain using a third-party mail server, create a subdomain for the mailing list (for example, `lists.example.com`), and create MX records pointing to WebFaction’s mail servers.

See *Managing DNS Records with the Control Panel* and *Using External Name Servers* for more details.

To create a support ticket to request a mailing list, see *Opening a Ticket*.

### 9.5 Email Limitations and Restrictions

WebFaction does not arbitrarily limit the total number of messages you may store on our mail servers. Stored messages count toward your total disk space allotment, however. Email storage is not unlimited.

Incoming and outgoing email messages may not exceed 35MB, including attachments.

Please limit your average number of outgoing messages to 500 messages per day. If you need to send more mail, then we strongly recommend a dedicated mail service, such as iContact or MailChimp.

To minimize spam, outgoing port 25 traffic is blocked on WebFaction web servers. To send mail, you can use a local delivery agent (see *Sending Mail from an Application*), WebFaction’s SMTP server (see *Configuring Other Mail Clients*), or a third-party SMTP server through ports 465 (SSL) or 587 (TLS).
Using WebFaction’s SMTP server, you may not send email with a sender address domain of host.webfaction.com (for example, user@web555.webfaction.com), nor with a sender address domain used by common email providers, including:

- aol.com
- gmail.com
- hotmail.com
- live.com
- outlook.com
- yahoo.com
- yandex.com
- yandex.ru
- qq.com

To send messages from such providers’ addresses, please use the provider’s SMTP server. All outgoing mail with such a sender address domain is silently discarded unsent; no error or bounce message is returned to the sender.

As always, please consider the WebFaction Acceptable Use Policy, which prohibits unsolicited bulk email and prohibits mailing lists which are not opt-in.

### 9.6 Using Google Apps for Email

If you have a Google Apps account, you can use Google Apps mail instead of WebFaction’s mail server. To configure a domain to use Google Apps for email:

1. Log in to the WebFaction control panel.
2. Click Domains / websites → Domains. The list of domains appears.
3. Click on the domain to switch to Google Apps mail.
4. In the Email section, click to select External.
5. Click Add Mail Server five times, to add five rows to the list of mail servers. Priority and Mail Server fields appear.
6. In the Priority and Mail Server fields, enter the following value pairs:

<table>
<thead>
<tr>
<th>Priority</th>
<th>Mail Server</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>ASPMX.L.GOOGLE.COM</td>
</tr>
<tr>
<td>5</td>
<td>ALT1.ASPMX.L.GOOGLE.COM</td>
</tr>
<tr>
<td>5</td>
<td>ALT2.ASPMX.L.GOOGLE.COM</td>
</tr>
<tr>
<td>10</td>
<td>ALT3.ASPMX.L.GOOGLE.COM</td>
</tr>
<tr>
<td>10</td>
<td>ALT4.ASPMX.L.GOOGLE.COM</td>
</tr>
</tbody>
</table>

7. Click the Save button.

You may wish to complete additional configuration steps:

- To configure SPF records for spam protection:
  - If you plan to send mail only from Google Apps, create an SPF record with Google’s recommended value: `v=spf1 include:_spf.google.com ~all`
  - If you plan to send mail from both Google Apps and WebFaction’s SMTP server, create an SPF record with this value: `v=spf1 a:smtp.webfaction.com include:_spf.google.com ~all`
• To configure Google’s DKIM signature for spam protection:
  1. Create a new subdomain of the form `prefix._domainkey.domain`, where `prefix` is the DKIM selector prefix (typically `google`) and `domain` is your domain name. For example, to add the subdomain for `example.com`, create `google._domainkey.example.com`.
  2. Create a new TXT record for the DKIM subdomain with the public key value provided by Google.

• To point a subdomain (for example, `webmail.example.com`) to Google Apps:
  1. Log in to the WebFaction control panel.
  2. Click `Domains / websites → Domains`. The list of domains appears.
  3. Click on the domain to point to Google Apps.
  4. In the Hosting section, click to select `Cname`. The Cname field appears.
  5. In the Cname field, enter `ghs.google.com`.
  6. Click the Save button.

See also:
  • Managing DNS Records with the Control Panel
  • Google Apps Help: Configuring Your MX Records
  • Google Apps Help: Authenticate email with DKIM
  • Google Apps Help: Web address
WebFaction supports two kinds of databases, MySQL and PostgreSQL (also known as Postgres). Both of database types support many advanced features and have large user-bases. In this section, you will learn how to create, manage, and access databases of both types.

## 10.1 Creating a New Database with the Control Panel

To create a new database with the control panel:

1. **Log in to the WebFaction control panel.**
2. Click **Databases → Databases**. The list of databases appears.
3. Click the **Add new database** button. The **Create a new database** form appears.
4. In the **Name** field, enter a name for the database.
5. In the **Database type** menu, click to select **PostgreSQL** or **MySQL**.
6. If applicable, choose a server to host the database. In the **Machine** menu, click to select a server.
7. If desired, change the database encoding. To change the database encoding:
   a) Click **Change**. A menu appears.
   b) In the menu, click to select an encoding. For example, **latin7**.
8. Choose a database owner.
   To choose an existing user, in the **Database owner** menu, click to select a username.
   To create a new user:
   a) In the **Database owner** menu, click to select **Create a new postgresql user** or **Create a new mysql user**, as applicable. The **Username**, **Password**, and **Confirm password** fields appear.
   b) In the **Username** field, enter a username.
   c) In the **Password** field, enter a password.
   (See also: 
   See *Strengthening Passwords* for important information about choosing passwords.
   d) In the **Confirm Password** field, reenter the password.
9. **Optional**: Enable additional database features. In the **Add Ons** section, click to select one or more features.
10. Click the **Save** button.

The database is created and a confirmation message appears. See *Connecting to a Database* for connection details.
10.2 Managing Database Users

Each database must have a user as owner of the database, but additional users may be granted access to the database. You may use the control panel to create or delete users, or grant users permission to use specific databases.

10.2.1 Creating a Database User with the Control Panel

To create a database user with the control panel:

1. Log in to the WebFaction control panel.
2. Click Databases → Database Users. The list of database users appears.
3. Click the Add new database user button. The Create a new database user form appears.
4. In the Username field, enter a name for the database user.
5. In the Database type menu, click to select the type of database the new user may access.
6. If applicable, choose the server on which the user is created. In the Machine menu, click to select a server.
7. In the Password field, enter a password.

See also:

See Strengthening Passwords for important information about choosing passwords.
8. In the Confirm password field, reenter the password.
9. Click the Save button.

The database user is created and a confirmation message appears. You may choose the new user as owner of a new database or grant the user permissions on an existing database.

10.2.2 Modifying a Database User’s Permissions with the Control Panel

You can grant or remove a database user’s access to one or more databases. To modify a database user’s permissions:

1. Log in to the WebFaction control panel.
2. Click Databases → Database Users. The list of database users appears.
3. Click on the user to modify. The user’s details appear, including the Permissions list.
4. Add or remove the databases.

To revoke access to a database, click the - (minus) button beside a database.

To grant access to a database:

(a) At the end of the permissions list, click the + (plus) button. A menu of databases appears.
(b) In the menu of databases, click to select a database to grant the user access to.
5. Click the Save button.

The database user’s privileges are updated and a confirmation message appears.
10.2.3 Changing a Database User’s Password

To change a database user’s password:

1. Log in to the control panel.
2. Click Databases → Database Users. The list of database users appears.
3. Click on the user to modify. The user’s details appear.
5. In the Password field, enter the new password.

See also:

See Strengthening Passwords for important information about choosing passwords.

6. In the Confirm password field, reenter the password.
7. Click the Save button.

The user’s password is changed and a confirmation message appears. Use the new password to connect to any databases that the user has access to.

10.3 Connecting to a Database

To connect to a local database (for example, from a script running on a WebFaction server), use the following connection details:

- **hostname:** localhost or server_name.webfaction.com, where server_name is the server name
- **port:** for MySQL, use 3306; for PostgreSQL, use 5432.
- **database:** the name of the database
- **username:** a valid database username with ownership of or permissions to the database

For instructions on common connection methods, including how to connect remotely or using the command line tools, please see the following sections.

10.4 Accessing a Database from the Web

WebFaction provides two tools, phpMyAdmin and phpPgAdmin, to simplify many common database administration tasks and provide web-based access to your databases.

10.4.1 Access phpMyAdmin

To log in to phpMyAdmin:

1. Log in to the control panel.
2. Click Databases → Databases. The list of databases appears.
3. In the row of the database to access, click phpMyAdmin. The phpMyAdmin home page appears.

**Note:** You may be prompted about the security certificate. Please accept the certificate. The prompt occurs since you are connecting directly to one of the WebFaction web servers, rather than the main control panel site.
4. In the *Username* field, enter the username of a database user with access to one or more databases.

5. In the *Password* field, enter the database user’s password.

6. Click the *Go* button.

In the menu on the left, a list of databases appears.

---

**Note:** Attempts to load SQL files larger than 20MB will fail. To import SQL data too large for phpMyAdmin, *import data with the mysql command line tool.*

---

### 10.4.2 Access phpPgAdmin

**Note:** Only databases owned by a logged in user are available in phpPgAdmin. Additional users granted access to a database will not be able to access or modify that database with phpPgAdmin.

To log in to phpPgAdmin:

1. Log in to the control panel.

2. Click *Databases* → *Databases*. The list of databases appears.

3. In the row of the database to access, click *phpPgAdmin*. The *phpPgAdmin* home page appears.

   **Note:** You may be prompted about the security certificate. Please accept the certificate. The prompt occurs since you are connecting directly to one of the WebFaction web servers, rather than the main control panel site.

4. In the menu on the left, click *PostgreSQL*. A login form appears.

5. In the *Username* field, enter the username of a database user that owns one or more databases.

6. In the *Password* field, enter the database user’s password.

7. Click the *Login* button.

A list of databases appears.

**Note:** Attempts to load SQL files larger than 20MB will fail. To import SQL data too large for phpPgAdmin, *import data with the psql command line tool.*

---

### 10.5 Accessing a Database from the Command Line

MySQL and PostgreSQL each provide a command line interface, which you can use to issue commands to your databases while logged into your web server with SSH. MySQL uses `mysql`; PostgreSQL uses `psql`.

#### 10.5.1 MySQL Command Line

To log in to a MySQL database enter this command at the terminal prompt, enter:

```
mysql -u username -D database_name -p
```

where:

- *database_name* is the name of the database as it appears on the control panel, and
• `username` is the name of a database user with permission to use the database, and press `Enter`.

For example, `user123` logs in to `user123_mysql_db`:

```bash
user123@webXX ~ $ mysql -u dbuser123 -D user123_mysql_db -p
Enter password:
Welcome to the MySQL monitor. Commands end with ; or \g.
Your MySQL connection id is 8047 to server version: 5.0.19
Type 'help;' or '"h' for help. Type '\c' to clear the buffer.
mysql>
```

### 10.5.2 PostgreSQL Command Line

To log in to a PostgreSQL database enter this command at the terminal prompt:

```bash
psql -U username database_name
```

where:

- `database_name` is the name of the database as it appears on the control panel, and
- `username` is the name of a database user with permission to use the database, and press `Enter`.

For example, `user123` logs in to `example_db`:

```bash
user123@webXX ~ $ psql -U user123 example_db
Password for user user123:
Welcome to psql 8.3.1, the PostgreSQL interactive terminal.
Type: \copyright for distribution terms
\? for help with psql commands
\g or terminate with semicolon to execute query
\q to quit
user123=>
```

### 10.6 Accessing a Database Remotely

You can access a database remotely by using an SSH tunnel, which establishes a secure connection through which ordinary database traffic can travel. It allows you to work with your database as if it were running on your local computer. You can establish an SSH tunnel with PuTTY or the `ssh` command line tool.

#### 10.6.1 Starting an SSH Tunnel with `ssh`

1. Open a terminal session.
2. Enter `ssh -L 3306:127.0.0.1:3306 username@webXX.webfaction.com` where `webXX` is your machine name (e.g. `web57`) and press `Enter`.

   **Note:** For PostgreSQL, substitute `3306` with `5432`:
   `ssh -L 5432:127.0.0.1:5432 username@webXX.webfaction.com`.

3. You may be alerted that the authenticity of the host cannot be established. Enter `yes` and press `Enter`.
4. When prompted, enter your password and press `Enter`.
5. Leave the SSH session open as long as you want to maintain the tunnel.
   You can now connect to your database at `127.0.0.1`, port `3306`.
6. Enter `exit` and press `Enter` to close the connection.

### 10.6.2 Starting an SSH Tunnel with PuTTY

1. Start PuTTY.
2. In the Category tree, click to expand `SSH`.
3. In the Category tree, click to select `Tunnels`.
4. In the Source port field, enter `3306`.

   **Note:** For PostgreSQL, substitute `3306` with `5432`.

5. In the Destination field, enter `127.0.0.1:3306`.

   **Note:** For PostgreSQL, substitute `3306` with `5432`:
   `127.0.0.1:5432`.

6. Click the Add button.
7. In the **Category** tree, click to select **Session**.

8. In the **Host Name (or IP address)** field, enter `webXX.webfaction.com` where `webXX` is your machine name (e.g., `web57`).

9. In the **Port** field, enter `22`.

10. Under **Connection type**, click to select **SSH**.

11. Click the **Open** button.
12. A PuTTY Security Alert dialog may open. If so, click the Yes button.

13. When prompted, enter your username and press Enter.

14. When prompted, enter your password and press Enter.

15. Leave the PuTTY window open as long as you want to maintain the tunnel.

   You can now connect to your database at 127.0.0.1, port 3306.

16. Enter exit and press Enter to close the connection.

10.7 Accessing a Database from a Script or Application

You can also access your databases from scripts or applications. The MySQL and PostgreSQL instances are available on the web server. Many languages offer libraries to simplify making and executing SQL queries.

For example, the Python package MySQL-Python provides access to MySQL databases. This script, for example, prints all of the rows in the names table.
Likewise, you might access a PostgreSQL database with Psycopg in a Python script. Psycopg is a PostgreSQL database adapter for Python; the package is installed by default. Here’s a script equivalent to the previous Python script, except that it reads from a PostgreSQL database:

```python
import psycopg2
db = psycopg2.connect(host='127.0.0.1',
                      database='user123s_pg_database',
                      user='user123',
                      password='averysecurepassword',)
cursor = db.cursor()
cursor.execute('SELECT * FROM names;')
result = cursor.fetchall()
print result
```

PHP provides built-in functions for working with MySQL. In this example, the PHP script prints all of the rows in the `names` table:

```php
<?php
mysql_connect("127.0.0.1", "user123", "averysecurepassword");
mysql_select_db("user123s_my_db") or die("Unable to select database");
$result = mysql_query("SELECT * FROM names");
mysql_close();
while ( $row = mysql_fetch_row($result) ) {
    echo implode(" ", $row), "
"
}
?>
```

10.8 Import and Export Database Records

SQL-style databases allow you to export, or `dump`, the contents of a database in a form which allows you to restore, or `import`, the state of that database on a bare database. This can be used to copy, rename, or backup databases.

**Note:** To minimize load and preserve performance on your server, please use `ionice` with database imports and exports larger than 500MB.

To use `ionice`, add `ionice -c2 -n6` before your database shell commands. For example, to export a PostgreSQL database with `ionice`, enter:

```
ionice -c2 -n6 pg_dump -U database_user -f dump.sql database_name
```

10.8.1 Export

To export a MySQL database, enter:
WebFaction User Guide

mysqldump -u database_user database_name -p > dump.sql

where *database_user* is the name of a user with access to a MySQL database of the name *database_name*, and press Enter. *mysqldump* prompts for the password configured for that database. The contents of the database are written to *dump.sql* in the directory where the command is run.

To export a PostgreSQL database, enter:

pg_dump -U database_user -f dump.sql database_name

where *database_user* is the name of a user with access to a PostgreSQL database of the name *database_name*, and press Enter. *pg_dump* prompts for the database password. The contents of the database are written to *dump.sql* in the directory where the command is run.

**Note:** On some WebFaction servers, *pg_dump* is not in your default search path and may result in a command not found error. Use the complete path to *pg_dump*, /usr/local/pgsql/bin/pg_dump, instead.

Once you have created the dump file, you can download that file with scp or SFTP.

### 10.8.2 Import

To import a MySQL database, enter:

mysql -u database_user -p -D database_name < file

where *database_user* is the name of a user with access to a MySQL database of the name *database_name* and file is the path to a MySQL dump file, and press Enter. *mysql* prompts for the database password.

**Note:** If you’re importing a dump file encoded with a character set other than *utf8* (for example, *latin1*), when invoking mysql you must use the option --default_character_set encoding, where *encoding* is the name of the dump file’s encoding. Thus, the complete command for importing a non-*utf8* dump file is:

mysql -u database_user -p -D database_name --default_character_set encoding < file

To import a PostgreSQL database, enter:

psql -U database_user database_name < file

where *database_user* is the name of a user with access to a PostgreSQL database of the name *database_name*, and file is the path to a PostgreSQL dump file, and press Enter. *psql* prompts for the database password.

**Note:** If your dump file was created as a PostgreSQL custom dump, then you must use *pg_restore* to import the data. To import a PostgreSQL database with *pg_restore* enter this command:

pg_restore -U database_user -d database_name file

and press Enter.

### 10.9 Backing Up a Database Automatically

Regular backups of your data are important. You can schedule a cron job to automatically backup a MySQL or PostgreSQL database.
**10.9.1 MySQL**

To schedule an automatic backup of a MySQL database:

1. **Open an SSH session to your account.**
2. Create a directory to store the database backups. Enter `mkdir $HOME/db_backups` and press Enter.
   
   (a) Create the file. Enter `touch $HOME/db_backups/database_name.cnf` where `database_name` is the name of the database, and press Enter.

   (b) Set the file permissions such that only you can read and write to the file. Enter `chmod 600 $HOME/db_backups/database_name.cnf` and press Enter.

   (c) Open the file in a text editor.

   (d) Insert these lines:

     ```
     [client]
     password='secret'
     ```

     where `secret` is the password for the database user.

   (e) Save and close the file.

4. **Edit your crontab to contain this line:**

   ```
   0 2 * * * mysqldump --defaults-file=$HOME/db_backups/database_name.cnf -u database_user database_name > $HOME/db_backups/database_name-$(date +%Y%m%d).sql 2>> $HOME/logs/user/database_name_cron.log
   ```

   where `database_user` is the name of a user with access to a MySQL database of the name `database_name`.

   **Note:** On some WebFaction servers, `mysqldump` is not in the search path used by cron and may result in a `command not found` error in your `$HOME/logs/user/database_name_cron.log` file. If this happens, then use the complete path to `mysqldump`, `/usr/bin/mysqldump`, instead.

Now the database is backed up at 2 a.m. each day.

**10.9.2 PostgreSQL**

To schedule an automatic backup of a PostgreSQL database:

1. **Open an SSH session to your account.**

2. Open a `$HOME/.pgpass` in a text editor (or create a new file, if it does not already exist).

3. Add a new line containing `*:*:database_name:database_user:password` where `database_user` is the name of a user with access to a PostgreSQL database of the name `database_name` and `password` is the password of the database user.

4. Set the file permissions such that only you can read and write to the `~/.pgpass` file. Enter `chmod 600 $HOME/.pgpass` and press Enter.

5. Create a directory to store the database backups. Enter `mkdir $HOME/db_backups` and press Enter.

6. **Edit your crontab to contain this line:**

   ```
   0 2 * * * /usr/local/pgsql/bin/pg_dump -Fp -b -U database_user database_name > $HOME/db_backups/database_name-$(date +%Y%m%d).sql 2>> $HOME/logs/user/database_name_cron.log
   ```

Now the database is backed up at 2 a.m. each day.
10.10 Delete a Database

If you no longer need a database, you can delete it with the control panel. Keep in mind, however, that the database will be deleted immediately and completely. Please make a backup; see Export for details.

10.10.1 Delete a Database with the Control Panel

To delete a database with the control panel:

<table>
<thead>
<tr>
<th>Warning: Deleting a database cannot be undone.</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Log in to the WebFaction control panel.</td>
</tr>
<tr>
<td>2. Click Databases → Databases. The list of databases appears.</td>
</tr>
<tr>
<td>3. Click the name of the database to be deleted. The database details appear.</td>
</tr>
<tr>
<td>4. Click the Delete button. A prompt, Are you sure you want to delete this database?, appears.</td>
</tr>
<tr>
<td>5. To delete the database, click the Yes, I'm sure button. To keep the database, click No, Cancel button.</td>
</tr>
</tbody>
</table>

If you to delete the database, it is immediately and irrecoverably deleted.

10.11 Enabling Procedural Languages for PostgreSQL

PostgreSQL databases can be extended with three trusted procedural languages: PL/pgSQL, PL/Tcl, and PL/Perl. By default, these languages are not enabled and must be specifically configured.

| Note: PL/Perl is not available on web20 or less or dweb6 through dweb17. |
| PL/Python is not a trusted procedural language and cannot be enabled on your server’s shared PostgreSQL database. |

To enable PL/pgSQL, PL/Tcl, or PL/Perl:

1. Open an SSH session to your account.

2. Start a shell session for your database. Enter `psql -U database_user -d database_name`, where `database_user` is the name of a user with access to a PostgreSQL database of the name `database_name`, and press Enter. A password prompt appears.

3. Enter the password for the database user and press Enter.

4. Enable the procedural language.
   - To enable PL/pgSQL, enter `create language plpgsql;` and press Enter.
   - To enable PL/Perl, enter `create language plperl;` and press Enter.
   - To enable PL/Tcl, enter `create language pltcl;` and press Enter.

CREATE LANGUAGE appears in the shell.

5. End your database shell session. Enter `\q` and press Enter.

The procedural language you selected is enabled. For more information on extending PostgreSQL with procedural languages, please see the PostgreSQL Manual chapter entitled Procedural Languages.
The various hosting plans that WebFaction offers are differentiated primarily by the quotas of system resources that they provide.

This section describes how quotas are enforced, how resources are measured on different types of hosting plans, and how you can view your resource usage.

11.1 Quotas on Shared Hosting

WebFaction’s shared hosting plans run on servers designed to host many (but not too many!) customers, with a large amount of RAM and storage. The resource quotas for these plans are soft limits enforced by automated monitoring systems.

If you exceed your quotas on a shared hosting plan, you will be notified via a support ticket and/or email.

In extreme cases, WebFaction may terminate your processes, archive your large files, or take other immediate corrective action prior to notification to ensure that other shared server customers are not disrupted by the exhaustion of available resources.

11.2 Quotas on Cloud Hosting

WebFaction’s cloud hosting plans run on managed dedicated virtual machines. The quotas on cloud hosting plans are estimates of resources available to you, based on the total capacity of the server minus the overhead of the server operating system and hosting infrastructure. Actual availability of resources may vary due to resource utilization by the server operating system and hosting infrastructure.

Since cloud server resources aren’t shared with other customers, you’re free to use all of the available resources on the server. If you exhaust the available resources on your cloud servers, you may be notified via a support ticket and/or email.

11.3 Types of Resources

11.3.1 RAM

On shared servers, our monitoring system will check the memory usage of your long-running processes at regular intervals throughout the day.

- If you are over your RAM quota by a small amount, then the monitor will send you a notification via email to let you know about the problem.
• If you are over your RAM quota by a large amount, then the monitor will terminate your processes, and then send you a notification via email to let you know about the problem and the action that was taken.

On cloud servers, we don’t monitor your memory usage. You’re the only customer on the cloud server, so you’re free to use all of the available memory if you need to do so. Note, however, that if you use all of the available memory on your cloud server, system load will go up and performance will suffer.

There is one other memory monitor that exists on both shared and cloud servers: the Linux OOM (“out of memory”) killer. This is a kernel feature that selectively terminates processes to ensure that the operating system has enough memory to function. No notifications are sent when the OOM killer terminates a process.

You can view your RAM usage in a SSH session with the `ps` command. To do so:

1. Log into a SSH session.
2. Type `ps -u $USER -o rss,pid,command` and press Enter.

The output will show the following information for each of your processes:

- Memory usage in KB
- Process ID
- The command running for the process

If you want to see your total memory usage in MB, then do the following:

1. Log into a SSH session.
2. Type `ps -u $USER -o rss,pid,command | awk '{sum += $1} END {print sum/1024}'` and press Enter.

### 11.3.2 Storage

On shared and cloud servers, our monitoring system will check your disk usage once every 24 hours. The items that we measure and apply to your quota are:

- Files owned by your shell users
- MySQL and PostgreSQL databases
- Mail stored for your mailbox accounts

The storage available to you is determined by the storage allowance of your hosting plans and add-on storage services. If you have multiple servers, then your available mail storage is the sum of all available unused storage from all of your plans.

For example, our 1GB shared hosting plan comes with 100GB of storage. If you have two 1GB hosting plans, with 75GB in use on the web server for the first plan, and 25GB in use on the web server for the second plan, then you have 100GB available for mail storage.

If you exceed your storage quota, we’ll notify you via email every two days to let you know about the problem. If you haven’t corrected the problem after fifteen days and haven’t responded to our messages to let you know how you plan to correct it, then your account may be disabled, and you will be notified via email of the action taken.

To view your disk usage statistics:

1. Log in to the control panel.
2. Click Usage → Disk usage.
11.3.3 Bandwidth

On shared and cloud servers, our monitoring system will check your bandwidth usage once every 24 hours.

If you exceed your bandwidth quota, we’ll notify you via email to let you know about the problem and to discuss upgrade options.

To view your bandwidth usage statistics:

1. Log in to the control panel.
2. Click Usage → Bandwidth usage.
If this user guide didn’t answer one of your questions, there are a number of other ways to get help.

12.1 Other Documentation

We have additional guides to help you with our services:

- WebFaction Software Documentation
- WebFaction API Documentation

12.2 Q&A Community

The WebFaction Q&A Community is a question and answer site where other WebFaction users and the WebFaction support team collaborate to answer questions and resolve problems. You can search the Q&A Community from any Q&A Community page to see if your question has been addressed previously. If it hasn’t, you can ask a new question to start a conversation and vote on the best responses. The WebFaction support team monitors new posts to the Q&A Community in the same way as a support ticket, so the support team will be on hand to provide their expertise, and if necessary, investigate your issue more closely.

12.3 Support Tickets

Our skilled support team is available to contact directly, by opening a support ticket. If your problem is not suited to the community (for example, the question involves sensitive data), open a support ticket where we can help you privately.

12.3.1 Opening a Ticket

To open a ticket:

1. Log in to the control panel.
2. Click Support → Open a ticket. The WebFaction ticketing system appears.
3. Click Submit a Ticket. The ticket form appears.
4. In the **Priority** menu, click to select a priority level.

Here are some guidelines to setting the priority level:

- **Low**: Feature requests, configuration questions, and other issues that are of a speculative or informative nature
- **Medium**: Non-critical errors, bugs, or other issues that are preventing sites and applications from working that are infrequently used or not live
- **Urgent**: Data loss, server crashes, and any other issue that prevents you from accessing your services or sites that were working previously

5. In the **Subject** field, enter a subject for your message. Try to be brief but descriptive. For example, “Web10 under heavy load” is preferable over “Sever problem.”

6. In the main text field, describe your problem. If possible, include these details:
   - Specific and detailed steps to reproduce the problem
   - Expected behavior
   - Names of applications, domains, websites, and machines involved
   - Time the problem occurred, with as much specificity as possible
   - Any relevant errors, warnings, and other output
   - System configuration details, such as operating system and browser version

7. **Optional**: To attach a file, click the **Choose file** button. This is commonly used to attach relevant screenshots, log files, and sample data.
Note: Please avoid submitting files in proprietary formats, such as Microsoft Word (.doc and .docx) and Adobe Photoshop (.psd). Frequently, proprietary formats can only be opened with specific software that our support team may not have readily available; this can delay investigating and resolving your issue.

8. In the CC field, enter any addresses to CC on messages sent by the support team.

9. When you are finished preparing your ticket, click the Submit button. You will be contacted by the WebFaction support team soon.

12.3.2 Checking the Status of a Ticket

To review any information exchanged between WebFaction support and your account:

1. Log in to the control panel.
2. Click Support → Open a ticket. The WebFaction ticketing system appears.
3. Click View Tickets. The ticket list appears.
4. Click the title of the ticket you want to review. A page with all messages relevant to the selected support ticket appears.

12.3.3 Closing a Ticket

If your problem or question has been resolved, please close the ticket. To close the ticket:

1. Log in to the control panel.
2. Click Support → Open a ticket. The WebFaction ticketing system appears.
3. Click View Tickets. The ticket list loads.
4. Click the title of the ticket you want to close.
5. In the Status menu, click to select Closed.
6. Click Update. The ticket’s status is changed to closed.
13.1 Moving to WebFaction from Other Hosting Providers

Moving your sites to WebFaction doesn’t need to be an ordeal. The strategies in this section help move many types of sites, with specific recommendations for common tasks, such as moving a WordPress installation or copying a MySQL database.

13.1.1 Moving a Site to WebFaction

While every application is a little bit different, try these common steps to move a site from your previous hosting provider to your WebFaction account.

See also:

See Moving a WordPress Site for a more detailed example.

1. **Create an application.**
   
   Common application choices include:
   
   - *Static/CGI/PHP* for PHP-based sites
   - *Static-only* for sites consisting of static HTML, JavaScript, and media files
   - *Custom* for servers that listen to incoming requests on a port

2. If applicable, **create a MySQL or PostgreSQL database.**

3. Copy your files to the application directory, `/home/username/webapps/app`, where `username` is your WebFaction account name and `app` is the name of the application as it appears on the control panel.

   See also:
   
   - See Connecting with FTP to learn how to configure your FTP client.
   - See Copying Files from an FTP Server for instructions on copying files from your previous hosting provider directly to your WebFaction server with FTP.

4. If applicable, modify your site’s configuration files to account for new paths, database names, passwords, and other differences between your previous host and your WebFaction account.

5. Copy your database.

   See also:
   
   - See Import and Export Database Records for instructions on importing a database dump file.
   - If your previous hosting provider offers phpMyAdmin access, see Importing a Database from phpMyAdmin to learn how to export your database and import it to WebFaction.
6. Create (or modify) a website entry to connect an application to a domain name and URL path.

**Note:** You can use `username.webfactional.com` and its subdomains, where `username` is your WebFaction account name. It’s ideal for testing a new site before using your own domain.

If you’re ready to use an existing domain, see *Pointing Your Domain to WebFaction’s Servers*. DNS changes take up to 48 hours to take effect, so plan ahead.

7. Confirm the website is working at the correct domain name and URL path.

Test different site functions, especially critical activities like logging in and accessing administrative areas, to make sure the move went successfully.

### 13.1.2 Copying Files from an FTP Server

To copy your files from your previous hosting provider with FTP:

1. **Open an SSH session to your account.**

2. Make a copy of the remote FTP files and directory structure. Enter `wget --mirror --ask-password ftp://user@host`, where `user` is the username for the remote FTP account, and `host` is the hostname or IP address of the remote FTP server, and press Enter.

   The files download into a new directory named after the FTP hostname. Large or numerous files and directories may require a long wait to download.

The files are downloaded to your WebFaction account and can be found through SFTP and SSH. Although the files are stored on the WebFaction server, they are not yet served publicly on the web. Please see *Moving a Site to WebFaction* for details.

### 13.1.3 Importing a Database from phpMyAdmin

To export a database from phpMyAdmin and import it to your WebFaction server:

1. Download your existing database.
   (a) Log in to your previous hosting provider’s phpMyAdmin.
   (b) In the left sidebar, click on the database to export.
   (c) Click the Export tab.
   (d) Click the Export tab.
   (e) If not already selected, click to select the following export options:
      - Export → SQL
      - Options → Structure
      - Options → Data
      - Save as file
   (f) Download the SQL dump file. Click the Go button.

2. Upload the dump file to your home directory.

**See also:**

See *Connecting with FTP* for details on configuring your SFTP client to connect your WebFaction server.
3. Create a new MySQL database with the control panel.

4. Import your database dump.
   
   (a) Open an SSH session to your account.
   
   (b) Enter
   
   \[
   \text{mysql} \ -u \ \text{username} \ -p \ -D \ \text{db_name} \ < \ \text{dump_file}
   \]
   
   where
   
   - \text{db_name} is the name of the MySQL database you created with the WebFaction control panel,
   - \text{username} is the name of a MySQL user with access to the database, and
   - \text{dump_file} is the path to the MySQL dump file you uploaded previously,
   
   and press Enter. A password prompt appears.
   
   (c) Enter the database password and press Enter.

   The contents of the database dump are loaded into your WebFaction database. To connect to the MySQL database, see Connecting to a Database.

13.1.4 Moving a WordPress Site

To import a WordPress site from another hosting provider:

1. Create a Static/CGI/PHP application for WordPress.

2. Import the database from your existing hosting provider.

   
   \textbf{Note:} If you are changing your WordPress site’s URL (for example, from example.com to username.webfactional.com), please see the WordPress documentation article Moving WordPress before importing your database.

   If your previous hosting provider offers phpMyAdmin, see Importing a Database from phpMyAdmin for detailed instructions.

   If you have a dump file, create a new database and import your dump file.

3. Copy the contents of the directory containing your WordPress site’s files, such as:
   
   - \text{index.php} and \text{wp-config.php}, and
   
   - subdirectories \text{wp-admin} and \text{wp-content},

   to your Static/CGI/PHP application directory, $HOME/webapps/wp_app, where \text{wp_app} is the name of the application as it appears on the control panel.

   \textbf{See also:}

   See Copying Files from an FTP Server for details on how to copy files from your previous hosting provider with your FTP account.

   
   (a) Open $HOME/webapps/wp_app/wp-config.php in a text editor.
   
   (b) Update the database name. Modify this line:

   \begin{verbatim}
   define('DB_NAME', '<database_name>');
   \end{verbatim}

   such that \text{<database_name>} is the name of the database you created as it appears on the WebFaction control panel.
(c) Update the database user. Modify this line:

```php
define('DB_USER', '<user>');
```

such that `<user>` is the name of a user that owns or has permission to use the database you created.

(d) Update the database password. Modify this line:

```php
define('DB_PASSWORD', '<password>');
```

such that `<password>` is the password for the database user.

(e) Update the database hostname. Modify this line:

```php
define('DB_HOST', 'some.host.name');
```

to this line:

```php
define('DB_HOST', 'localhost');
```

(f) Save and close the file.

5. Create a new website record to serve the Static/CGI/PHP application.

See also:

See Create a Website with the Control Panel for details on how to create a website record.

The WordPress site is available at the domain and URL you selected.

13.2 Application Security

For most users, taking routine precautions will prevent security problems. But security breaches still happen because perfection isn’t possible: new exploits appear every day, some of which have no immediate defense. Luckily, for many kinds of attacks, it’s possible to recover with a minimum of downtime and data loss.

This section describes how WebFaction secures servers, your security responsibilities, and what do if your account is compromised.

13.2.1 Cooperative Security

Maintaining security isn’t a matter of flipping a switch. Security is an ongoing process that requires cooperation between system administrators and users. It’s the responsibility of WebFaction system administrators to protect the security of the server, while it’s the responsibility of WebFaction customers to protect the security of their applications.

The WebFaction system administration team is dedicated to maintaining the security of servers by:

- keeping common system software up-to-date,
- securing server-wide utilities and services against known vulnerabilities, and
- monitoring the server for suspicious or disruptive activity.

Because there are few strict limits on what you may do with your account, we need your help to apply similar practices and protections to your account and applications.
13.2.2 Prevent Attacks

To prevent attackers from compromising your account, you should take some routine precautions that are known to reduce your likelihood of becoming a victim of hackers:

- **Keep software up-to-date, including plugins and templates.** The vast majority of compromised sites are caused by continuing to run old, unsecured versions of popular software. Stay informed about new versions of software you use. Many applications, like WordPress, have a dashboard that advises when new versions are available. Others have mailing lists or blogs that update only upon the release of new software versions or important news.

  If you’ve stopped using some software (or an add-on, like a plugin or template), then shut it down or remove it. Forgotten software is often out-of-date, insecure software. One way to reduce your risk is to eliminate possible avenues of attack. Removing unused software does that.

  **See also:**
  
  For more information about updating common application types, see Update Applications.

- **Choose strong passwords, then keep your passwords secret.**

  See Strengthening Passwords for important information about choosing passwords.

  To keep your passwords secret, avoid giving them away. A common way hackers gain access to accounts is by tricking people into giving away their security details. Be extremely suspicious when asked for your passwords. For example, WebFaction will never ask you for your account, email, or database passwords; such a request is likely an attempt to take control of your account.

  Another way hackers gain access to accounts is by finding passwords in unsecured places, like public pastebins and version control repositories. If you must store a password, then take great care to store it such that only you can access it. For example, if a configuration file contains a database password, then set the permissions on that file so that only you can read the file.

- **Review your account’s settings on a regular basis.** Periodically log in to the WebFaction control panel and review your settings. Look out for unexpected or unusual changes to your account, and make sure you’ve removed unused applications, databases, SSH or FTP users, and mailboxes. Also make sure your contact information is up-to-date. If your contact information isn’t up-to-date, we cannot contact you if your account is compromised.

- **Look for unusual account activity.** Periodically log in to your SSH account and review your crontab and running processes. By regularly logging in, you’ll know what’s normal, so you can recognize if things have gone awry.

  To review your crontab and running processes:

  1. **Open an SSH session to your account.**

  2. **Review your running processes.** Enter `ps -u username -o pid,command`, where `username` is your username, and press `Enter`. A list of process identifiers (PIDs) followed by the command for each process appears.

     **See also:**
     
     For more information about understanding your running processes, see Monitoring Memory Usage.

  3. **Review your crontab.** Enter `crontab -l` and press `Enter`. A list of recurring jobs appears, with lines consisting of the job’s schedule and the command to be run.

     **See also:**
     
     For more information about scheduling tasks with cron, see Scheduling Tasks with Cron.
• **Keep your own backups of your account data.** Backups provide a point of reference to compare your account against, if you suspect a problem. Also, in the event of a security breach, backups protect you against data loss and help to reduce recovery time.

• **If you suspect a security problem, contact WebFaction.** If for any reason you suspect your account has been compromised, then open a support ticket. The support team can help you investigate, and refer the problem to system administrators when needed.

### 13.2.3 Respond to Attacks

In the event of a security breach, don’t panic, but act quickly by following the guidelines in this section.

1. If you have discovered an attack on your account or server and WebFaction has not contacted you already, then open a support ticket and set the priority to Urgent.

   **Note:** If WebFaction contacted you about the attack, then some of the following steps may have been completed for you. The message from the support team contains details regarding your specific case, some of which may supersede this guide.

2. Disable any compromised sites:
   (a) Log in to the WebFaction control panel.
   (b) Click **Domains / websites → Websites**. The list of websites appears.
   (c) Click the name of an affected site. The site’s settings appear.
   (d) In the **Status** section, click **Disabled**.
   (e) Click the **Save** button.

3. Disable suspicious jobs in your crontab:
   (a) **Open an SSH session to your account.**
   (b) Open your crontab in a text editor. Enter `crontab -e` and press **Enter**. A list of recurring jobs appears, with lines consisting of the job’s schedule and the command to be run.

   **See also:**
   For more information about scheduling tasks with cron, see *Scheduling Tasks with Cron*.
   (a) For each suspicious line in your crontab, comment out the line by inserting a `#` at the beginning of the line.
   (b) Save and close the file.

4. Stop suspicious processes:
   (a) **Open an SSH session to your account.**
   (b) Review your running processes. Enter `ps -u username -o pid,command`, where **username** is your username, and press **Enter**. A list of process identifiers (PIDs) followed by the command for each process appears. Make a note of the PIDs for suspicious processes.

   **See also:**
   For more information about understanding your running processes, see *Monitoring Memory Usage*.
   (c) Send the signal to immediately halt the processes you identified in the previous step. Enter `kill -9 pids`, where **pids** is one or more PIDs separated by spaces, and press **Enter**.

5. Change your SSH, database, email, and control panel passwords.
• To change your SSH, SFTP, or FTP password, see Changing Your FTP or SSH Password.
• To change your database user passwords, see Changing a Database User’s Password.
• To change your mailbox passwords, see Change an Email Mailbox Password.
• To change your control panel password, see Change Your Control Panel Password.

**Note:** If you’re using SSH keys, your should remove your existing keys and create new ones. To remove your keys and create new keys:

(a) Open an SSH session to your account.
(b) Enter `rm $HOME/.ssh/authorized_keys` and press Enter.
(c) Follow the directions in Using SSH Keys to create and set up new keys.

6. Reinstall compromised applications from known, secure sources. It’s much safer to reinstall an application than to attempt to make a compromised application safe to use again. Instead, reinstall the software from a trusted source, such as:

- the control panel’s one-click installer,
- an official, secure distribution website (from HTTPS URLs where possible),
- an uncompromised version control repository, or
- a backup from before the attack took place.

If you’d like to restore from a backup and do not have one of your own, please contact the WebFaction support team; a WebFaction backup may be available.

7. Update your applications and any add-ons, like plugins and templates. Review all of your applications and confirm that you’re running versions without known vulnerabilities. If you are running vulnerable software, update it to a newer version without that vulnerability, or stop using the software. Do not continue to run vulnerable software.

See Update Applications for WebFaction documentation for updating common software packages.

8. When you’ve finished securing your applications, you can re-enable your sites:

(a) Log in to the WebFaction control panel.
(b) Click **Domains / websites → Websites.** The list of websites appears.
(c) Click the name of an affected site. The site’s settings appear.
(d) In the **Status** section, click **Enabled.**
(e) Click the **Save** button.

**Note:** If the option to re-enable your sites is not available, then your site may be locked. Contact WebFaction support for assistance.

### 13.2.4 Update Applications

We’ve created guides to updating some common application types:

- Django
- Joomla
- Trac
13.3 Migrating Servers

On occasion, you may want to move from one server to another. For example, you may be upgrading from a shared server to a cloud server. You can request a server migration at any time with the WebFaction control panel (Accounts → Resize or migrate plan). You choose the kind and location of the destination server, as well as the migration path you want to use.

There are two migration methods. You can choose to let WebFaction migrate servers for you or manually migrate from one server to another yourself. Whichever way you choose, you are responsible for verifying that the migration was completed successfully.

If you have chosen to migrate servers yourself, there are a few steps and choices ahead of you. The process may look daunting, but it’s easier with a little bit of planning and attention to detail.

13.3.1 Migrating Manually

There are two different procedures for migrating from one server to another yourself. The Simple Migration Guide minimizes the number of steps used to migrate, but you may incur some downtime as you move. The Advanced Migration Guide minimizes the duration of downtime with a more complex procedure. Choose a procedure based on your downtime requirements and the level of complexity with which you’re comfortable.

As always, consider contacting the WebFaction support team if you’re not clear on some particular step. The support team will be happy to provide guidance and assistance through this process.

13.3.2 Simple Migration Guide

This simplified migration guide minimizes the number of steps to migrate from one server to another. If you do not need to maximize the availability of your sites or you are uncomfortable working with DNS changes and your system’s hosts file, use this procedure.

Create Users

The first step in moving to a new server is to create on the destination server the same users that appear on the origin server. For each user on the origin machine, create an equivalent user on the destination machine.

Note: Some applications, such as WordPress, may not permit two applications to share the same name. If you encounter this during your migration, create an application with a different name, but remember to use the alternate name when importing database records and creating website entries.

Create Applications

The next step is to recreate applications on the destination server. For each application on the origin server (as noted by the Machine column), create a new application with the same name on the destination server.
Copy Files

The next step is to copy files from the origin server to the destination server. `rsync` makes this easy.

1. For each user on the origin server:
   (a) Open an SSH session on the origin machine.
   (b) Get a list of files to be copied. Enter `rsync -nPaAz ~/ username@destination.webfaction.com:`, where `username` is the current user name and `destination` is the name of the destination server, and press `Enter`. A list of files to be copied will appear; no files are copied at this time.
   (c) Verify that the files to be copied are those you intended.
   (d) Copy the files to the destination server. Enter `rsync -PaAz ~/ username@destination.webfaction.com:` (noting that the `n` switch has been omitted) and press `Enter`. The files will be copied. Depending on the number and size of the files to be copied, this process may take a few minutes to finish.

2. If applicable, verify that the permissions for your extra users are correct by accessing files with the new extra users you would expect to have access to. If needed, *grant access to your extra users*.

Copy Crontabs

If you have configured or modified your users’ crontabs, the contents of your users’ crontabs must be copied from the origin server to the destination server. For each user:

1. Open an SSH session on the origin server.
2. Export the contents of the crontab to a file. Enter `crontab -l > username_cron`, where `username` is the name of the current user and press `Enter`. A file, `username_cron`, will be created in the current directory.
3. Copy the file to the destination server. Enter `scp username_cron username@destination.webfaction.com:` and press `Enter`. The file is copied to the destination server.
4. Close the SSH session.
5. Open an SSH session on the destination server.
6. Import the crontab. Enter `crontab username_cron` and press `Enter`.

Create Databases and Database Users

The next step is to recreate the databases and their users on the destination server.

Many application installers create a database automatically. If you have successfully recreated these applications, their databases and users do not need to be duplicated manually.

For all other databases and users, you must recreate each yourself. For each database on the origin server, *create a new database* on the destination server. For each database user on the origin server, *create a new user* and *grant permissions*. Be sure to use the same database names and usernames on the destination server as those on the origin server.
Copy Database Records

Once the databases are set up to receive the data from the origin server, it’s time to export the data from the origin server and import that data to the databases on the destination server.

1. Open an SSH session on the origin server.
2. For each MySQL database on the origin server, dump the contents of the database to a file. Enter `mysqldump -u username database -p > database.sql`, where:
   - `database` is the name of the database
   - `username` is the name of a user that owns or has permission to use the database
   and press Enter. A dump file, `database.sql`, is created in the current directory.
3. For each PostgreSQL database on the origin server, dump the contents of the database to a file. Enter `pg_dump -U username -f database.sql database` and press Enter. A dump file, `database.sql` is created in the current directory.
4. Copy the dump files to the destination server. Enter `scp ./*.sql username@destination.webfaction.com:` and press Enter. All `.sql` files are copied to the destination server.
5. Close the SSH session on the origin server.
6. Open an SSH session on the destination server.
7. For each MySQL database on the destination server, import the corresponding dump file. Enter `mysql -u username -p -D database < database.sql` and press Enter. The contents of the file are loaded into the specified database.
8. For each PostgreSQL database on the destination server, import the corresponding dump file. Enter `psql -U username database < database.sql` and press Enter. The contents of the file are loaded into the specified database.

Edit Website Records

The next step is to modify your website entries to use the applications on the destination server.

1. Log in to the control panel.
2. Click Domains / websites → Websites. The list of websites appears.
3. Modify the site records. For each website entry on the origin server:
   (a) Click the name of the website entry. The site’s details appear.
   (b) In the Machine menu, click to select the destination server.
   (c) For each application in the Contents section:
      i. Remove the origin server application. Click x. The application is removed from the list.
      ii. Click Add an application → Reuse an existing application. The Reuse an existing web app form appears.
      iii. In the Application menu, click to select the destination server application. For example, if you removed my_wp - origin then click to select my_wp - destination.
      iv. In the URL field, enter the same URL as the origin server application’s URL.
      v. Click the Save button.
(d) Click the Save button.

Finishing Touches

Now that you have verified your destination server is operating smoothly, it is time to make any last minute updates, and clean up.

1. If needed, copy any new files or migrate any new data from the origin server to the destination server.
2. Reply to your existing support ticket (or open a new ticket) to inform the support team that your migration is complete and you’re ready for your data to be deleted on the origin server.

Congratulations, you have successfully migrated from one server to another.

13.3.3 Advanced Migration Guide

This advanced version of the migration process minimizes downtime at the expense of added complexity. Use this procedure if you need to maximize the availability of your sites and applications and you are comfortable working with DNS changes and your system’s hosts file.

Create Users

The first step in moving to a new server is to create on the destination server the same users that appear on the origin server. For each user on the origin machine, create an equivalent user on the destination machine.

Create Applications

The next step is to recreate applications on the destination server. For each application on the origin server (as noted by the Machine column), create a new application with the same name on the destination server.

Note: Some applications, such as WordPress, may not permit two applications to share the same name. If you encounter this during your migration, create an application with a different name, but remember to use the alternate name when importing database records and creating website entries.

Copy Files

The next step is to copy files from the origin server to the destination server. rsync makes this easy.

1. For each user on the origin server:
   (a) Open an SSH session on the origin machine.
   (b) Get a list of files to be copied. Enter
       \[ rsync -nP-Za ~@/username@destination.webfaction.com: \]
       where username is the current user name and destination is the name of the destination server, and press Enter. A list of files to be copied will appear; no files are copied at this time.
   (c) Verify that the files to be copied are those you intended.
   (d) Copy the files to the destination server. Enter
       \[ rsync -P-Za ~@username@destination.webfaction.com: \]
       (noting that the n switch has been omitted) and press Enter. The files will be copied. Depending on the number and size of the files to be copied, this process may take a few minutes to finish.
2. If applicable, verify that the permissions for your extra users are correct by accessing files with the new extra users you would expect to have access to. If needed, grant access to your extra users

Copy Crontabs

If you have configured or modified your users’ crontabs, the contents of your users’ crontabs must be copied from the origin server to the destination server. For each user:

1. Open an SSH session on the origin server.

2. Export the contents of the crontab to a file. Enter `crontab -l > username_cron`, where `username` is the name of the current user and press Enter. A file, `username_cron`, will be created in the current directory.

3. Copy the file to the destination server. Enter
   
   ```
   scp username_cron username@destination.webfaction.com: 
   ```

   and press Enter. The file is copied to the destination server.

4. Close the SSH session.

5. Open an SSH session on the destination server.

6. Import the crontab. Enter `crontab username_cron` and press Enter.

Create Databases and Database Users

The next step is to recreate the databases and their users on the destination server.

Many application installers create a database automatically. If you have successfully recreated these applications, their databases and users do not need to be duplicated manually.

For all other databases and users, you must recreate each yourself. For each database on the origin server, create a new database on the destination server. For each database user on the origin server, create a new user and grant permissions. Be sure to use the same database names and usernames on the destination server as those on the origin server.

Copy Database Records

Once the databases are set up to receive the data from the origin server, it’s time to export the data from the origin server and import that data to the databases on the destination server.

1. Open an SSH session on the origin server.

2. For each MySQL database on the origin server, dump the contents of the database to a file. Enter
   
   ```
   mysqldump -u username database -p > database.sql
   ```

   where:

   - `database` is the name of the database
   - `username` is the name of a user that owns or has permission to use the database

   and press Enter. A dump file, `database.sql`, is created in the current directory.

3. For each PostgreSQL database on the origin server, dump the contents of the database to a file. Enter
   
   ```
   pg_dump -U username -f database.sql database
   ```

   `database.sql` is created in the current directory.

4. Copy the dump files to the destination server. Enter

   ```
   scp ./*.sql username@destination.webfaction.com: 
   ```

   and press Enter. All `.sql` files are copied to the destination server.
5. Close the SSH session on the origin server.
6. Open an SSH session on the destination server.
7. For each MySQL database on the destination server, import the corresponding dump file. Enter
   `mysql -u username -p -D database < database.sql` and press Enter. The contents of the file are
   loaded into the specified database.
8. For each PostgreSQL database on the destination server, import the corresponding dump file. Enter
   `psql -U username database < database.sql` and press Enter. The contents of the file are
   loaded into the specified database.

Reconfigure Domains

Now it is time to create the environment to test the applications on your migrated server.

To create this environment, you must use the control panel to modify your domain name records such that the
destination server will not be used to serve pages and data (at least not until they’ve been tested).

For each domain in use by the existing origin server websites, configure an A or AAAA record such that the IP
address of the record is set to the IP address of the origin server.

Note: To find the IP address of the origin server:
1. Log in to the WebFaction control panel.
2. Click Account → Services.
3. Review the table’s IP address column.

Create Website Records

The next step is to recreate your website entries.
1. Log in to the WebFaction control panel.
2. Click Domains / websites → Websites. The list of websites appears.
3. For each website entry on the origin server, create a new website entry with the same settings, except for these
differences:
   • in the Name field, enter a unique name;
   • in the Machine field, click to select the destination server;
   • each application added to the site must be the migrated application on the destination server. For example, if `my_wp - origin` were in use in the origin server’s website record, use `my_wp - destination` where destination and origin are the destination and origin servers, respectively.

Test Your Migrated Applications

Now it is time to verify that everything on the new server is working correctly. Because of the DNS changes made
previously, you must reconfigure your computer to use the destination server instead of the origin server for each of
your domains.

Warning: Always create a backup before modifying system files.
1. Open your hosts file in a text editor. Different operating systems store this file in different locations:
   - **Windows**: `%SystemRoot%\system32\drivers\etc\` (typically, `c:\windows\system32\drivers\etc\`)
   - **Mac OS X**: `/private/etc/hosts/` or `/etc/hosts/`
   - **Linux**: `/etc/hosts`

2. For each **A** and **AAAA** record you made previously, add this line to the file:
   
   ```plaintext
   ip example.com
   ```

   where *ip* is the IP address of the destination server (such as `192.0.2.5` or `2001:0db8:85a3:0000:0000:8a2e:0370:7334`) and *example.com* is the domain for which you created the **A** or **AAAA** record.

3. Save and close the file.

Now you can access your websites as they will appear on the destination server. Take the time to verify that each application works as you expect it to. If needed, make any necessary configuration changes to make your new applications work.

For example, you may need to update the port number used in conjunction with some application types, including all custom applications listening on a port. Other applications which require port number changes include:

- mod_wsgi-based applications (such as Django) in their `~/webapps/app_name/apache2/httpd.conf` files
- Passenger-based applications (such as Rails and Redmine) in their `~/webapps/app_name/nginx/conf/nginx.conf` files
- Private MySQL instances in their `~/webapps/app_name/etc/my.cnf` files
- Private PostgreSQL instances in their `~/webapps/app_name/data/postgresql.conf` files
- Pyramid applications in their `~/webapps/app_name/development.ini` files

Only when you are confident the applications on the destination server are working properly should you move on to the next phase of migration.

**Warning:** Once you’re finished testing, don’t forget to revert the changes made to your hosts file.

## Direct Traffic to the New Server

Once you’ve verified that the sites on the destination server are working properly, you may begin directing traffic to the new server.

To direct incoming traffic to the destination server, you must use the control panel to modify your domain name records such that they point to the destination server, instead of the origin server. This is a modification of the domain configuration changes you made previously.

To modify your domain name records:

1. Log in to the WebFaction control panel.
2. Click **Domains / websites → Domains**. The list of domains appears.
3. For each domain:
   - (a) Click on the domain name. The domain’s settings appear.
(b) For each origin server IP address (in other words, for each IPv4 and IPv6 address, as applicable):
   i. Remove the origin server IP address. Click the - (minus) button.
   ii. Click Add IP Address. A field appears.
   iii. In the field, enter the destination server’s IP address.
(c) Click the Save button.

Incoming traffic is now directed to the destination server. To allow time for DNS servers to update their caches, wait 24 hours before continuing to the next step. To confirm that incoming traffic is limited to only the new server, review the origin server log files.

Delete Origin Server Websites

Once traffic has transitioned to the new server, it is safe to remove origin server website records. To remove the origin server website records:

1. Log in to the WebFaction control panel.
2. Click Domains / websites → Websites. The list of websites appears.
3. For each website hosted on the origin server:
   (a) Click on the website’s name.
   (b) Click the Delete button. A prompt, Are you sure you wish to delete the website?, appears.
   (c) To delete the website, click the Yes, I’m sure button. To keep the website (for example, you selected the wrong website), click No, Cancel.

Once you have deleted all of the origin server websites, continue to the next step.

Remove DNS Records

Once you’ve removed the origin server websites, it’s safe to remove the A and AAAA records you made previously.

To remove the A and AAAA records:

1. Log in to the WebFaction control panel.
2. Click Domains / websites → Domains. The list of domains appears.
3. For each domain:
   (a) Click on the domain name. The domain’s settings appear.
   (b) In the Hosting section, click to select WebFaction.
   (c) Click the Save button.

The A and AAAA records are removed.

Finishing Touches

Now that you’ve transitioned traffic to the destination server, it’s time to make any last minute updates and clean up.

1. If needed, copy any new files or migrate any new data from the origin server to the destination server.
2. Reply to your existing support ticket (or open a new ticket) to inform the support team that your migration is complete and you’re ready for your data to be deleted on the origin server.
Congratulations, you have successfully migrated from one server to another.

13.3.4 Migrating from a CentOS 6 Server to a CentOS 7 Server

If you’re migrating from a CentOS 6 server to a CentOS 7 server, please be aware of the following upgrade notes.

General

Many common applications, such as WordPress, Subversion, Static-only and Static/CGI/PHP applications, continue to work without any changes, but others may require changes to run on the newer server. The following sections contain details about specific software and applications.

In our testing, binaries compiled for CentOS 6 continue to work on CentOS 7. Some system libraries may have changed or have been removed, however. If you are running software that depends on such libraries, you may need to recompile on the destination server.

Private MySQL Instances

If you’re running a private MySQL instance, then changes between MySQL versions require that you run an upgrade command. To upgrade a private MySQL instance:

1. Open an SSH session to your account on the destination server.
2. Run the MySQL upgrade command. Enter `mysql_upgrade --protocol=tcp -P port -v -u root -p`, where `port` is the port number assigned to the private MySQL instance, and press Enter. A password prompt appears.
3. Enter the password for the root user and press Enter. You can find the root user’s password in the application’s Extra info field in the control panel.

The database is upgraded.

Private PostgreSQL Instances

If you’re running a private PostgreSQL instance, then changes between PostgreSQL versions require that you complete several migration steps. Some steps must be completed on the origin server (prior to migration). The remaining steps must be completed on the destination server (after migration).

Before migration

Before beginning your migration, make a backup of your private PostgreSQL instance data:

1. Find the origin server’s private PostgreSQL instance’s port number in the control panel.
2. Open an SSH session to your account on the origin server.
3. Enter `/usr/pgsql-9.1/bin/pg_dumpall -h localhost -p port_number > $HOME/webapps/pgsql_app/dumps/dumpall.sql`, where `port_number` is the port assigned to the origin server’s private PostgreSQL instance, and press Enter.
After migration

After migration, upgrade the private PostgreSQL instance’s configuration and reload your data:

1. Open an SSH session to your account on the destination server.
2. Update the PostgreSQL version in the instance’s `bin/start` and `bin/stop` scripts. Enter
   ```bash
   sed -i -e 's/9.1/9.4/' $HOME/webapps/pgsql_app/bin/start,stop
   ```
3. Replace `unix_socket_directory` with `unix_socket_directories` in
   ```bash
   sed -i -e 's/unix_socket_directory/unix_socket_directories/' $HOME/webapps/pgsql_app/pgsql_app/data/postgresql.conf
   ```
4. Rename the existing data directory. Enter
   ```bash
   mv $HOME/pgsql_app/data $HOME/pgsql_app/data.old
   ```
5. Make a new data directory. Enter
   ```bash
   ```
6. Copy the original configuration files from the old data directory to the new data directory. Enter
   ```bash
   cp $HOME/webapps/pgsql_app/data.old/*.conf $HOME/webapps/pgsql_app/data/
   ```
7. Find the destination server’s private PostgreSQL instance’s port number in the control panel.
8. Update the port number in the configuration file. Enter
   ```bash
   sed -i -e 's/port = \[0-9\]+/port = port_number/g' $HOME/webapps/pgsql_app/data/postgresql.conf
   ```
   where `port_number` is the port assigned to the destination server’s private PostgreSQL instance, and press Enter.
9. Start the private PostgreSQL instance. Enter
   ```bash
   $HOME/webapps/pgsql_app/bin/start
   ```
10. Import the dump file you created before the migration. Enter
    ```bash
    psql -h localhost -p port_number postgres < $HOME/webapps/pgsql_app/dumps/dumpall.sql
    ```

The private PostgreSQL instance and its data are migrated.

**PHP**

Versions of PHP prior to PHP 5.4 are neither supported nor installed on CentOS 7 servers. If you’re using PHP, then we recommend that you upgrade to a more recent version of PHP.

Before upgrading, please review the applicable PHP migration guides for your intended PHP version and any intermediate versions:

- Migrating from PHP 5.5.x to PHP 5.6.x
- Migrating from PHP 5.4.x to PHP 5.5.x
- Migrating from PHP 5.3.x to PHP 5.4.x
- Migrating from PHP 5.2.x to PHP 5.3.x
Other upgrade steps may be required by the PHP libraries or application you’re using. Please review their documentation for additional upgrade instructions.

To upgrade to a more recent version of PHP:

1. **Open an SSH session to your account.**

2. Switch to the PHP-based application’s directory. Enter `cd $HOME/webapps/app/`, where `app` is the name of your PHP-based application, and press Enter.

3. Create a `.htaccess` file, if it does not already exist. Enter `touch .htaccess` and press Enter.

4. Open the `.htaccess` file in a text editor.

5. Add the following lines to switch to PHP 5.6:

   ```
   <FilesMatch \.php$>
     SetHandler php56-cgi
   </FilesMatch>
   ```

   Alternatively, you may substitute `php56-cgi` with `php55-cgi` for PHP 5.5 or `php54-cgi` for PHP 5.4.

6. Save and close the file.

**Python**

Versions of Python prior to Python 2.5 are neither supported nor installed on CentOS 7 servers. If you’re using Python, then we recommend that you upgrade your applications to Python 2.7 or later to make it easier to migrate your applications and to enjoy the benefits of bug fixes and security releases.

Compiled Python extensions may not run after migration. Python on CentOS 7 servers is compiled with UCS-4 (UTF-32) instead of UCS-2 (UTF-16); they are not binary compatible. As a result, you may need to recompile extensions to Python. Typically, reinstalling libraries with such extensions (with `pip` or `setup.py`, for example) recompiles the binaries.

CentOS 7’s Python 2.6 does not support the deprecated standard library module `bsddb`. If you’re using Python 2.6 with the `bsddb` module, then we recommend that you upgrade to Python 2.7. If you’re unable to upgrade, then you can install the `bsddb185` library as a substitute for the standard library’s `bsddb` module.

CentOS 7’s Python 2.5 does not support the deprecated standard library module `bsddb`. If you’re using Python 2.5 with the `bsddb` module, then we recommend that you upgrade to Python 2.7.

**Ruby**

Versions of Ruby prior to 1.9 are neither supported nor installed on CentOS 7 servers. If you’re using Ruby, then we recommend that you upgrade to a more recent version of Ruby.

### 13.3.5 Migrating from a CentOS 5 Server to a CentOS 7 Server

If you’re migrating from a CentOS 5 server to a CentOS 7 server, please be aware of the following upgrade notes.
General

Many common applications, such as WordPress, Subversion, Static-only and Static/CGI/PHP applications, continue to work without any changes, but others may require changes to run on the newer server. The following sections contain details about specific software and applications.

In our testing, most binaries compiled on a CentOS 5 server will not run on a CentOS 7 server. Additionally, some system libraries may have changed or have been removed. Typically, you must recompile binaries on the destination server.

Private MySQL Instances

If you’re running a private MySQL instance, then changes between MySQL versions require that you complete several migration steps. Some steps must be completed on the origin server (prior to migration). The remaining steps must be completed on the destination server (after migration).

Before migration

Before beginning your migration, update users’ password hashes to use a more secure algorithm:

1. Find the origin server’s private MySQL instance’s port number in the control panel.
2. Open an SSH session to your account on the origin server.
3. Log in to private MySQL instance as the root user. Enter
   \texttt{mysql -P \textless port\_number \textendash u root \textendash p --protocol=tcp}, where \texttt{port\_number} is the port assigned to the origin server’s private MySQL instance, and press \texttt{Enter}. A password prompt appears.
4. Enter the password for the root user and press \texttt{Enter}.
5. Get a list of users to update. Enter
   \texttt{select user, host from mysql.user where length(password)=16;} and press \texttt{Enter}.
6. For each user and host listed, enter
   \texttt{set password for 'user'@'host' = password('password');} where:
   - \texttt{user} and \texttt{host} are a user name and hostname pair from the previous step and
   - \texttt{password} is the user’s password (you may use an existing or new password)
   and press \texttt{Enter}.

After migration

After migration, upgrade the private MySQL instance:

1. Open an SSH session to your account on the destination server.
2. Run the MySQL upgrade command. Enter
   \texttt{mysql\_upgrade \textendash --protocol=tcp \textendash P port \textendash v \textendash u root \textendash p}, where \texttt{port} is the port number assigned to the private MySQL instance, and press \texttt{Enter}. A password prompt appears.
3. Enter the password for the root user and press \texttt{Enter}. You can find the root user’s password in the application’s Extra info field in the control panel.

The database is migrated.
Private PostgreSQL Instances

If you’re running a private PostgreSQL instance, then changes between PostgreSQL versions require that you complete several migration steps. Some steps must be completed on the origin server (prior to migration). The remaining steps must be completed on the destination server (after migration).

Before migration

Before beginning your migration, make a backup of your private PostgreSQL instance data:

1. Find the origin server’s private PostgreSQL instance’s port number in the control panel.
2. Open an SSH session to your account on the origin server.
3. Enter `/usr/bin/pg_dumpall -h localhost -p port_number > $HOME/webapps/pgsql_app/dumps/dumpall.sql`, where `port_number` is the port assigned to the origin server’s private PostgreSQL instance, and press Enter.

After migration

After migration, upgrade the private PostgreSQL instance’s configuration and reload your data:

1. Open an SSH session to your account on the destination server.
2. Update the PostgreSQL version in the instance’s `bin/start` and `bin/stop` scripts. Enter `sed -i -e 's//usr//usr/pgsql-9.4/' $HOME/webapps/pgsql_app/bin/start,stop` and press Enter.
3. Replace `unix_socket_directory` with `unix_socket_directories` in `~/.postgresql.conf`. Enter `sed -i -e 's/unix_socket_directory/unix_socket_directories/g' $HOME/webapps/pgsql_app/data/postgresql.conf` and press Enter.
4. Rename the existing data directory. Enter `mv $HOME/pgsql_app/data $HOME/pgsql_app/data.old` and press Enter.
6. Copy the original configuration files from the old data directory to the new data directory. Enter `cp $HOME/webapps/pgsql_app/data.old/*.conf $HOME/webapps/pgsql_app/data/` and press Enter.
7. Find the destination server’s private PostgreSQL instance’s port number in the control panel.
8. Update the port number in the configuration file. Enter `sed -i -e 's/port = [0-9]+/port = port_number/g' $HOME/webapps/pgsql_app/data/postgresql.conf`, where `port_number` is the port assigned to the destination server’s private PostgreSQL instance, and press Enter.
9. Start the private PostgreSQL instance. Enter `$HOME/webapps/pgsql_app/bin/start` and press Enter.
10. Import the dump file you created before the migration. Enter

```
psql -h localhost -p port_number postgres < $HOME/webapps/pgsql_app/dumps/dumpall.sql
```

and press Enter.

The private PostgreSQL instance and its data are migrated.

**Python**

Versions of Python prior to Python 2.5 are neither supported nor installed on CentOS 7 servers. If you’re using Python, then we recommend that you upgrade your applications to Python 2.7 or later to make it easier to migrate your applications and to enjoy the benefits of bug fixes and security releases.

Compiled Python extensions may not run after migration. Python on CentOS 7 servers is compiled with UCS-4 (UTF-32) instead of UCS-2 (UTF-16); they are not binary compatible. As a result, you may need to recompile extensions to Python. Typically, reinstalling libraries with such extensions (with `pip` or `setup.py`, for example) recompiles the binaries.

CentOS 7’s Python 2.6 does not support the deprecated standard library module `bsddb`. If you’re using Python 2.6 with the `bsddb` module, then we recommend that you upgrade to Python 2.7. If you’re unable to upgrade, then you can install the `bsddb185` library as a substitute for the standard library’s `bsddb` module.

CentOS 7’s Python 2.5 does not support the deprecated standard library module `bsddb`. If you’re using Python 2.5 with the `bsddb` module, then we recommend that you upgrade to Python 2.7.

**Django**

In addition to changes to Python on CentOS 7 servers, Django applications require a binary and libraries compiled for the destination server after migration (otherwise, an error while loading shared libraries error will occur). To finish a Django application migration:

1. Create an additional Django application of the same version as the migrated application.

2. Update the Django application’s binary and libraries.
   
   (a) Open an SSH session to your account on the destination server.

   (b) Copy the Apache HTTP Server binaries from the additional Django application to the migrated application. Enter

   ```
cp $HOME/webapps/additional/apache2/bin/httpd* $HOME/webapps/migrated/apache2/bin/
```

   where `additional` is the additional Django application and `migrated` is the migrated Django application, and press Enter.

   (c) Copy the contents of the additional Django application’s `modules` directory to the migrated Django application’s `modules` directory. Enter

   ```
cp $HOME/webapps/additional/apache2/modules/* $HOME/webapps/migrated/apache2/modules/
```

   and press Enter.

   (d) Restart the migrated Django application. Enter

   ```
$HOME/webapps/migrated/apache2/bin/restart
```

   and press Enter.

3. Verify that your Django application is now running properly.

4. Remove the additional Django application.
Trac

Migrated Trac applications must be switched over to a newer version of Python for continued Subversion integration; otherwise, a
Can’t synchronize with repository "(default)" (Unsupported version control system "svn": No module named svn)
error will occur. To finish migrating a Trac application to a CentOS 7 server:

1. Modify the Trac application’s CGI file to use Python 2.6.
   
   a) Open $HOME/webapps/tracapp/cgi-bin/trac.cgi, where tracapp is the name of the Trac application, in a text editor.
   
   b) Change the first line of the file from #!/usr/local/bin/python2.4 to 
      #!/usr/local/bin/python2.6.
   
   c) Save and close the file.

2. Move the Trac application’s libraries the new required location.
   
   a) Open an SSH session to your account on the destination server.
   
   b) Remove the symbolic link to the Trac static assets. Enter
      rm $HOME/webapps/tracapp/htdocs
      and press Enter.
   
   c) Move the Trac libraries. Enter
      mv $HOME/webapps/tracapp/lib/python2.4 $HOME/webapps/tracapp/lib/python2.6
      and press Enter.
   
   d) Recreate the symbolic link to the Trac static assets. Enter
      ln -s $HOME/webapps/tracapp/lib/python2.6/Trac-0.12-py2.4.egg/trac/htdocs $HOME/webapps/tracapp/htdocs
      and press Enter.

PHP

PHP-based applications no longer need a symbolic link to a PHP binary nor certain .htaccess directives. For each PHP-based application:

1. Open an SSH session to your account.

2. Switch to the PHP-based application’s directory. Enter
   cd $HOME/webapps/migrated/
   where migrated is the name of the PHP-based application, and press Enter.

3. Open .htaccess in a text editor.

4. Remove the lines that look like this:

   Action php56-cgi /php56.cgi
   AddHandler php56-cgi .php

   The exact lines vary according to the version of PHP (for example, php55-cgi for PHP 5.5).

5. Save and close the file.

6. Remove the symbolic link to the PHP binary that corresponds to the lines removed from the .htaccess file. For example, enter
   rm php56.cgi
   and press Enter.

Versions of PHP prior to PHP 5.4 are neither supported nor installed on CentOS 7 servers. If you’re using PHP, then we recommend that you upgrade to a more recent version of PHP.

Before upgrading, please review the applicable PHP migration guides for your intended PHP version and any intermediate versions:
• Migrating from PHP 5.5.x to PHP 5.6.x
• Migrating from PHP 5.4.x to PHP 5.5.x
• Migrating from PHP 5.3.x to PHP 5.4.x
• Migrating from PHP 5.2.x to PHP 5.3.x

Other upgrade steps may be required by the PHP libraries or application you’re using. Please review their documentation for additional upgrade instructions.

To upgrade to a more recent version of PHP:

1. **Open an SSH session to your account.**
2. Switch to the PHP-based application’s directory. Enter `cd $HOME/webapps/app/`, where `app` is the name of your PHP-based application, and press Enter.
3. Create a `.htaccess` file, if it does not already exist. Enter `touch .htaccess` and press Enter.
4. Open the `.htaccess` file in a text editor.
5. Add the following lines to switch to PHP 5.6:

   ```html
   <FilesMatch \.php$>
     SetHandler php56-cgi
   </FilesMatch>
   ```

   Alternatively, you may substitute `php56-cgi` with `php55-cgi` for PHP 5.5 or `php54-cgi` for PHP 5.4.
6. Save and close the file.

If you’ve migrated from an old server (< web120 or < dweb61) then note that PHP on the new server is served via php-cgi as opposed to mod_php. This means that if you’re using directives such as “`php_value ...`” in some `.htaccess` files you will have to move these to a `php.ini` file.

You can find affected `.htaccess` files by running the following command in a SSH session:

```
egrep -r --include .htaccess '(php_flag|php_value)' ~
```

More information is available in our PHP documentation.

**Ruby**

Versions of Ruby prior to 1.9 are neither supported nor installed on CentOS 7 servers. If you’re using Ruby, then we recommend that you upgrade to a more recent version of Ruby.

**Rails**

In addition to changes to Ruby on CentOS 7 servers, Rails applications require a binary and libraries compiled for the destination server after migration (otherwise, an error while loading shared libraries error will occur). To finish migrating a Rails application to a CentOS 7 server:

1. **Create an additional Rails application** of the same version as the migrated application.
2. Update the Rails application’s binary and libraries.
   (a) Open an SSH session to your account on the destination server.
(b) Copy the nginx file from the additional Rails application to the migrated application. Enter
\[ \text{cp } \text{HOME/webapps/additional/nginx/sbin/nginx} \text{ HOME/webapps/migrated/nginx/sbin/nginx} \]
where additional is the additional Rails application and migrated is the migrated Rails application and press \text{Enter}.

(c) Copy the contents of the additional Rails application’s gems directory to the migrated Rails
application’s gems directory. Enter
\[ \text{cp -R } \text{HOME/webapps/additional/gems/* } \text{HOME/webapps/migrated/gems/} \]
and press \text{Enter}.

(d) Restart the migrated Rails application. Enter \$\text{HOME/webapps/migrated/bin/restart} and press \text{Enter}.

3. Verify that your Rails application is now running properly.

4. Remove the additional Rails application.

13.4 Strengthening Passwords

Various parts of your account require a password, such as SSH and FTP users, mailboxes, databases, and applications. It’s important to create strong passwords to avoid data loss and to preserve your privacy.

Strong passwords are

- difficult for others to guess,
- easy for you to remember, and
- unique.

A strong password needs to be difficult for others to guess. Attackers use various methods to guess passwords, including using widely-available lists of commonly-used passwords. For that reason, avoid dictionary words or common series of numbers in your passwords.

Similarly, attackers may attempt to use publicly-available information about you to guess your passwords. For example, avoid using any form of your birth date in a password, since social media sites often make it easy for others to learn your birth date. Consider what other facts about you may be collected from public sources and avoid using such information in passwords.

A strong password needs to be easy for you to remember. A password written down next to your computer or stored in your email inbox is less secure than one kept secret. If you must record your passwords, use secure password management software, such as KeePass.

Finally, a strong password needs to be unique, so that one compromised password does not cause more than one system to be compromised. Avoid reusing passwords.

13.4.1 Password Requirements

In an effort to improve the strength of passwords, WebFaction imposes some requirements on user account and other passwords. New passwords need to meet the following requirements:

- The password must not be a dictionary word.
- The password must not be too simple or systematic. For example, 123456789 or qwertyuiop are unacceptable passwords.
- The password must not be a previously used password.
• The password must not be closely similar to a previously used password. Closely similar passwords include those with only minor differences from previous passwords (such as a single character difference) and those which are palindromes, rotations, or case changes of previous passwords.

• The password must be longer than six characters.

The password may contain any ASCII character, including alphanumeric characters and special characters (like !@#$%).

13.5 Payment Card Industry Data Security Standard (PCI DSS) Compliance

PCI DSS is a security standard for organizations which handle card and cardholder data.

13.5.1 WebFaction Servers and Compliance

All WebFaction servers are designed to pass PCI security scans. If your website is implemented such that no vulnerabilities are introduced, a PCI security scan of your domain should pass. That said, there is more to PCI DSS compliance than passing a security scan. PCI DSS compliance depends heavily on the PCI merchant compliance requirements imposed for your organization.

Note: There is considerable disagreement among security professionals about how PCI DSS applies to web hosts. Furthermore, there is little clarification from the PCI Security Standards Council. As a result, you may see advice from other web hosts describing different requirements. This document can only be our recommendation, not an official determination, regarding PCI DSS compliance. Ultimately, the only official determination of what is required for your PCI DSS compliance is your payment service provider.

13.5.2 PCI DSS Merchant Classification

PCI DSS classifies merchants into several different levels and types based significantly on transaction volume and card handling methods. The various levels and types determine the manner and frequency of security audits and scans.

For most merchants, security audits take the form of a self-assessment questionnaire (SAQ) and quarterly security scans of any computers which handle card data. Be wary of web hosts who claim that their hosting is PCI compliant without specifying which levels, types and parts of compliance. Passing the security scans are only a portion of compliance.

13.5.3 Determining Your Needs

To determine your PCI DSS compliance needs, first you must contact your payment provider to find out whether you need a full independent assessment or if you are eligible for a self-assessment. Most merchants will be eligible to complete the self-assessment process, but some merchants, particularly those that process a very large volume of transactions or have previously suffered a security breach, will need to have an independent third party, a Qualified Security Assessor (QSA) carry out the audit.

If you are required to have a QSA carry out your audit, you should contact your payment provider or QSA for recommendations and how to proceed.

If you are not required to have a QSA carry out your audit, you must determine your SAQ validation type and, thus, which SAQ type (labeled A-D), you must complete.
13.5.4 Self-Assessment Questionnaires

Merchants operating websites typically must concern themselves with SAQ A, C, or D.

SAQ A

If you are eligible to complete SAQ A, then you probably will not be required to complete any security scans. You can use any of our plans and remain PCI DSS compliant.

SAQ C

If you must complete SAQ C then WebFaction hosting will be within the scope of compliance. All of our servers will pass the security scans associated with this SAQ. We cannot guarantee that they will pass on the first test, because it depends also on the design and implementation of your site, but WebFaction servers are set up such that a scan is not prevented from passing.

That said, passing the security scan is only part of the compliance process. The other part is answering Yes to every question in the questionnaire. We do not believe that it is possible for any shared or VPS host to be compliant with SAQ C as it is currently written, even if it passes the security scan.

For example, one SAQ C question is, Is access to system components and cardholder data limited to only those individuals whose jobs require such access? It it not clear how that question applies when multiple independent users share the same physical hardware. Under a strict reading of the question you would be forced to answer No.

Additionally, some payment service providers want a scan of every domain which points to the same physical server. In a shared or VPS hosting environment, there could be hundreds of domains belonging to dozens of users all pointing to the same physical server. Meeting such a requirement is not feasible. You must determine what your payment service provider requires and how it applies to shared hosting.

If you are required to complete SAQ C, you have these options:

- If possible, change the way you process card payments to become eligible for SAQ A.
- Use PCI DSS Compensating Controls. If you do not meet one or more requirements but put other controls in place which meet the rigor and intent of the original requirements, you may still be compliant. You must discuss with your payment service provider what controls they consider acceptable.

SAQ D

SAQ D is the highest level of PCI DSS compliance and is significantly more stringent than SAQ C. Becoming PCI DSS compliant to to this level should not be undertaken lightly. We do not think WebFaction’s service can provide such a level of compliance.

If there is a way for you to become PCI DSS compliance by SAQ C rather than SAQ D, you should.

13.6 Using Multiple Servers

Most WebFaction accounts use a single server, where all of the account’s applications, databases, and files are stored and served from one web server. Under some situations, however, it may be beneficial to operate from two or more servers. This special topics guide describes when you might need an additional server, how to add one to your account, and how to put the additional server to work.
13.6.1 Choosing to Add a Server

There are two common reasons to add a server to your account: load balancing and consuming more memory than one web server can provide.

If your account is host to a high-load website, you may choose to add an additional server to your account. Rather than seeing your site slow down due to the bottleneck of a single web server, you can opt to spread the load across more than one machine. With an additional machine, you can use round-robin DNS load balancing: each incoming request is directed to one of your account’s web servers in turn. While it is not automatic failover or load-aware load balancing, this approach is simpler than many alternatives and often alleviates problems with high load websites.

On the other hand, if you account is host to many applications, you may find that you need more memory than a single server can provide. You can add an additional web server to your account to run more applications.

13.6.2 Adding an Additional Server

If you’ve decided you need an additional web server, you can request an additional plan on a different server through the control panel. You can add additional machines as needed under a single account; you do not need to start a new account to make use of more than one server.

To request an additional web server:

1. Log in to the WebFaction control panel.
2. Click Account → Add or remove plan. The Upgrade, Downgrade or change your services form appears.
3. In the field, enter your request. For example, enter Please add a shared hosting plan on a different web server to this account.
4. Submit your request. Click Request service change.

Our support team will respond to your upgrade request shortly. To see the additional service on your account once your upgrade request has been processed:

1. Log in to the WebFaction control panel.
2. Click Account → Services. The list of services associated with your account appears.

Once added, your additional plan appears in the list.

13.6.3 Configuring an Additional Server

Once you have an additional server provisioned to your account, you can immediately configure it for your use. The control panel displays the servers available to your account when creating applications, websites, and database; you will also have SSH access to the additional server.

Using an Additional Server for Load Balancing

To load balance a website across two or more servers, you must replicate the application(s) and website(s) records on the additional web server with the control panel:

1. Create duplicates of the application(s) to migrate on the additional web server.
2. Copy database records to the additional server.

**Note:** Database replication and synchronization is not provided.

3. Create duplicates of the website records on the additional server.
Using an Additional Server to Host Additional Applications

To use your additional server to host additional applications:

1. *Create an application on the additional web server.*
2. *Create a website record on the additional web server.*
Symbols
2FA, 6

A
Accounts, 16
Cancellations, 24
Add-ons, 17
Affiliates, 22
Android 4.3 (Jelly Bean)
Email client, 63
Android 4.4 (KitKat)
Email client, 64
Android 5.0 and 5.1 (Lollipop)
Email client, 68
Apple Mail, 54, 59
Applications, 33
Create, 34

B
Backups, 16
Bandwidth consumption, 18

C
Certificates, 38
Add a certificate, 39
Renew a certificate, 40
Use a certificate, 40
Contact information, 18
Control panel, 4
Change password, 5
Log in, 5
Recover password, 6
Two-step login, 6

D
Databases, 115
Back up, 126
Command line, 120
Connection details, 119
Creating, 117
Delete, 127
Export, 125
Import, 126
phpMyAdmin, 119
phpPgAdmin, 120
PostgreSQL procedural languages, 128
Remote access, 121
Shell, 120
SSH tunnel, 121
Users, 117
Disk consumption, 18
DNS, 27
A, 28
CNAME, 28
MX, 28
 Overrides, 27
Records, 27
Servers, 25
SPF, 29
SRV, 30
Troubleshooting, 30
TXT, 30
Domains, 24
Add, 26
DNS records, 27
DNS servers, 25
Name servers, 25, 26
Troubleshooting, 30
DSS, 161

E
Email, 45
Address, 47
Agents, 51
Autoresponder, 108
Change mailbox password, 48
Create address, 49
Create mailbox, 47
Filtering, 107
Forwarding, 108
Google Apps, 114
Limitations, 113
Lists, 113
Mailbox, 47
Mailing lists, 113
Script, 112
Spam, 109
Webmail, 106
Email client, 51
Agents, 51
Android 4.3 (Jelly Bean), 63
Android 4.4 (KitKat), 64
Android 5.0 and 5.1 (Lollipop), 68
Apple Mail, 54, 59
fetchmail, 51
getmail, 52
Gmail, 72
iOS 7, 69
iOS 8, 70
iOS 9, 71
iPad, 69–71
iPhone, 69–71
iPod Touch, 69–71
Mac OS X, 53
Mail, 54, 59
Mail.app, 54, 59
Microsoft Outlook 2007, 77
Microsoft Outlook 2010, 83
Mobile, 63
Mozilla Thunderbird, 90
Mozilla Thunderbird (Mac OS X), 61
msmtp, 53
Other clients, 105
Outlook 2007, 77
Outlook 2010, 83
Outlook.com, 74
Settings, 105
Thunderbird, 90
Thunderbird (Mac OS X), 61
Web clients, 71
Windows 8 Mail, 104
Windows clients, 77
Windows Live Mail, 92
Windows Mail, 97
fetchmail, 51
File permissions
File permissions, 15
FTP, 13
FTP, 14
Clients, 13
Password, 14
Users, 14
getmail, 52
Gmail, 72
Google Apps, 114
Help, 131
HTTPS, 38
IMAP, 105
Invoices, 22
iOS 7
Email client, 69
iOS 8
Email client, 70
iOS 9
Email client, 71
iPad
Email client, 69–71
iPhone
Email client, 69–71
iPod Touch
Email client, 69–71
Logs, 41
Mac OS X
SSH, 11
Mail, 54, 59
Mail.app, 54, 59
Mail2script, 112
Mailbox, 47
Change password, 48
Create, 47
Mailing lists, 113
Mailman, 113
Microsoft Outlook 2007, 77
Microsoft Outlook 2010, 83
Mozilla Thunderbird, 90
Mozilla Thunderbird (Mac OS X), 61
msmtp, 53
Multiple servers, 162
my.webfaction.com, 4
Outlook 2007, 77
Outlook 2010, 83
Outlook.com, 74
Password
FTP, 14
SSH, 14
Passwords, 160
Payment Card Industry Data Security Standard (PCI DSS), 161
Payments, 19
  History, 22
  Invoices, 22
  Make a payment, 20
  Sources, 21
PCI, 161
PCI DSS, 161
phpMyAdmin, 119
phpPgAdmin, 120
Plans, 17
POP, 105
PuTTY, 12

Q
Q&A Community, 133

R
Registration, 25
Roundcube
  Mobile, 106

S
Server details, 7
  IP address, 10
  Name, 9
  Operating system, 9
Server migration, 144
  CentOS 5 to CentOS 7, 154
  CentOS 6 to CentOS 7, 152
SMTP, 105
Spam, 109
SSH, 11
  Keys, 11
  Linux, 11
  Mac OS X, 11
  Password, 14
  PuTTY, 12
  Troubleshooting, 13
  Users, 14
SSL, 38
Support, 131
  Tickets, 133

T
Thunderbird, 90
Thunderbird (Mac OS X), 61
Tickets, 133
Two-factor authentication, 6
Two-step login, 6

U
Usage Quotas, 128
Users, 15

Index 167