

---

***NTT/VERIO***

**Shadowing to VPS v2**  
**Administrator's Guide**

**First Edition**  
**October 2005**

---

# Table of Contents

**Introduction ..... 1**

- Executive Summary ..... 1
- Overview of the Process ..... 1
- Process Timeline..... 2
- Regarding Specialized Configurations ..... 2

**Prior to Initiating a Shadow Account ..... 3**

- Becoming Familiar with the Shadow Process..... 3
- Becoming Familiar with FreeBSD..... 3
  - Using FreeBSD Directory Structure ..... 3
  - Using FreeBSD User Permissions ..... 4
  - Accessing the FreeBSD General Commands Manual..... 6
- Using the Backroom ..... 6
- Requesting an Audit of the Shadow Process ..... 7
- Saving FrontPage Web Content..... 9

**Using your Shadow Account..... 9**

- Initiating your Shadow Account..... 9
- Using the Backroom of your Shadow Account ..... 10
  - Recopying Content to the Shadow Account ..... 11
    - Regarding POP..... 12
    - Regarding IMAP ..... 12
  - Changing DNS Settings ..... 13
  - Reversing Changes to DNS Settings..... 13
  - Completing the Shadow ..... 14
  - Canceling the Shadow..... 14
- Connecting to your Shadow Account ..... 14
  - Using SSH to Connect ..... 14
  - Using FTP to Connect..... 15
- Issuing Shadow-Related Commands and Functions ..... 16
- Other Shadow-Related Commands..... 17
- Controlling Access to your Shadow Account ..... 18
- Managing Groups ..... 18
- Vinstall Additional Add-Ons ..... 18
- Perl Modules ..... 19
- Installing FrontPage Server Extensions ..... 19

**Before Terminating your Previous VPS Account ..... 21**

- Verifying Web Site Configurations ..... 21
- Verifying your Email Settings ..... 22
- Verifying Urchin Web Analytics ..... 22
- Moving Your Digital Certificate..... 23
- Finalizing the Shadow Process ..... 23

**Taking Note of Special Concerns ..... 24**

**Notices..... 26**

**Document Conventions ..... 27**

## Table of Tables

Table 1: Files Created on your Shadow Account .....	4
Table 2: User Permission Bits .....	4
Table 3: User Permission Bit Combinations.....	5
Table 4: Backroom Options located in the Backroom.....	7
Table 5: Backroom Options Available in your Shadow Account.....	11
Table 6: Shadow-Related Functions which Modify vmigrate .....	17
Table 7: Other Shadow-Related Commands.....	18
Table 8: Verifications and Guidelines for your Web site .....	22
Table 9: Taking Note of Special Concerns .....	25

# Introduction

Using the instructions included in this document and by applying your previous Virtual Private Server (VPS) experience, you can conduct a self-migration (referred to as a *shadow process*) from FreeBSD VPS version one (VPS v1) to VPS version two (VPS v2). By means of a shadow process, you can conduct this on your own and without extensive technical support. This introduction provides you with an executive summary, an overview of the shadow process, a process timeline, and a note regarding specialized configurations.

## Executive Summary

Support for VPS v2 began in May 2003. Since that time, account owners and their clients have utilized the enhanced control, flexibility, and secure isolation provided by VPS. For example, VPS v2 adheres more closely to the UNIX-style FreeBSD operating system than previous versions. This increases the amount of knowledge an administrator can transfer from other FreeBSD operating system environments.

Although previous versions of VPS are available for purchase, VPS v2 provides you with support for newer features and enhancements. This is true not only for the features VPS provides to manage users and content but also for external, open source database, scripting, mail, and Web analytics. Improvements to the process of moving to VPS v2 decrease the time an administrator must invest to learn a customized VPS operating system.

## Overview of the Process

The current shadow process addresses the following areas of your VPS account in a largely automated fashion with a high level of reliability:

- Multithreaded, multi-user Structured Query Language (MySQL) open source database
- PHP: Hypertext Preprocessor (PHP) open source scripting
- Sendmail open source mail transfer agent (MTA)
- Urchin Web analytics
- User administration
- Content management

This document provides you with information about options included in the Web Hosting Backroom (referred to as the *Backroom*) of your VPS account. It also describes the special purpose directories, files, and commands included in your shadow account.

The shadow process to a VPS v2 account begins when you initiate a shadow to your previous VPS account. For the duration of the shadow process, you have two VPS accounts. At the end of the shadow process, it is your previous VPS account which terminates. At that point, you shadow account becomes the single VPS account and that account utilizes all of the features and benefits of VPS v2.

Initiate the process is through the Backroom of your VPS account. Within 24 hours after you have successfully established a shadow account, you receive a shadow activation notice by email. Your shadow account includes all content from your previous VPS account configuration.

## Process Timeline

The duration of your shadow account is up to 21 days. During that time, there are up to four sets of tasks to perform, as follows:

- Configure content, settings, and applications
- Test all content, settings, and applications
- Update DNS
- Complete the shadow

Following a shadow activation email, you receive additional email notifications to remind you of these tasks, seven and fourteen days after you initiate the shadow account.

After you configure and test all content settings, and applications, you update DNS for all domains associated with your VPS account and serviced by the `secure.net` name servers such as `ns1.secure.net` and `ns2.secure.net`.

**Note:** If `secure.net` does not service your domain names, you must update your DNS to point to the IP address of the shadow account. You receive email notifications to remind you of these tasks 18 and 19 days after you initiate the shadow account.

At any time within 21 days of initiating the shadow account and conducting the shadow process, you can complete the process. Completing the process terminates your previous VPS account. You receive email notifications to remind you to complete the process 20 and 21 days after you start the shadow account.

## Regarding Specialized Configurations

The automated portion of the shadow process is sufficient for most VPS account configurations. When you initiate the shadow process, a VPS v2 account is automatically provided for this purpose. The automated portion of the process creates a shadow account with same administrative user (Admin User) as the previous VPS account and adds a root user. The root and account owner passwords are the same as for the previous VPS account owners.

This document does not address issues associated with a highly customized VPS account configuration including significant changes to the file and naming structures as well as services of a VPS account. The shadow process, Backroom options and menu-driven commands automate a large part of your shadow to VPS v2. However, as the capabilities of the VPS account allow for multiple configuration options and there are items which the commands cannot perform, you may need to perform additional steps. For your highly customized configurations, plan time to manually configure some features. For example, there is no automated shadow process for Miva Merchant. The Backroom of your VPS account includes an audit option you can use to determine the number of items to configure manually.

## Prior to Initiating a Shadow Account

This section familiarizes you with the shadow process and the FreeBSD operating system. It also provides you with an overview of shadow-related options available in the Backroom. Finally, you can use the information provided by this section to request an audit of the shadow process for your individual configuration.

### Becoming Familiar with the Shadow Process

You must familiarize yourself with the following information prior to initiating the shadow process:

- “Taking Note of Special Concerns” on page 24.
- The *Virtual Private Server Handbook*.
- The *FreeBSD General Commands Manual*.

**Note:** The *Virtual Private Server Handbook*, in a portable document format (PDF), is accessible from the Backroom. For more information about how to access the FreeBSD General Commands Manual, see “Accessing the FreeBSD General Commands Manual” on page 6.

### Becoming Familiar with FreeBSD

This section provides you with information about using the FreeBSD directory structure and user permissions. In addition, this section refers you to additional resources to know more about FreeBSD.

#### *Using FreeBSD Directory Structure*

You must familiarize yourself with the differences in the way your shadow account (and by extension your new, VPS v2 account) organizes the files and directories. Your previous versions VPS account mounts all directories from the following root (or *home*):

```
/home/login  
/home/login/path/to/file
```

Your shadow account, just as your previous VPS account, utilizes a file structure the follows that of FreeBSD, a UNIX-style operating system. However, your shadow account mounts all directories from a *root* directory appearing as a single forward slash character (/). This means that as you configure shadow account content, settings and applications, do not use the tilde character (~) to represent virtual path to an actual root. For example, what you configure as *~/path/to/file* for your previous VPS account must appear as follows for your shadow account:

```
/path/to/file
```

The operating system provides mount points, directories where you add additional file systems can be onto the root file system.

Initiating a shadow account creates the following files and directories on your shadow account:

File/Directory	Description
<code>/.migrate</code>	Directory where the shadowing process automatically places content and data from your previous VPS account.  <b>Caution:</b> Do not edit the content of the <code>/.migrate</code> directory.
<code>/.migrate/accountname</code>	A subdirectory of <code>/.migrate</code> containing a copy of the file system from your previous VPS account.
<code>/.migrate/bin</code>	A subdirectory of <code>/.migrate</code> containing binary files from your previous VPS account. User utilities fundamental to both single-user and multi-user environments.
<code>/.migrate/bin/vmigrate</code>	A menu-driven command located in <code>/.migrate/bin</code> . Use the <code>vmigrate</code> command to place the content and data from your previous VPS account. Using this command, you can choose the extent to which the shadow process is an automated or a manual one.
<code>/var/log/vmigrate</code>	Contains a log of changes made by the automated portions of the shadow process.

**Table 1: Files Created on your Shadow Account**

## Using FreeBSD User Permissions

UNIX provides a basis for FreeBSD, a multi-user operating system. FreeBSD enables several users to work simultaneously on unrelated tasks. The operating system enables you to configure your VPS account so that these users' requests can share hardware devices, peripherals, memory and processing capacity.

The FreeBSD directory uses a directory structure that includes control of the permissions you grant to *users*, *groups*, and *everyone else* (neither users nor groups). The structure enables you to configure permissions for users and groups. Control user access by configuring permissions to your precise needs.

The following table describes user permission bits and the abilities they specify for each user.

Permission Bit	Specifies
<code>r</code>	User can read files
<code>w</code>	User can write to files
<code>x</code>	User can execute files.
en dash (-)	A null value, no permission granted for the ability.

**Table 2: User Permission Bits**

The following table provides you with a guide to permission combinations you can issue to users, groups, and users.

Permission	Directory listing
No read, no write, no execute	---
No read, no write, execute	--x
No read, write, no execute	-w-
No read, write, execute	-wx
Read, no write, no execute	r--
Read, no write, execute	r-x
Read, write, no execute	rw-
Read, write, execute	rwX

**Table 3: User Permission Bit Combinations**

Following is an example of a typical setup for permissions on a user file, including group permissions:

```
rw-r--r--
```

In the previous example, *rw* specifies read (*r*) and write (*w*) permissions for the owner of the file. The group and others have read and null permissions (*r--*). This way, the group and others cannot write to the owner's file.

Use the `ls -l` command line argument to see a directory listing including a column with information about a file's permissions for the owner, group, and everyone else. Issuing an `ls -l` command line argument in a directory may show results as in the following:

```
% ls -l
total 530
-rw-r--r-- 1 root  wheel   512 Sep  5 12:31 myfile
-rw-r--r-- 1 root  wheel   512 Sep  5 12:31 otherfile
-rw-r--r-- 1 root  wheel 7680 Sep  5 12:31 email.txt
...
```

You can use the `chmod` utility to change permissions. For more information about the `chmod` utility, refer to the *FreeBSD General Commands Manual*.

## Accessing the FreeBSD General Commands Manual

You can access a version of the *FreeBSD General Commands Manual*, often referred to as a set of *man pages* several ways. You can run `man` command on your VPS account command prompt, as follows:

```
yourv2 ~> man command
```

```
BUILTIN(1)                FreeBSD General Commands Manual
BUILTIN(1)

NAME
    builtin, alias, alloc, bg, bindkey, break, breaksw, builtins, case,
    cd,
    chdir, command, complete, continue, default, dirs, do, done, echo,
    echotc, elif, else, end, endif, endsw, esac, eval, exec, exit,
    export,
    false, fc, fg, filetest, fi, for, foreach, getopts, glob, goto, hash,
    hashstat, history, hup, if, jobid, jobs, kill, limit, log, lo88gin,
    logout,
    ls-F, nice, nohup, notify, onintr, popd, printenv, printf, pushd,
    pwd,
    read, readonly, rehash, repeat, sched, set, setenv, settc, setty,
    setvar,
    shift, source, stop, suspend, switch, telltc, test, then, time, trap,
    true, type, ulimit, umask, unalias, uncomplete, unhash, unlimited,
    unset,
    unsetenv, until, wait, where, which, while - shell builtin commands

SYNOPSIS
    builtin [-options] [args ...]

DESCRIPTION
    Shell builtin commands are commands that can be executed within the
    run-
    ning shell's process.
```

Also, you can access the manual on the World Wide Web at <http://www.freebsd.org/>, as well as other locations on the Web.

## Using the Backroom

In the Backroom, there are two shadow-related options. One of the options assists you with the process of determining the extent to which the process of moving to VPS v2 is automated for your account configuration. Once you determine to make the change to VPS v2, the other option enables you to start that process.

**Note:** There is no other way to initiate the shadow account (`s`). There are not any supported commands, functions, or scripts available from the root directories that provide an equivalent to these options in the Backroom.

The following table describes the options available in the Backroom:

Option	Purpose
Perform Audit	Performs an analysis (or <i>audit</i> ) of benefits of an automated shadowing process for your VPS account.
Shadow Selected Account	Creates shadow accounts you can configure a new, VPS v2 accounts. You select one or more accounts to shadow as well as a physical location where the shadow account resides. The shadow accounts provide you with a 21-day period in which to configure your VPS v2 accounts.

**Table 4: Backroom Options located in the Backroom**

## Requesting an Audit of the Shadow Process

The Backroom provides you with an option designed to assist you with an analysis of what to expect from the shadow process, specifically for your account. The report is an estimate designed to help you gauge the number of tasks you perform.

The Shadow Analysis option provides you with an analysis (or *audit*) of benefits of an automated shadowing process for your VPS account. The audit reports which of the configurations and contents automated commands can shadow in an automated fashion. The audit also reports which of the configurations and contents you must plan to handle in a manual fashion.

**Note:** You must make certain to verify that any of the CGI binary files, in particular the executable contents, function correctly on the VPS v2 account. These files are less likely to migrate in a highly automated fashion.

The information arrives as an email. In the Backroom, provide the email where you prefer to receive the audit report. If you do not specify an address, the report is delivered to your default contact email address.

Prior to initiating the shadow process, follow these steps to locate the audit option and to analyze the shadow process for the VPS account you specify:

**Note:** By default, this option delivers the results of its audit to the email address included as the administrative email address. The option also includes a field for you to specify another email to send the report to.

1. Start your Web browser to access the Backroom.
2. Type the correct username and password and press **Login**.
3. Verify your account contact email address is correct. If it is not, correct it immediately.
4. Click **Administrative Interface**.
5. Select the previous VPS account you wish to shadow to VPS v2.
6. Click **Upgrade to VPS v2**.
7. Select **Perform Audit** and enter an email address (or leave the email address field blank in order to send to the account contact email address).

The following example provides a sample of the information emailed following a successfully requesting an audit.

Dear Customer,

Below is an assessment of your VPS v1 account.

This report is an estimate of which configurations and content can be migrated using our migration scripts, and which configurations would need to be migrated manually by you.

Please note this report is only an estimate and is provided to help you gauge the amount of work that would be required to migrate this account from VPS v1 to VPS v2.

----- VPS v1 ACCOUNT DETAILS -----

User/login: example  
 Domain/hostname: example.example.net  
 Current Disk Usage: 7.8meg out of a total 1095.7meg

----- E-MAIL CONFIGURATION DETAILS -----

1 hostnames can be configured on the new server:  
 Host: example.example.net

----- SUB-USER DETAILS -----

----- SERVICES/APPLICATIONS ASSESSMENT -----

The following items were identified as configurations that CANNOT be migrated using our migration scripts.

You will have to manually migrate these applications.

Installed: Urchin Web Statistics - ## Can not migrate ##  
 Version: 3.404  
 Base: /usr/local/urchin3404crlid  
 Link: Linked to /usr/local/urchin  
 Reason: Licensing issues

If you have used 'vinstall' to add software to your server, you are advised to vinstall the same packages after migrating to VPS v2.

----- WEB SERVER CONFIGURATION ASSESSMENT -----

3 Web VirtualHosts will be moved:

VirtHost: user1.example.net  
 Admin: example@example.net  
 Home: /home/example/www/user1.example.net/htdocs  
 cgi-bin: /cgi-bin/  
 -> "/home/user1/www/user1.example.net/cgi-bin/"

VirtHost: user2.example.net  
 Admin: example@example.net  
 Home: #/home/example/www/user2.example.net/htdocs  
 cgi-bin: /cgi-bin/  
 -> "/home/user2/www/user2.example.net/cgi-bin/"

VirtHost: user3.example.net  
 Admin: example@example.net  
 Home:  
 cgi-bin: /cgi-bin/  
 -> "/home/user3/www/user3.example.net/cgi-bin/"

Some manual intervention may be required for CGI programs. Each CGI should be examined and then thoroughly tested in the VPS v2 environment.

Apache Modules loaded in configuration:  
 Module: mod\_frontpage.so

In order to continue using FrontPage server extensions and to transfer FrontPage web content to your new VPS v2, you will need to perform the following tasks manually:

- save each FrontPage web to a local computer.

- install FrontPage server extensions on your VPS v2 shadow account.
- publish each FrontPage web to your shadow account.

----- FINAL NOTES -----

You can begin the migration process for this account in the Backroom  
[https://mybackroom.securesites.com/customer/backroom/account\\_info/](https://mybackroom.securesites.com/customer/backroom/account_info/)

We *strongly* recommend reviewing all migration documentation before migrating. In addition, we recommend familiarizing yourself with the architecture of VPS v2, since there are many common features, such as virtual subhosts, user permissions, file ownership, etc., that function very differently on VPS v2.

## Saving FrontPage Web Content

**Caution:** Although your previous VPS account includes installed server extensions, you must install a new set of server extensions to the shadow account. Otherwise, any Web site (or FrontPage Web) you publish does not function correctly on the shadow account. Prior to initiating a shadow account, save your FrontPage Web content to a local resource.

VPS accounts support the Microsoft FrontPage Web site creation and management program. A FrontPage Web requires server extensions which support the following functions:

- Multi-user authoring
- Remote authoring
- Web site forms
- Discussion Webs
- Full text search capability
- Hit counters

The Shadow Analysis option reviews the content of your previous VPS account to confirm any installed Microsoft FrontPage server extensions the program requires.

When you determine to move FrontPage Web content from on your previous VPS account, there are several steps to take. First, save (or *publish*) the FrontPage Web to a local computer, one without association with your previous VPS account. Later, after you initiate a shadow account, install server extensions to the shadow account. After that, publish the FrontPage Web to your shadow account.

## Using your Shadow Account

The Backroom of your shadow account provides you with five shadow-related options. The shadow account also enables you to issue a specific set of commands and functions. These commands and functions place the configuration information from your previous VPS account to the correct directories and files of your VPS v2 account.

This section provides information about initiating your shadow account, using the Backroom of your shadow account, connecting to your shadow account, issuing shadow-related commands and functions, other shadow-related commands, controlling access to your shadow account, managing groups, `vinstall` add-ons, and Perl modules.

## Initiating your Shadow Account

The Backroom includes a Shadow Selected Account option which initiates a shadow process for the VPS account(s) you select. After you initiate the process, look for an email

including the login name, server host, and IP address for a special-purpose VPS account (also called a *shadow account*).

Follow these steps to locate the Shadow Selected Account option and to initiate a shadow account:

1. Start your Web browser to access the Backroom.
2. Type the correct username and password and then press **Log in**.
3. Verify your account contact email address is correct. If it is not, correct it immediately.
4. Select the VPS v1 account(s) you wish to shadow to VPS v2.
5. Select **Review**. The Account Information Interface appears.
6. Select a VPS v2 server location. For example, you can select as *VPS v2 Standard – Dulles, VA FreeBSD VPS v2*.
7. Select **Shadow Selected Account**.
8. Look for email confirming the following information for your shadow account(s):
  - *login name*
  - *server host*
  - *IP address*

The following is an example of the information emailed after successfully establishing a shadow account.

```
** This letter contains important account migration information!**  
** Please retain a cop of this letter for future reference.**  
Example, John  
example123
```

```
The shadow account example1234 you ordered on 99 June 2099 has been  
configured for your use.
```

```
...  
Shadow Account Information  
Login Name (Admin User): example1234  
Server Host: exm-ex00123  
IP Address: 128.222.33.4444
```

```
Original Account Information  
Login Name: example1234  
Server Host: exm-ex00123  
Hostname (Domain Name): example1234.tempdomainname.com
```

```
It is your responsibility to complete the following steps within the next  
21 days:
```

```
...
```

## Using the Backroom of your Shadow Account

The Backroom of your shadow account provides you with options you can use to recopy content from your previous VPS account, to update DNS on your shadow account, to return to previous DNS settings, to complete the process, and to cancel the shadow account. This section provides information about using the Backroom of your shadow account. The options provide you with the ability to recopy content, change DNS settings, reverse changes to DNS settings, completing the shadow process, and canceling the shadow process.

The following table provides an overview of the shadow-related options located in the Backroom of your shadow account.

Option	Purpose
Recopy Content	Copies all content from your previous VPS account and places the copy in a <code>/.migrate</code> directory on your shadow account. For details, see “Recopying Content to the Shadow Account” on page 11.
Update DNS	Update DNS is a time-sensitive option. It provides functions which would otherwise occur automatically and without your input. If you never select this option, you receive an email notification when the update is going to occur. And if you do not need to speed up (or slow down) the process, you can simply wait for the shadow account process to make the update automatically. For details, see “Changing DNS Settings” on page 13.
Revert DNS	This option reverses DNS updates you initiated the last time you used Update DNS. For details, see “Reversing Changes to DNS Settings” on page 13.
Complete Shadow	This option concludes the shadow process. All content is removed from your previous VPS account. Once you select this option, you cannot revive the previous account or return to that configuration. For details, see “Completing the Shadow” on page 14.
Cancel Shadow	Use this option to cancel the shadow account and ends the shadow process. This option cancels the process and does not begin or finish any further shadow tasks. As this option terminates your shadow account, any configuration on that account is lost. For details, see “Canceling the Shadow” on page 14.

**Table 5: Backroom Options Available in your Shadow Account**

## Recopying Content to the Shadow Account

The Recopy Content option, located in the Backroom of your shadow account, copies all content from your previous VPS account and places the copy in a `/.migrate` directory on your shadow account.

**Note:** Before you select Recopy Content, verify that you have sufficient disk space available. If you previously copied all content then migrated that content to the correct directories, selecting Recopy Content means that you are utilizing as much as two times the disk space your previous account required. When you select Recopy Content you could potentially overwrite modifications you made to the configuration of your shadow account. Any changes you made to customize the mail, Web content, or databases on your shadow account are lost when you select this option.

If you are concerned about recent email, Web content, or databases now located on your previous VPS account run the menu-driven `vmigrate` command and the specific functions in order to move that newer content to your shadow account

For example; email content can accumulate during the shadow process. Use this option to place the most current email content on your shadow account.

**Note:** Rather than overwriting mail files from the time you first initiated your shadow account, the Recopy Content option adds current `users` information in the `/.migrate` directory and appends it with a marker (`_v1`). Each subsequent time you use the

Recopy Option, the information from the time you initiated your shadow account continues to be retained this way. Only user information appended with the `_v1` marker is ever overwritten.

After using the Recopy Content option, issue the `vmigrate 1) users` command. Doing this moves users' current information, including their mailbox information, to the correct directories and files in your VPS v2 account. The `vmigrate 1) users` command retains it and adds the more current information appended with a marker (`_v1`). This is true for each subsequent time you recopy.

In addition to adding a suffix to the information, the Recopy Content option also places the information in different directories than when you first run the `vmigrate` command. The content is handled differently, depending on whether your account is configured to use POP or IMAP.

## Regarding POP

If your previous VPS account is configured to utilize POP exclusively, the mailbox on that account is a file named as in the following example:

```
~/var/mail/username
```

The time first run the `vmigrate` command, the mailbox is placed in the `.migrate` directory of the shadow account as follows:

```
/var/mail/username
```

Each time you utilize the Recopy Content option, the mailbox is placed in the `.migrate` directory of the shadow account:

```
/home/username/username_v1
```

**Note:** This is a different path than to your original `vmigrate` command. The second copy is not shadowed to `/var/mail/username_v1`.

## Regarding IMAP

If your previous VPS account is configured to utilize IMAP exclusively, the mailbox on that account is a file named as in the following example:

```
~/var/mail/username
```

In addition, mailbox information is located in the following files:

```
~/usr/home/username/mbox
```

```
~/usr/home/username/mail/saved-messages
```

```
~/usr/home/username/mail/my-favorites
```

```
~/usr/home/username/mail/other_names_of_choice
```

**Notes:** On your previous VPS account:

- IMAP clients can automatically empty the contents of `/var/mail/username` and add it to `~/usr/home/username/mbox` when the IMAP client begins to run.
- You have additional mailbox files, each file is located in the following location:
- `~/usr/home/username/mail`.
- Some IMAP clients change the `~/usr/home/username/mail` directory to `~/usr/home/username/Mail/`.

The first time you run the `vmigrate` command, mailbox content is copied to the following directories and files in your shadow account:

```
/home/<username>/mbox
```

```
/home/<username>/mail/saved-messages
```

```
/home/<username>/mail/my-favorites
```

```
/home/<username>/mail/other_names
```

When you issue the Recopy Content command, mailbox content is copied to the following directories and files in your shadow account:

```
/home/<username>/mbox_v1
```

```
/home/<username>/mail/saved-messages_v1
```

```
/home/<username>/mail/my-favorites_v1
```

```
/home/<username>/mail/other_names_of_choice_v1
```

## Changing DNS Settings

The Update DNS option is a time-sensitive one. It provides functions which would otherwise occur automatically and without your input.

**Note:** Do not update your DNS within the first 72 hours of initiating a shadow account. Although settings to a lower TTL apply the instant you initiate the shadow process, it can take up to 72 hours for the 10 second TTL setting change to take affect. If you do select the option to update your DNS before the first 72 hours then wait at least a day to verify the changes. After you allow 72 hours and your shadow account's TTL setting are at 10 seconds, you might still encounter propagation concerns. For example, the TTL settings on your accounts can only influence Internet (and other) service providers which accept them. Any connector who overrides your accounts TTL settings receives the new DNS information only when they refresh their cache.

If you never select this option, you receive an email notification when the update is going to occur. And if you do not need to speed up (or slow down) the process along, you can simply wait for the shadow account process to make the update automatically. The shadow process automatically updates all DNS settings 48 hours (two days) before the shadow completion deadline (21 days).

No less than 72 hours after you initiate the shadow account, you can select this option. Before you do so, you must have previously completed all of the migration tasks, as well as configured and tested all aspects of the shadow account.

This option updates DNS for all domains associated with your previous VPS account using `secure.net` name servers (for example, `ns1.secure.net`, `ns2.secure.net`) as the authoritative name servers. This option updates DNS with the IP address of the shadow account.

The shadow process automatically lowers Time To Live (TTL) settings for domains on the `secure.net` from 24 hours to 10 seconds. This means that on the shadow account, when you update DNS, the changes take affect within 10 seconds. This enables you to verify the change is successful within a much shorter period of time.

If you use this option and subsequently request an extension of the shadow process, the automatic changes to the DNS and TTL settings does not occur. Your request for an extension is overrides this option.

## Reversing Changes to DNS Settings

The Revert DNS option, located in the Backroom of your shadow account, reverses DNS updates you initiated the last time you used Update DNS. This option changes DNS using the IP address of your previous VPS account. This means all Web site traffic is routed to your previous VPS account rather than the shadow account. If you have allowed 72 hours since you initiated the shadow account, this change can occur within 10 seconds since TTL settings remain set to 10 seconds until the shadow is complete.

**Note:** TTL settings on your shadow account can only influence Internet (and other) service providers which accept them. Any connector who overrides your account's TTL settings receives the new DNS information only when they refresh their cache.

## Completing the Shadow

The Complete Shadow option concludes the shadow process by terminating your previous VPS account. Your shadow account becomes your live, active VPS account.

**Note:** This option removes all content from your previous VPS account. Once you select this option, you cannot revive the previous account or return to that configuration.

Verify you perform the following tasks before you use Complete Shadow:

- Issue the `vmigrate` command and functions
- Manually configured the shadow account for all configurations outside the scope of the `vmigrate` command.
- Verified executable files and other contents located in the `cgi-bin` directory.
- Test the shadow account to ensure it is functioning properly.
- Update the DNS to point to the IP address of the shadow account using Update DNS.

## Canceling the Shadow

Use this option to cancel the shadow account and ends the shadow process. This option simply cancels the process. It does not begin or finish any further shadow-related tasks. Since this option terminates your shadow account, any configuration on that account is lost.

**Note:** Once you select Cancel Shadow, the shadow account is terminated and cannot be reinstated. You cannot have an extension of the standard 21 day migration period on the accounts for which you select Cancel Shadow and then reinitiate a shadow. Selecting Cancel Shadow for one account, however, does not affect your eligibility for an extension on other VPS accounts you own.

If you have previously updated the DNS to point to the IP address for the shadow account, the DNS is automatically pointed again to the IP address for your previous VPS account. This option cancels the process and does not begin or finish any further shadow tasks. As this option terminates your shadow account, any configuration on that account is lost. Initiate and then cancel the shadow process only once. If you cancel the process and then begin another, you may no longer have an option to cancel. There are no email notifications sent to confirm your cancellation.

## Connecting to your Shadow Account

Connecting to your shadow account is only slightly different than connecting to your previous VPS account. The shadow account has both an Admin User and a root user. File structure differences impact your decision as to the user with which you determine to connect. This section includes information about using Secure Shell (SSH) and File Transfer Protocol (FTP) to connect to your shadow account.

**Note:** When you connect to your shadow account to perform shadow tasks, you must first connect as the Admin User. Use the IP address of the shadow account. Once connected, use the `su` command to access the root user profile.

## Using SSH to Connect

In a UNIX-style operating system, a root user (also called *super user*) has unlimited abilities including the ability to execute commands that the Admin User cannot. You make most of the changes on your server as the root user, not as a user with administrative permissions. As a security measure, you cannot use a Secure Shell (SSH) client to connect directly to the server as the root user even when you use a correct password.

Instead, you must use an SSH client to connect to the server as the Admin User and after you have performed the necessary task, use the `su` command to become the root user. Do this to assure your root password is secure, to execute the commands you need, and to navigate from the Admin User to become the root user.

After you connect using the new IP address of the shadow account with the Admin User password authentication, run the `su -l root` command to become the root user. After issuing the command, enter the root password which is the same as the Admin User password.

Copyright (c) 1980, 1983, 1986, 1988, 1990, 1991, 1993, 1994

The Regents of the University of California. All rights reserved.  
FreeBSD 4.7-RELEASE-p28 (VKERN) #42: Tue Jun 21 10:33:20 MDT 2005

As the Admin User you have a limited set of privileges, compared to the root user. For most administrative tasks, you will need to `su` to the root user.

As Administrative User you can do some simple administrative tasks such as adding users and Web administration. The `sudo` command enables you to perform the following commands:

```
adduser          vadduser          vedituser          pw                rmuser
vrmuser         vlistuser         vlist              edquota          quota
restart_apache  apachectl        vaddhost          su webadmin      su -l
webadmin
```

The following example shows how to add a user using `vadduser` with the `sudo` command:

```
% sudo vadduser
```

By default, you can perform the above commands without a password; however, `sudo` can be set to require a password for additional security. To add additional functionality to the `sudo` command, edit the `/usr/local/etc/sudoers` file as root. For more information on `sudo` see the `sudo` man pages:

```
% man sudo
```

```
examplev2 ~>
```

As you navigate, you can verify the user with which you logged in most recently by issuing the `whoami` command, as in the following example:

```
examplev2 /home/examplev2# whoami
root
examplev2 /home/examplev2#
```

## Using FTP to Connect

The shadow process introduces file structure changes you see as new files and directories appearing in each user's home directory. The shadow account includes an assigned virtual host (appears as *VirtualHost*) for each user. All files under each *VirtualHost* directory have the same ownership as the user to which it was assigned. When you connect as a user you read, write, and execute only the files owned by the user. *VirtualHost* files appear in the `Web` (`www`) directory. When you connect as the Admin User, you read only the files owned by that user, including any user's *VirtualHost* files. However, an Admin User cannot write to any other user's *VirtualHost* files. Only the root user modifies the Apache configuration file (`www/conf/httpd.conf`) on your shadow account.

## Issuing Shadow-Related Commands and Functions

In general, you can run one menu-driven command, `vmigrate`, which enables you to propagate all the configuration information from the `.migrate` directories where your previous VPS account information is temporarily stored. The command includes six shadow-related functions plus a quit function. These commands and functions call and run a set of special-purpose scripts.

To run the `vmigrate` command, login to your shadow account and issue these commands, as root:

```
cd /.migrate/bin
./vmigrate
```

**Note:** Always run functions one (1) through six (6) in the sequence presented by the menu-driven `vmigrate` command.

The `vmigrate` menu displays as follows:

```
VPS1 to VPS2 Migration/Update Utility
```

- 0) quit
- 1) users
- 2) domains
- 3) php
- 4) mysql
- 5) sendmail
- 6) urchin

Selection:

The following table describes the tasks performed by special-purpose functions which modify the `vmigrate` command:

Function	Tasks performed by the function
0) quit	Indicates that any following commands and functions you issue do not relate the shadow process.
1) users	Propagates user information from the <code>/.migrate</code> directory to your shadow account.  User data and information may include mail information as well as user files. This means that user information can be time-sensitive even if user's configurations are not changed during the shadowing period.
2) domains	Propagates domain name services information to the shadow account.  It is possible to point Web traffic to your shadow account by use of this function.  <b>Note:</b> Treat domains configuration information as highly time-sensitive.

3) php	Propagates PHP open-source scripting information from the <code>/.migrate</code> directory to your shadow account.
4) mysql	Propagates MySQL database configuration information from the <code>/.migrate</code> directory to your shadow account. <b>Note:</b> Treat databases configuration information as highly time-sensitive.
5) sendmail	Propagates the Sendmail MTA from the <code>.vmigrate</code> directory to your shadow account. In addition, this function moves, procmail mail processing and SpamAssassin spam filtering if your configuration includes them. <b>Note:</b> Sendmail data and information may include user information as well as Sendmail-related configuration information. This makes it critical for you to run this function only after having run the 1) <code>users</code> function.
6) urchin	Propagates all information regarding Urchin Web analytics configuration from the <code>/.migrate</code> directory to your shadow account. <b>Note:</b> To assure accurate logging, treat Urchin database information as time-sensitive. For example, if a significant amount of time has passed since you first initiated the shadow account; use the Recopy Content option immediately prior to running this function.

**Table 6: Shadow-Related Functions which Modify vmigrate**

## Other Shadow-Related Commands

After you issue the `vmigrate` command and its shadow-related functions, it is possible to issue stand-alone commands. These commands perform the same tasks as do the functions associated with the `vmigrate` command. In fact, the `vmigrate` command and functions call to the very same special-purpose migration scripts. They do not perform tasks in a manner that is unique from the manner in which the `vmigrate` command and functions perform them.

**Note:** Run these commands only after issuing the `vmigrate` command and its functions. This prevents full propagation of configuration information to your shadow account.

The following table describes the tasks performed by other special-purpose commands provided to assist you with the shadow process:

Command	Tasks performed by the command
<code>migrate_mysql</code> , same as <code>vmigrate 4</code> )	Propagates the MySQL database configuration information from the <code>/.migrate</code> directory to your shadow account.
<code>migrate_php</code> , same as <code>vmigrate 3</code> )	Propagates the PHP open-source scripting information from the <code>/.migrate</code> directory to your shadow account.
<code>migrate_sendmail</code> , same as <code>vmigrate 5</code> )	Propagates the Sendmail open source MTA configuration information from the <code>/.migrate</code> directory to your shadow account.  <b>Note:</b> If you run this command prior to using <code>vmigrate</code> and, in particular, the <code>1) user</code> function, user files (such as <code>.forward</code> , <code>.spamassassin</code> , and <code>.procmail</code> ) do not propagate to your shadow account.

**Table 7: Other Shadow-Related Commands**

## Controlling Access to your Shadow Account

Previous VPS versions enabled only an Admin User to be the owner of files. Your shadow account enables each user to own files and directories. Users can change permissions to specific files or directories that they own.

VPS v2 accounts provide you with the option to assign shell access to user permissions. VPSv2 accounts also automatically assign new users to a group when you do not. Previous versions of VPS enable only the Admin User to have shell access. Once configured, users with shell access can directly connect to their home directory on the server, work with files, and run commands.

The `/www/htdocs` directory on your shadow account is assigned to the `webadmin` user. The `webadmin` user is a part of a standard, FreeBSD configuration. If your main Web site is migrated to the main `/www/htdocs` directory, you cannot log in with as Admin User and edit files those files. Instead, change the ownership of the `htdocs` directory or set up the Main domain as a VirtualHost.

## Managing Groups

**Note:** In most cases, you do not need to manually edit the `/etc/group` file. Use the `vadduser` command to add users; the command prompts you for which groups to add a user to.

VPS v2 accounts automatically assign all users to a group. A group consists of users identified by their user name or by their group identification (GID). Groups appear in the `/etc/group` file. When users are migrated they keep the same permissions as they did on the previous VPS account. For example, if a user had FTP access on the previous VPS account, they are automatically placed in the FTP group (in `/etc/group`) on your shadow account.

## Vinstall Additional Add-Ons

Since your shadow account is a new account, use `vinstall` for additional programs that you may have installed on your previous VPS account. There may not be a `vinstall` for some of the programs that you previously installed in the VPS v1 account with `vinstall`. If this is the case,

install the program using FreeBSD ports collection. For information on how to install programs using the ports collection refer to the *Virtual Private Server Handbook*.

## Perl Modules

Perl is not a part of the automated shadow process. If you are using Perl and you have installed modules that you use, install these modules on your VPS v2 server as well. VPS v2 no longer uses `vcpan` as the default method of installing Perl modules. Instead, VPS v2 now uses the default Perl method of installing modules. To install a module using Comprehensive Perl Archive Network (CPAN), type the following at the shell prompt:

```
% perl -MCPAN -e shell
```

The first time you run CPAN, you are prompted for your preferences regarding where to download your modules and other settings. For most settings, just accept the default. When you select your mirror preferences, select from four to five mirrors.

**Note:** You do not have to know anything about the mirror sites or where they are located. It serves your VPS v2 account just as well if you simply choose the first five (1, 2, 3, 4, and 5) as any others.

Configuring your CPAN settings rarely require reconfiguration, making this a one-time task, in general. From a CPAN command line (`cpan>`), to install a module type the following command in order to get and install the module:

```
cpan> install <Module_name>
```

To save space on your server, be sure to do a clean of the Module after installation by typing the following at the CPAN command line to delete all unnecessary files the server used during installation:

```
cpan> clean <Module_name>
```

## Installing FrontPage Server Extensions

---

**Caution:** Although your previous VPS account includes installed server extensions, you must install a new set of server extensions to the shadow account. Otherwise, any FrontPage Web you publish does not function correctly on the shadow account.

VPS accounts support the Microsoft FrontPage Web site creation and management program. Verify you have saved (or *published*) the FrontPage Web to a local computer, one without association with your previous VPS account. If you have not, do so immediately.

To install server extensions to the shadow account, connect to your VPS v2 server by means of SSH, `su` to root, and run the following command:

```
# vinstall frontpage
```

Virtual subhosts can have the Microsoft FrontPage Server Extensions installed in their home directories. These server extensions are fully functional and give virtual subhost users access to all features of FrontPage.

**Note:** The FrontPage File Upload Component does not work on the Apache Web server (which your Virtual Private Server uses)

The install program checks to see what FrontPage extensions have already been installed. It then prompts you to select the virtual subhost domain you want to install the server extensions for.

**Note:** Do not use `Ctrl-C` to prematurely stop the installation. Doing so can create errors in your Web server configuration file. Allow the installation to fully run its course and close properly.

After installing the server extensions, publish the FrontPage Web to your shadow account.

**Note:** Do not use File Transfer Protocol (FTP) programs to upload a FrontPage Web. FTP can corrupt FrontPage server extensions.

To upload files to your Web site through FrontPage Publish:

1. After you are finished designing a Web page, click **File**.
2. Click **Publish Web**. The Publish Web window appears.
3. In the text box, type the location where you want your Web pages published.
4. Click **Publish**. The Web page is uploaded to your selected location.

To upload files to your Web site through your Control Panel:

1. Select **My Website** from the drop-down list at the top of the window. The My Website Home page appears.
2. Click **Manage my website files**. The Properties window appears displaying the `htdocs` directory.
3. Click **Upload File**. The Upload File window appears.
4. Type the file name and location in the Select File to Upload text box (or click **Browse** to locate the directory containing the file, then double-click the file name).
5. Click **Save**. The destination directory window appears with a message informing you that the file was uploaded to the current directory.
6. To upload more files to this directory, repeat steps four and five for each file.

**Note:** You can upload files to your Web site one at a time or you can zip all the files together and upload that zip file and then unzip it remotely. (If you do not have a zip program, go to the Web site that provides the zip program you want, and then follow the instructions on the screen to download the program to your local computer.)

## Before Terminating your Previous VPS Account

As noted previously in this document (as in “Completing the Shadow” on page 14), you must perform a series of verification tasks prior to the end of the 21-day period allowed for the shadow account or before you use the Complete Shadow option located in the Backroom. This section provides guides to verifying Web site configurations, email setup, and Urchin Web analytics. This section also provides you with descriptions of how to move your digital certificate and, finally, how to terminate your previous VPS account and make your shadow the active, VPS v2 account.

### Verifying Web Site Configurations

Verify the following areas of your Web site configurations before you point DNS to the new IP address and direct your traffic to the Web sites:

- Web site access is unobstructed
- All Web content saved from your previous VPS account to a local computer
- FrontPage server extensions installed to your shadow account
- All necessary Web content uploaded to your shadow account
- Virtual hosting operates correctly
- Common Gateway Interface (CGI) scripts run without conflict

**Note:** Always verify Web site configurations after you issue the `vmigrate` command and its functions.

Before you verify Web site configurations, ensure you have access to the correct IP address for your shadow account. Email notifications begin once you establish a shadow account. Those emails include the address. Also, the Shadow Details page located in the Backroom includes the address. Refer to either recourse to ensure you have the correct address.

The following table provides you with verifications and guidelines for your recently migrated Web site configurations:

Verifications	Guidelines
Web site access is unobstructed	Use your Web browser to verify your main Web site functions correctly. The correct URL for this task does not include a Web resource identifier ( <i>www</i> ) in the URL. Access your main Web site by using the IP address of the shadow account, similar to the following: <i>http://vps2.ip.add.ress</i>

Verifications	Guidelines
Virtual hosting functions correctly	<p>Always test a virtual host before moving DNS services to your shadow account. Access the virtual host by using an Web address you compose of the following elements:  <i>ip.add.re.ss/~user_name/</i></p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>• The IP address of your shadow account (<i>ip.add.re.ss/</i>)</li> <li>• The user that the virtual host is under (<i>~user_name/</i>)</li> </ul> <p>This address provides an index of sites under <i>user_name</i> or a listing of <i>/home/user_name/www directory</i>. Click the domain that you want to test to show the results for the Web site you are testing.</p>
CGI scripts run without conflict	<p>Check active scripts, including CGI scripts, for any conflicts. For example, a previous VPS account stores a virtual host's CGI information in the following directory:  <i>/www/cgi-bin</i></p> <p>For a shadow account, move CGI scripts to <i>cgi-bin</i> directory for the VirtualHost on the shadow account. By default, the shadow process assigns a <i>cgi-bin</i> directory for each VirtualHost directory. Following is an example of the directory path:  <i>/home/userid/www/example.com/cgi-bin</i></p> <p>If a virtual host had its own <i>cgi-bin</i> directory on the previous VPS account then any scripts in that <i>cgi-bin</i> directory are moved to the correct <i>cgi-bin</i> directory automatically.</p>

Table 8: Verifications and Guidelines for your Web site

## Verifying your Email Settings

Check the following files to verify they have set up correctly; they affect email delivery.

```
/etc/mail/aliases
/etc/mail/virtusertable
/etc/mail/access
/etc/mail/local-host-names
```

The following mail files are replaced on the shadow account.

```
~/etc/virtmaps - /etc/mail/virtusertable
~/etc/spammers - /etc/mail/access
```

## Verifying Urchin Web Analytics

**Note:** To assure accurate logging, treat Urchin database information as time-sensitive. For example, if a significant amount of time has passed since you first initiated the shadow account; use the Recopy Content option immediately prior to running the `vmigrate 6) urchin` function.

The automated portion of the shadow process detects your installation of version 3.x.x of Urchin Web analytics. The process then installs a compatible 3.x.x version.

If your previous VPS account includes a 3.x.x version of MySQL, the `vmigrate` command installs the most current of 3.x.x version of MySQL. And if your previous VPS account includes a 4.x.x version of MySQL, the `vmigrate` command installs the most current of 4.x.x version of MySQL.

## Moving Your Digital Certificate

If you use shared \*.seuresites.com digital certificate you do not need to make any changes on the shadow account. The certificate moves and sets up for you. The DNS for the certificate is not automatically updated. You need to contact support by way of email with the \*.seuresites.com canonical name (CNAME) record you would like pointed to the shadow account. Include the CNAME and the IP address of the shadow account.

Running `vmigrate` commands and functions do not move any custom digital certificate to your shadow account. Follow these steps to copy your custom digital certificate:

1. Copy the certificate and private key files to the `/etc` directory from the `.migrate` directory of your shadow account as follows:

```
%cp /.migrate/account_name/etc/ssl.cert /etc
```

```
%cp /.migrate/account_name/etc/ssl.pk /etc
```

2. Add the following lines to the Apache configuration file (`usr/local/apache/conf/httpd.conf`) outside of all Apache directives:

```
SSLCertificateFile /etc/ssl.cert
```

```
SSLCertificateKeyFile /etc/ssl.pk
```

3. Restart Apache run the following command as root from the command line:

```
%restart_apache
```

## Finalizing the Shadow Process

Using the instructions included in this document and by applying your previous Virtual Private Server (VPS) experience, you can conduct a self-migration (referred to as a *shadow process*) from FreeBSD VPS version one (VPS v1) to VPS version two (VPS v2). By means of a shadow process, you can conduct this on your own and without extensive technical support. This introduction provides you with an executive summary, an overview of the shadow process, a process timeline, and a note regarding specialized configurations.

The duration of your shadow account is up to 21 days. At the end of that period, the process completes and your previous VPS account terminates automatically. Prior to that time, you can choose to finish (or *complete*) the process. The option to complete the shadow process is available as an option in the Backroom of your shadow account. By selecting this option, you terminate your previous VPS account as well as its shadow. After selecting the Complete Shadow option, you have only one, active VPS account, one that utilizes VPS v2 features rather than those offered by VPS v1.

Prior to the conclusion of the 21 day period or before you complete the shadow process, verify you have configured and tested all content, settings, and applications. Also, verify and test time-sensitive aspects of your shadow account such as DNS, mail, and database configurations.

## Taking Note of Special Concerns

Take note of the information provided by the following table provides regarding VPS v2 accounts and the shadow process:

Topic	Special Concerns
Manual configuration changes	Once you initiate the shadow account, changes you make to the configuration of your previous VPS account does not automatically become part of the shadow account configuration. During the shadow process, any changes you manually perform for your previous VPS account, you must also perform for the shadow account.
Root user	Your shadow account has a root user as well as an administrator. The root user is a <i>super user</i> . Root provides all privileges and abilities on the account. Because of the capabilities of the root user, connecting to the shadow account by way of SSH as the root user using a password is not allowed. (You can connect by way of SSH as the root user if you have created an SSH key.) To connect to the shadow account you SSH as the administrative user and then <code>su</code> to root.
Disk Space	If you have added additional disk space to your previous VPS account the additional space is added to the shadow account also. You cannot remove the additional space until after the shadow is complete. Once the shadow is complete the additional disk space can be removed from the Backroom.
Miva	Miva is not supported on your shadow account.
SMTPAuth	One of the changes in moving to a VPS v2 account that can have a widespread affect depending on how many email users you have is email authentication. Before a user can send through the shadow account they must be authenticated. VPS v2 accounts use simple mail transfer protocol (SMTP) authentication only. SMTP Authentication (SMTPAuth) requires that each time a user attempts to send email through the server they must authenticate with the login and password. This change is fairly easy to implement since most mail clients allow you to setup the login and password you would like to use for SMTPAuth. Your email users need to enable SMTP Authentication in their mail clients before they are allowed to send through the shadow account.  For detailed instructions regarding how to verify that your email settings support SMTP authorization, refer to help (and other resources) provided by your email software provider.

Topic	Special Concerns
PHP	Whenever PHP 4.x.x is detected, the automated portion of the shadow process installs a current 4.x.x version of PHP to the shadow account. This does not occur if the previous VPS account includes a 3.x.x or previous version of PHP. Maintain support for PHP by upgrading your previous VPS account with a current 4.x.x version of PHP prior to initiating a shadow.
Majordomo	If you have any Majordomo mailing lists in the default location of <code>~/usr/local/majordomo/Lists/</code> , those lists are copied to the shadow account default location of <code>/usr/local/majordomo/lists/</code> .

**Table 9: Taking Note of Special Concerns**

# Notices

## Document Source

This document was written by:  
NTT/VERIO, Inc.  
Documentation and Standards Group  
5050 Conference Way North, Boca Raton, FL 33431

**Copyright © 2005 by NTT/VERIO Inc. All rights reserved.**

## Disclaimers

The following paragraph does not apply to the United Kingdom or any country where such provisions are inconsistent with local law: NTT/VERIO CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of expressed or implied warranties in certain transactions; therefore, this statement might not apply to you.

This publication could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. NTT/VERIO might make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time.

This publication might contain reference to, or information about, NTT/VERIO products (machines and programs), programming, or services that are not announced in your country. Such references or information must not be construed to mean that NTT/VERIO intends to announce such NTT/VERIO products, programming, or services in your country.

The examples used in this document are for instructional purposes only. Any names, persons, associations, company names, domain names, User IDs, Dealer IDs, email addresses, or other addresses contained in this document are not intended to represent actual persons, associations, company names, domain names, User IDs, Dealer IDs, email addresses, or other addresses and any that do are entirely coincidental.

If this document contains graphic representations of system functions, they are sourced from a development environment. These graphics represent only examples of actual plans, products or services. The user interface that you see might be the result of different branding schemes, Internet browsers, plans, or products; therefore, the graphics on your screen might look different from the graphics in this document.

Some system functions require access privileges. Contact your local group for these privileges.

## Trademarks

NTT/VERIO and NTT/VERIO-related product names are trademarks of NTT/VERIO Inc.  
All other trademarks in this document are the property of their respective owners.

## Contact NTT/VERIO

If you have comments or questions about the content in this document, please send an email message to the [VerioDocuments@verio.net](mailto:VerioDocuments@verio.net) and include any specific details.

Requests for technical information about NTT/VERIO products should be made to NTT/VERIO Marketing Representatives.

# Document Conventions

The conventions used in this document are designed to be completely predictable and are used for the following specific purposes.

## Conventions List

### Typeface

*Italic*

### Usage

Used to indicate the following:

- The first mention of new terms in any information unit. For example: The *rudaplex* and the *strataguide* have been the modified for this model.
- References to titles of books, chapters, headings, CDs, diskettes, or software programs. For example: Refer to *The Technical Manual* for technical term descriptions.
- Variables that the user types. For example: Type the *User ID* in the User ID text box.

### Bold

- Used to indicate the following:
- Exact text strings typed. For example: Type **ABCDEFGF**.
- Keyboard keys pressed. For example: **Press Ctrl+a**, then press **Enter**.

### Blue Underline

Used to indicate linked email, IP, Network, or Web addresses. For example: Go to <http://www.microsoft.com> for more information about Microsoft products.

### Cross-Reference

Used to indicate a reference to another part of the same document. The grey portion of the cross-reference is hot linked to the appropriate section of the document, followed by a page number, also hot-linked to the same portion of the document. For example:

For more information about the Document Conventions, see the "Document Conventions" on page 27.

### Operating System Text

Used to indicate text that appears in a shell session for an operating system. The displayed text pertains to operating system text only, not application elements. For example:

Type `LIST MAIN FOLDER`. The screen displays the Main folder.

### Program Code

Used to indicate code listings. For example:

```
{
# do something;
}
# check to see if $user has the attrib 'attrib'
if (hasKey($user_obj, 'attrib', $dbh) != 1)
{
print "User not Authorized to update!";25
}
}
```

### Window Element

Window elements consist of anything that is displayed on window (exclusive of the operating system). This includes toolbar menu items, drop-down lists and items in a drop-down list, buttons, or anything else a user sees on screen. For example:

- From the Printer drop-down list, choose Local Printer. The Are You Sure? dialog box appears. Click OK.
- The following message appears: User Not Authorized

## Special Elements

These elements provide a variety of information ranging from warnings that the reader should not neglect to supplementary information and tips that will simply enhance their reading experience.

**Tip** Used to point out helpful ideas, some not-so-obvious features, quick or alternate ways to get a particular job done, and techniques you might not discover by yourself. The **Tip List** special element is used when multiple tips are used.

**Note:** Used to highlight certain information for the reader. Generally, the Note element provides additional information on the current topic. The **Notes:** special element is used when multiple notes are required.

**Important:**

Used for information that is considered more pertinent to the reader than information presented in Note elements.

---

**Caution:**

*Used as a hazard light in NTT/VERIO documents. Information included in a Caution element could save the reader from hours of lost work.*

---