OpenTeck.inc

Linux Training

ClarkConnect 4.3

Ahmad Shah Fazel

2009

Linux Overview

What is Linux?

Linux is an open-source "UNIX-like" operating system, with many similarities to UNIX operating systems like Sun Microsystem's Solaris and Hewlett Packard's HP-UX. The Linux kernel and many applications included in Linux distributions are developed by countless programmers worldwide.

Most of the software included in a Linux distribution, including the Linux kernel, is licensed under the GNU General Public License, permitting others to examine, modify, and create derivative works from the code for both commercial and noncommercial purposes.

To be technically correct, Linux is an operating system with kernel, and is not itself a complete operating system.

Kernal:

The Linux kernel provides the basic services and device drivers used by all other programs running on a Linux OS.

The shell

The shell acts as an interface between the user and the kernel. When a user logs in, the login program checks the username and password, and then starts another program called the shell. The shell is a command line interpreter (CLI). It interprets the commands the user types in and arranges for them to be carried out. The commands are themselves programs: when they terminate, the shell gives the user another prompt (% on our systems).

Some benefits of using Linux:

* Cost:

One of the key benefits of using Linux is cost: most Linux distributions are available at no charge.

* Security

* Stability

* Excellent networking capability built into your operating system

* Freedom from viruses

Linux Origins

● 1984: The GNU Project and the Free Software

Foundation

* Creates open source version of UNIX utilities

* Creates the General Public License (GPL)

.Software license enforcing open source principles

● 1991: Linus Torvalds

* Creates open source, UNIX-like kernel, released under the

GPL

* Ports some GNU utilities, solicits assistance online

- 1994: Linux kernel version 1.0 is released

● Today:

* Linux kernel + GNU utilities = complete, open source,

UNIX-like operating system

What is Open Source?

*Open source: software and source code available to all

* The freedom to distribute software and source code

*The ability to modify and create derived works

*Integrity of author's code

.The Free Software Foundation and the Four

Freedoms

Linux principles

● Everything is a file (including hardware)

● Small, single-purpose programs

● Ability to chain programs together to perform complex tasks

● Avoid captive user interfaces

Logging in to a Linux System

● Two types of login screens: virtual consoles

(text-based) and graphical logins (called display

managers)

● Login using login name and password

● Each user has a home directory for personal

file storage

Switching between virtual consoles and the graphical environment

● A typical Linux system will run six virtual consoles and one graphical console

* Server systems often have only virtual consoles

* Desktops and workstations typically have both

● Switch among virtual consoles by typing:

Alt-F ***[1–6]***

The root user

● The root user: a special administrative account

* Also called the superuser

* `root` has near complete control over the system

■ ...and a nearly unlimited capacity to damage it!

● Do not login as `root` unless necessary

* Normal (unprivileged) users' potential to do damage is more limited

Changing Identities

● **su -** creates new shell as root

● **sudo** ***command*** runs ***command*** as root

* Requires prior configuration by a systemadministrator

● **id** shows information on the current user

File and Directory Names

● Names may be up to 255 characters

● All characters are valid, except the forwardslash

* It may be unwise to use certain special characters in

file or directory names

* Some characters should be protected with quotes when referencing them

- Names are case-sensitive

* Example: `MAIL`, `Mail`, `mail`, and `mAiL mail`

* Again, possible, but may not be wise

Linux File Structure

In the Linux file structure files are grouped according to purpose. Ex: commands, data files, documentation. All directories are grouped under the root entry "/".

Some Important Directories

- Home Directories: `/root`,`/home/`*`username`*
- User Executables: `/bin`, `/usr/bin`, `/usr/local/bin`
- System Executables: `/sbin`, `/usr/sbin`, `/usr/local/sbin`
- Other Mountpoints: `/media`, `/mnt`
- Configuration: `/etc`
- Temporary Files: `/tmp`
- Kernels and Bootloader: `/boot`
- Server Data: `/var`, `/srv`
- System Information: `/proc`, `/sys`
- Shared Libraries: `/lib`, `/usr/lib`, `/usr/local/lib`

ClarkConnect 4.3

Introduction

ClarkConnect is a server Operating System (OS) that provides enterprise-level network security and application services to the Small/Medium-sized Business (SMB) market. It protects against incoming threats, enables your organization to enforce outgoing policy and increases productivity through integration of services.
Configuration using an easy-to-use web interface for the helps keep the required knowledge of Linux to a minimum. You should, however, have at least a working knowledge of basic network concepts in order to make optimal use of the installation wizard.
This document describes how to install and configure your ClarkConnect server/gateway

Features

The following features are included in ClarkConnect:

- Web-based manager
- Auto software updates
- Stateful firewall
- Multi-WAN support
- Intrusion detection
- Internal DHCP server
- Caching DNS server
- RAID support
- Multi-processor support
- Intrusion prevention
- Egress blocking support
- PPTP & IPSec VPN
- Managed/Dynamic VPN
- Dynamic DNS
- Groupware/Collaboration
- Flexshares
- SMTP server
- Antispam (Dual)
- Antivirus
- POP and IMAP servers
- Webmail
- Banner ad blocking
- Web proxy
- Content filtering
- Bandwidth manager
- Web server (HTTP)
- PHP support
- MySQL support
- SSL certificate manager
- SSL support (HTTPS)

- FTP server
- Mail Archive
- Encrypted Volumes
- Print sharing (CUPS)
- File sharing (SAMBA)
- LAN/server backup
- Health monitoring/alerts
- Daily security audit
- Linux 2.6 kernel
- Technical support

Compatibility

Overview

ClarkConnect 4.x is based on Red Hat Enterprise Linux 4. For the most part, hardware that is compatible with Enterprise Linux will be compatible with ClarkConnect.

Here are some tips when selecting hardware:

- Avoid the latest technologies and chipsets. This will reduce the likelihood of compatibility issues and the possible reliability issues that might come with unproven hardware.
- Avoid desktop systems. You may save a few hundred dollars on a desktop system, but they are more likely to fail when used as a server/gateway.

In case you missed the previous bullet point, ***avoid desktop systems***.

- Check the vendors web site for Linux compatibility. If you can purchase ServerXYZ with a version of Red Hat Enterprise Linux pre-installed, then the system is very likely compatible with ClarkConnect.

Recommended

The following vendors ship servers with Linux pre-installed and have a good record:

- Dell servers (***not desktops***')
- HP servers
- IBM servers

Not Recommended

The following vendors have a poor track record for Linux support.

- Supermicro
- Promise
- Dell Optiplex Desktop

RAID Support

Overview

Both software and hardware RAID are supported in ClarkConnect.

Installation

Starting the Install

Installation CD

A bootable CD drive is required to install the ClarkConnect software. The rest of the software is installed from the CD-ROM or directly over your high-speed Internet connection.

Starting the Installation

The contents of all your hard disks on the target computer will be completely erased.

- if necessary, change your BIOS settings to run bootable CDs
- Insert the ClarkConnect CD
- Turn on your target computer
- Follow the installation wizard

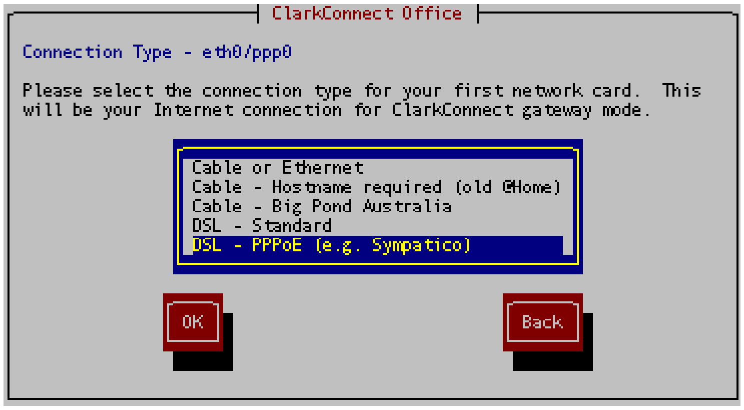
Configuration Options

Selecting Your Server Type

ClarkConnect now supports standalone server mode. This mode is used to create a server on a local area network (behind an existing firewall). Only one network card is required. Gateway Mode allows your system to act as a firewall and server on your local network and at least two network cards. If you have two or more network cards installed in the server and want to protect your local network against threats originating from the Internet, then select gateway mode.

Selecting Your Network Connection Typeh

If you are installing with a CD-ROM, you will need to select the type of Internet connection you have (DSL, DSL/PPPoE, Cable).



ClarkConnect Office

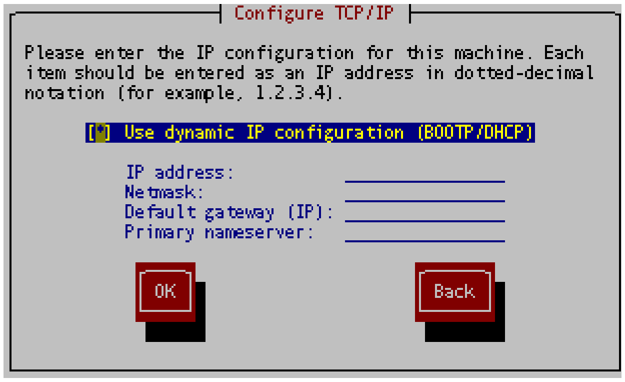
Connection Type - eth0/ppp0

Please select the connection type for your first network card. This will be your Internet connection for ClarkConnect gateway mode.

```
Cable or Ethernet
Cable - Hostname required (old @Home)
Cable - Big Pond Australia
DSL - Standard
DSL - PPPoE (e.g. Sympatico)
```

Configuring Your Network

Unless your Internet Service Provider (ISP) provides a static IP address, it is recommended that you use Dynamic IP Configuration. If your ISP assigns a static IP you will need to enter the individual TCP/IP settings as provided by your ISP. Make sure you have these settings available during the installation process.


Configure TCP/IP

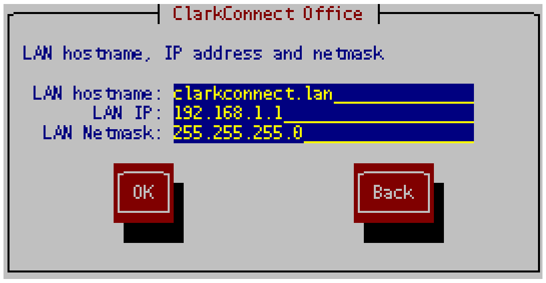
Please enter the IP configuration for this machine. Each item should be entered as an IP address in dotted-decimal notation (for example, 1.2.3.4).

[*] Use dynamic IP configuration (BOOTP/DHCP)

IP address: __________
Netmask: __________
Default gateway (IP): __________
Primary nameserver: __________

Configuring Your LAN IP Address

If you are installing ClarkConnect as a gateway, you must specify the network settings for your local area network. The ***LAN hostname*** can be used instead of the IP address for many network tools. For instance, you will be able to access the web-based administration tool at https://<LANhostname>:81 in your web browser.


ClarkConnect Office

LAN hostname, IP address and netmask

LAN hostname: clarkconnect.lan
LAN IP: 192.168.1.1
LAN Netmask: 255.255.255.0

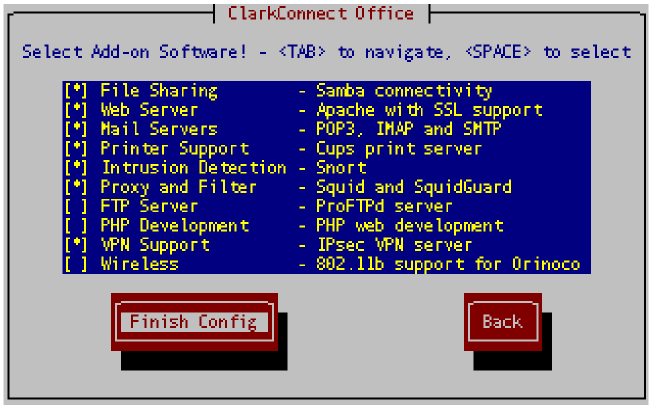
Selecting Your Hostname - Password - Timezone

The next few screens will ask for your system name, system password and time zone.

Selecting Your Hard Disk Partitioning Settings

Selecting Your Software

Select the software components to install on your system. With the ClarkConnect web-based configuration, you can add other modules at any time.



```
ClarkConnect Office

Select Add-on Software! - <TAB> to navigate, <SPACE> to select

[*] File Sharing         - Samba connectivity
[*] Web Server           - Apache with SSL support
[*] Mail Servers         - POP3, IMAP and SMTP
[*] Printer Support      - Cups print server
[*] Intrusion Detection  - Snort
[*] Proxy and Filter     - Squid and SquidGuard
[ ] FTP Server           - ProFTPd server
[ ] PHP Development      - PHP web development
[*] VPN Support          - IPsec VPN server
[ ] Wireless             - 802.11b support for Orinoco
```

Configure Partitioning and RAID

Overview

For some installations, you may want to define a custom partition scheme instead of using the default. Typically, custom partitioning is required for:

- Software RAID
- Creating a separate /home partition

Select Advanced Partitioning

If you do not wish to use the default partitioning scheme on your system, then select ***advanced partitioning*** in the installation wizard .The tool for creating partitions will appear at a later stage in the installer. Continue with the rest of the installation wizard after selecting the partition type on this screen.

Using the Disk Druid Partition Tool

When the installer displays a disk partitioning setup page, select the ***Disk Druid*** option on this Screen

Example: Software RAID 1

Using software RAID is a common way to protect against a hard disk failure. Here is a step-by-step guide to implement Software RAID 1 on regular IDE hard disks.

Preparing the Hardware

For software RAID 1, you need two hard disks. Since the RAID partitions on both the hard disks must be of equal size, it is a good idea to use two hard disks with (roughly) the same storage capacity. In our example, we are using two IDE disks on two different disk controllers. These hard disks are detected in Linux as:

- /dev/hda
- /dev/hdc

Deleting Existing Partitions

Some hard disks may have partitions already defined. These existing partitions (if any) must first be deleted.

- Use the tab key to move to the main window (one tab after highlighting the ***Back*** button)
- Use the up/down arrows to select a partition
- Use the tab key to highlight the ***Delete*** button and hit return
- Repeat until all partitions are deleted

Creating the Swap Partition

After all the partitions are deleted, we can start our RAID configuration. First, we are going to start with the swap memory partitions. Putting swap memory on a software RAID partition is not recommended. For this reason, simply create swap partitions on both hard disks.

- Tab to the ***New*** button and hit return
- Tab down to ***File System Type*** and select ***swap***
- Tab to ***Allowable Drives*** and mark only hda and take the mark off of hdc.
- Tab down to ***Size (MB)*** and type in the size of your RAM in megabytes (MB)
- Tab down to ***OK*** and hit return.

Repeat the same process, but this time mark hdc as an ***allowable drive*** and take the mark off of hda.

Creating RAID Partitions

The boot partition (/boot) is where we are going to start with our RAID solution.

- Tab to the ***New*** button and hit return
- Tab down to ***File System Type*** and select ***software raid***
- Tab to ***Allowable Drives*** and mark only hda and take the mark off of hdc.
- Tab down to ***Size (MB)*** and type in 100
- Tab down to ***OK*** and hit return.

Repeat the same process, but this time mark hdc as an ***allowable drive*** and take the mark off of hda. Now that we have two identical 100 MB partitions on both disks, we can create the software RAID disk:

- Tab to the ***RAID*** button and hit return
- Type in /boot in the ***Mount Point*** field
- Tab to ***RAID Level*** and select RAID1
- Tab to ***RAID Members*** and make sure the two partitions created earlier are selected.

This example creates the /boot partition. Go through the same process for the root partition (/) and optionally any other partition that you want to create (/home, /var, etc.).

Configuring the Boot Loader

We are almost done with the software RAID configuration. Next, the installation wizard will ask for the boot loader settings.

- Select Grub as your boot loader
- Disable the boot password (unless you really need it)

Testing Software RAID

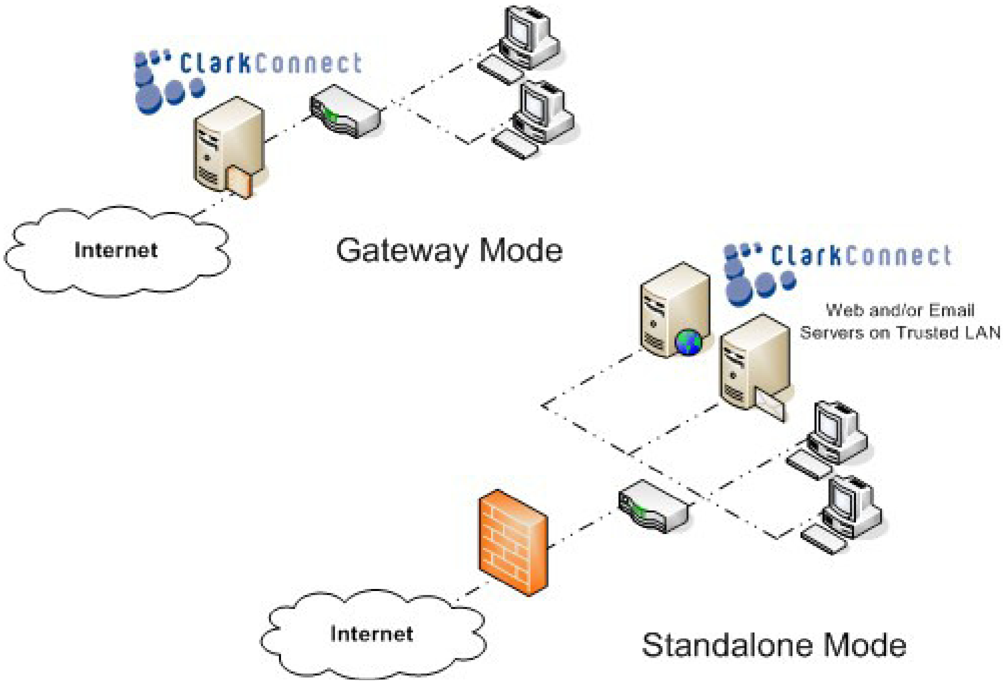
If you would like to sanity check your RAID system, then:

- Power down the machine
- Unplug the data connector from the drive (just unplugging the power is going to make the BIOS unhappy and the system will not be bootable)
- Power up the machine

Network Mode

The ClarkConnect system can run in tow modes:

- ***Standalone Mode - No firewall*** - for a standalone server without a firewall (1 network card)
- ***Gateway*** - for connecting your LAN to the Internet (2 network cards)



Hostname

A hostname is the full name of your system. If you have your own domain, you can use a hostname like ***gateway.example.com***, ***mail.example.com***, etc. If you do not have your own domain then make one up, for instance: ***gateway.lan***, ***mail.lan***. The hostname does require at least one period (.).

Name/DNS Servers

On DHCP and DSL/PPPoE connections, the DNS servers will be configured automatically. In these two types of connections there is no reason to set your DNS servers. Users with static IP addresses should use the DNS servers provided by your Internet Service Provider (ISP).

Accessing Login Prompt

If you are an advanced user and would like to access the standard login prompt, hit Alt-F2 on your keyboard. To return to ClarkConnect console, hit Alt-F7 (Alt-F1 for versions 4.0 or earlier).

Web-based Administration

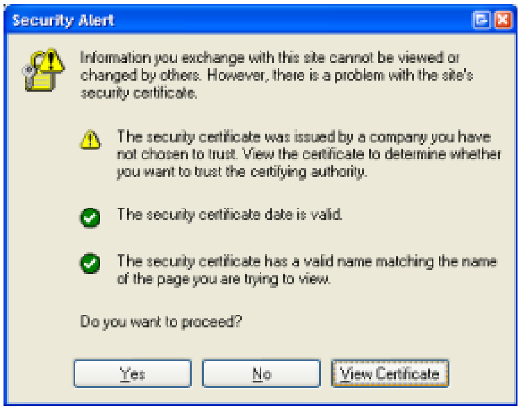
Overview

Once you have your network up and running with the network configuration tool, you can configure all other ClarkConnect features from the web browser of any desktop or laptop computer.

Access

To access the ClarkConnect web-based administration tool, type the following into your web browser: https://IP_Address:81 for example: https://192.168.1.1:81

The IP address that you need to use was selected during installation. If you do not remember this information, you can always connect a keyboard and monitor to the system and check the network configuration tool.



Security Alert

Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.

The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.

The security certificate date is valid.

The security certificate has a valid name matching the name of the page you are trying to view.

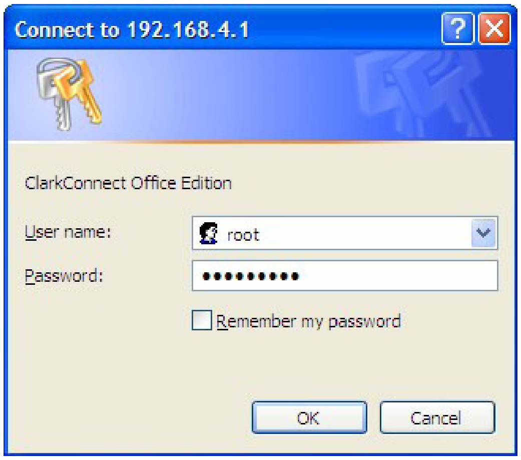
Do you want to proceed?

Certificate Warning

You will see a warning about your security certificate (see adjacent screenshot). Click on the appropriate button to ignore the message. Your connection is still secure and encrypted, but your server certificate is not official. A valid certificate costs over $100 a year to maintain and is not necessary in this situation.

Username and Password

You will then see a login prompt (see adjacent screenshot). Login with the username ***root*** and your system password.



Connect to 192.168.4.1

ClarkConnect Office Edition

User name: root

Password: ●●●●●●●●●

□ Remember my password

Technical Notes

Please note the following about the web-based administration tool:

- It uses the encrypted protocol (***https*** instead of ***http***)
- It runs on a non-standard port (the :81 appended to the web page address) so that it does not interfere with an existing web server

DHCP Server

Description	DHCP server for dynamically assigning IP addresses.
Package Name	cc-dnsmasq
Configuration Page	Network >> IP Settings >>DHCP

The Dynamic Host Configuration Protocol (DHCP) allows hosts on a network to request and be assigned IP addresses. This service eliminates the need to manually configure new hosts that join your network.

Domain Name

The server can auto-configure the default domain name for systems using DHCP on your network.

You can either use a registered domain (for example: ***example.com***) or you can simply make one up (for example: ***lan***). Example:

- A desktop system on your local network has a system name ***scooter*** and uses DHCP.
- The domain name specified in the DHCP server is ***example.com***.
- On startup, the desktop system appends ***example.com*** to its system name. Its full hostname would become ***scooter.example.com***.

IP Ranges

Keep a range of IP addresses available for systems and services that require static addresses. For instance, VPN and some types of network printers require static IP addresses.

In a typical local area network, the first 99 IP addresses are set aside for static addresses while the remaining addresses from 100 to 254 are set aside for the systems using the DHCP server. Adjust these settings to suit your needs and your network.

DNS Address

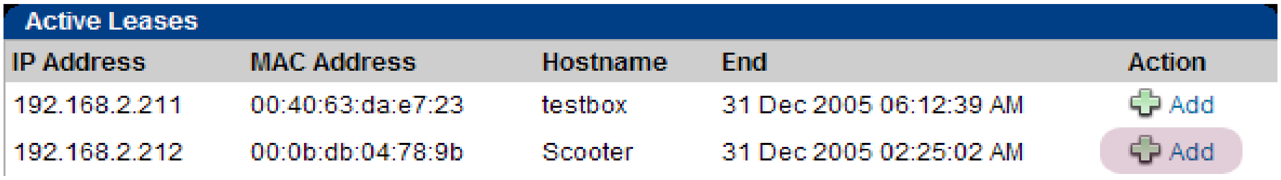
The server can auto-configure the DNS settings for systems using DHCP on your network. By default, the IP address of the caching DNS server on your ClarkConnect system is used. You should change this setting if you want to use an alternate DNS server.

WINS Address

If you have a Microsoft Windows Internet Naming Service (WINS) server on your network, you can provide the IP address to all Windows computers on your network. This will allow Windows systems to access resources via Network Neighborhood. You can enter the LAN IP address of your ClarkConnect system here if you have enabled the WINS server on ClarkConnect.

Active and Static Leases

A list of systems that are actively using the DHCP server is shown in the ***Active Leases*** table. If you would like to make a DHCP lease for a particular system permanent, you can click on the appropriate ***Add*** button in this list. In the screenshot below, the button to add 192.168.2.212/Scooter as a static lease is shown.



Active Leases

IP Address	MAC Address	Hostname	End	Action
192.168.2.211	00:40:63:da:e7:23	testbox	31 Dec 2005 06:12:39 AM	Add
192.168.2.212	00:0b:db:04:78:9b	Scooter	31 Dec 2005 02:25:02 AM	Add

Hosts and DNS Server

Hosts and DNS Server Information		
Description	Hosts file and local DNS server configuration.	
Package Name	cc-dnsmasq	
Configuration Page	Network >> IP Settings >>Hosts and DNS Server	

Hosts (/etc/hosts) is a simple text file that associates IP addresses with hostnames. If you have the caching DNS server installed, all the entries in the hosts file will be made available.

IP Settings

IP Settings Information	
Description	IP, hostname and DNS settings.
Package Name	cc-network
Configuration Page	Network IP Settings IP Settings

Configuration

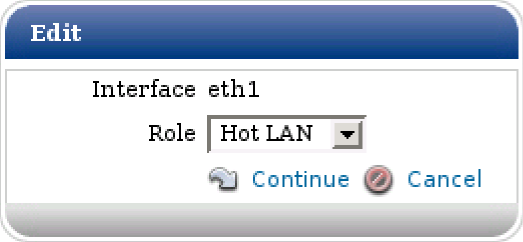
Linux will auto-detect most PCI-based network cards.

Network Roles

When configuring a network interface, the first thing you need to consider is the network role. Will this network card be used to connect to the Internet, for a local network, for a network with just server systems? The following network roles are supported in ClarkConnect and are described in further detail in the next sections:

- External - network interface with direct or indirect access to the Internet
- LAN - local area network
- Hot LAN - local area network for untrusted systems

On a standalone system, your network card should be configured with an external role, not a LAN role.



Edit

Interface eth1

Role Hot LAN

External

The external role provides a connection to the Internet. On a ClarkConnect system configured as a gateway, the external role is for your Internet connection. On a ClarkConnect system configured in standalone mode, the external role is for connecting to your local area network.

Multi-WAN

Description	Support for multiple connections to the Internet.
Package Name	cc-multiwan
Configuration Page	Network IP Settings Multi-WAN

The multi-WAN feature in ClarkConnect allows you to connect your system to multiple Internet connections. ClarkConnect multi-WAN not only provides load balancing, but also automatic failover.

How It Works

ClarkConnect multi-WAN has the following features:

- auto-failover
- load balanced

Network Tools

Network Tools Information	
Description	**Tools to monitor and diagnose the network.**
Package Name	cc-nettools
Configuration Page	Network IP Settings Network Tools

Provides basic networking tools to help diagnose network problems.

Firewall

1 to 1 NAT

1-to-1 NAT Firewall Information	
Description	Configuration tool for 1-to-1 NAT.
Package Name	cc-firewall-dmz
Configuration Page	Network Firewall 1-to-1 NAT

1-to-1 NAT maps a real Internet IP to an IP on your local area network (LAN).

Incoming

Firewall Incoming Information	
Description	Tool for configuring incoming connections on the firewall.
Package Name	cc-firewall
Configuration Page	Network Firewall Incoming

Configuration

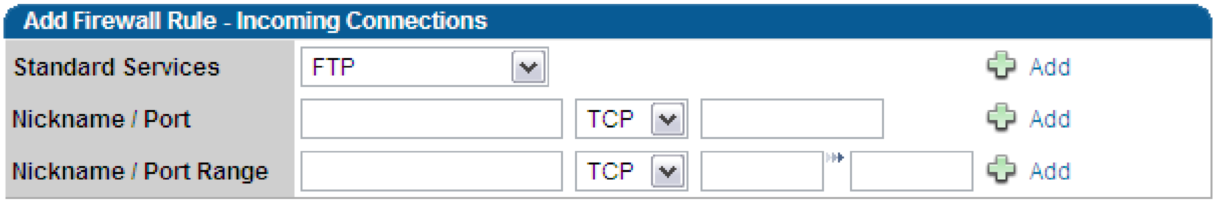
Allow Incoming Connections

If you want to run a server ***on*** your ClarkConnect system, you must open the appropriate port on the firewall to allow access to users on the Internet. For instance, if you are running the web server and secure web server, make sure port 80 and 443 are open.

You can also open up ports to allow for remote management of your ClarkConnect system. For example, you can open up port 22 to allow for SSH access and port 81 to give access to Welcoming.

Select ***Firewall Incoming*** in the web-based administration tool. There are three ways to add an incoming firewall rule:

- select a standard service in the ***Standard Services*** drop down
- input a single port number in the ***Port Number*** box.
- input multiple consecutive ports in a port range in the ***Port Range*** box.



Add Firewall Rule - Incoming Connections

Standard Services	FTP			Add
Nickname / Port		TCP		Add
Nickname / Port Range		TCP		Add

Block Internet Hosts

If you want to block a remote site from accessing your ClarkConnect system, add the IP address or network to the block list. This is typically used to unwanted connections from. If you want to block web sites from your users, the Content Filter is a more effective solution.

Outgoing

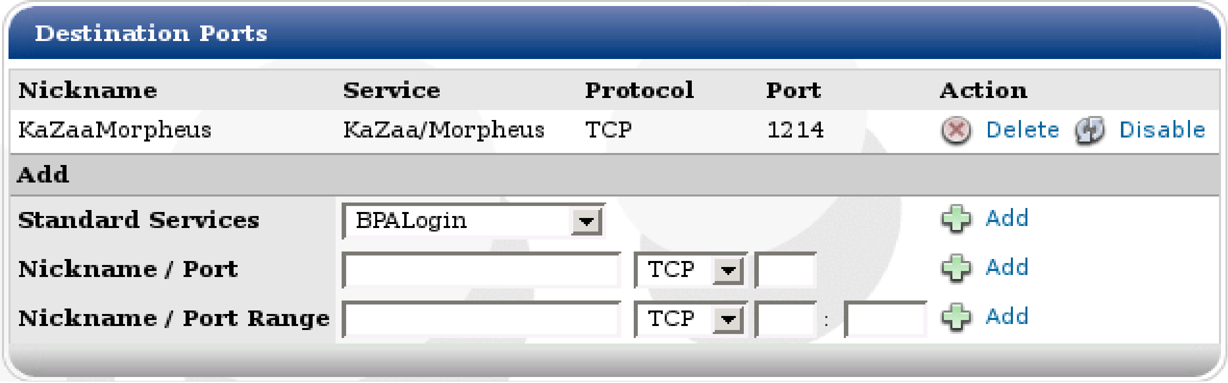
Outgoing Information	
Description	Tool for blocking or allowing (depending on mode) outgoing connections on your network.
Package Name	cc-firewall
Configuration Page	Network Firewall Outgoing

Configuration

From the ***Firewall Outgoing*** page, you can block or allow certain kinds of traffic from leaving your network depending on the ***mode/policy***.

Outgoing Traffic - By Port/Service

Destination Ports prevents/allows a connection on a particular port/service. For instance, adding port 80 (web) disables/enables web-surfing for your entire local network.



Destination Ports

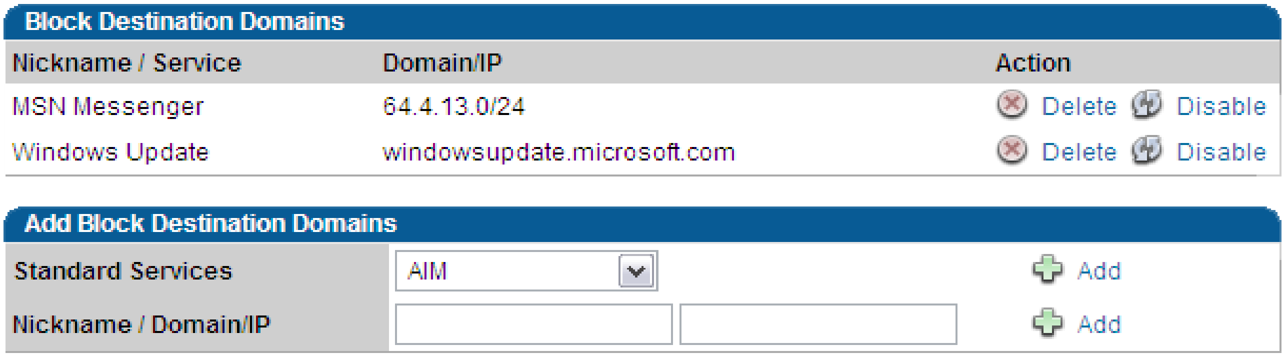
Nickname	Service	Protocol	Port	Action
KaZaaMorpheus	KaZaa/Morpheus	TCP	1214	Delete Disable

Add

Standard Services	BPALogin		Add
Nickname / Port		TCP	Add
Nickname / Port Range		TCP :	Add

Outgoing Traffic - By Host/Destination

Destination Domains allows you to block/allow certain networks and sites. For instance, if your Outgoing Mode is set to allow all outgoing traffic, blocking windowsupdate.microsoft.com blocks Windows from connecting to the windows update site. Keep in mind, some sites use multiple servers to handle network traffic and are not easily blocked. If you block destinations with the firewall bear in mind that users of the proxy may not be blocked. If you require proxy users to be blocked, your best option is to block the destinations using the DansGuardian Content Filter Module.



Block Destination Domains

Nickname / Service	Domain/IP	Action
MSN Messenger	64.4.13.0/24	Delete Disable
Windows Update	windowsupdate.microsoft.com	Delete Disable

Add Block Destination Domains

Standard Services	AIM	Add
Nickname / Domain/IP		Add

Peer-to-Peer

Peer-to-Peer Information	
Description	A tool to block peer-to-peer traffic.
Package Name	cc-firewall-p2p
Configuration Page	Network Firewall Peer-to-Peer

Configuration

The following applications can be blocked and/or throttled:

- eDonkey, eMule, Kademlia
- KaZaA, FastTrack
- Gnutella
- Direct Connect
- BitTorrent, extended BT
- AppleJuice
- WinMX
- SoulSeek
- Ares, AresLite

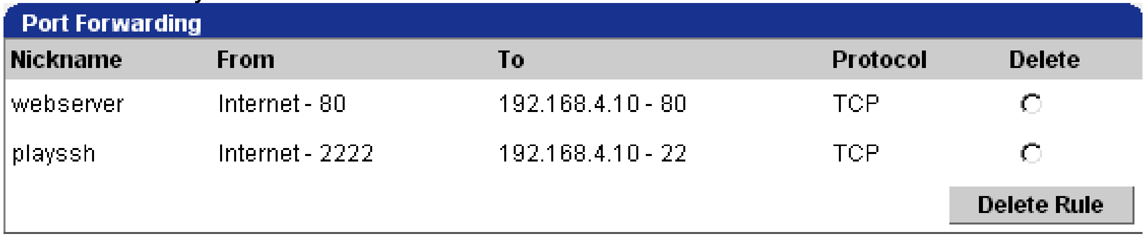
Port Forwarding

Port Forwarding Information	
Description	Tool for forwarding ports to systems on your local network.
Package Name	cc-firewall
Configuration Page	Network Firewall Port Forwarding

Configuration

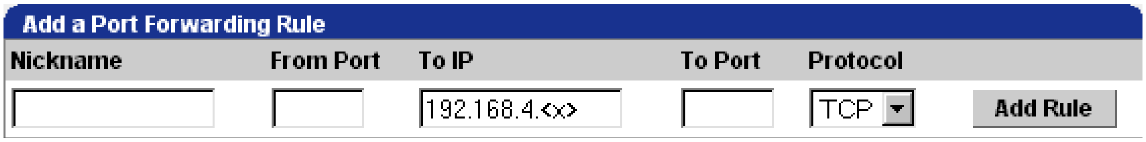
If you run servers ***behind*** your ClarkConnect gateway, you can use the ***Port Forwarding*** page to forward ports to a system on your local area network. In the example below, two port forwarding rules are configured:

- A web server (port 80) is running on the LAN at 192.168.4.10
- SSH (port 22) is also running on 192.168.4.10. Since port 22 is already used on the gateway, we specify an alternate port (2222). We then configure our SSH client to use port 2222 to connect directly to 192.168.4.10 from the Internet.



Port Forwarding

Nickname	From	To	Protocol	Delete
webserver	Internet - 80	192.168.4.10 - 80	TCP	○
playssh	Internet - 2222	192.168.4.10 - 22	TCP	○



Add a Port Forwarding Rule

Nickname	From Port	To IP	To Port	Protocol	
		192.168.4.<x>		TCP	Add Rule

Intrusion Detection

Intrusion Detection Information	
Description	An advanced intrusion detection system.
Package Name	cc-snort
Configuration Page	Network Security Intrusion Detection

The intrusion detection package is included with ClarkConnect to make users more aware of some of the daily hostile traffic that can pass by your Internet connection. The software is able to detect and report unusual network traffic including attempted break-ins, trojans/viruses on your network, and port scans.

Intrusion Prevention

Intrusion Prevention Information	
Description	An advanced intrusion prevention system.
Package Name	cc-snortsam
Configuration Page	Network Security Intrusion Prevention

The intrusion prevention system blocks suspected attackers from your system.

Services

New exploits are discovered everyday. The intrusion detection software maintains and uses a list of 2000+ rules. You can receive automatic updates by subscribing to the Intrusion Detection Updates service.

The Intrusion Prevention system displays a list of IP addresses that have been blocked due to inappropriate network traffic.

Account Manager

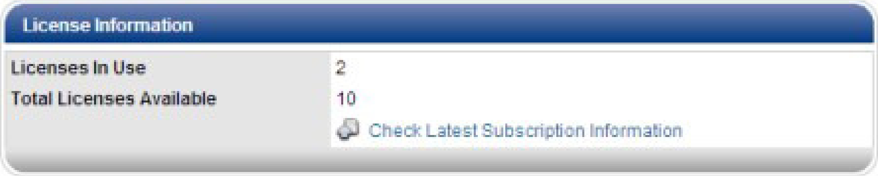
Users

User Manager Information	
Description	Tool to add and manage users on the system.
Package Name	cc-users
Configuration Page	Account Manager All Accounts Users
Keywords	LDAP

The user manager page allows you to add, delete and manage users on the system

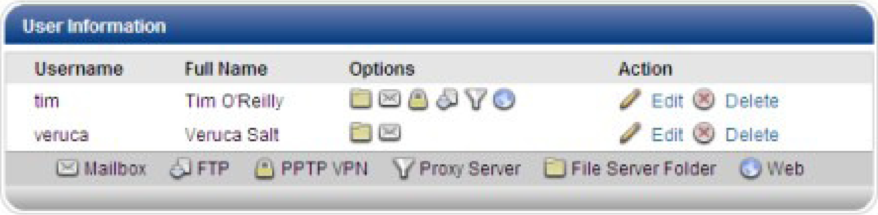
User

The first thing you will see on the user manager page is a summary of existing users. This summary includes the username, name and the enabled options for each user. Depending on the platform/version you are using, you may see a dialog box indicating how many mailbox accounts are in use and how many are available. The Enterprise Edition allows you to purchase additional mailbox licenses to increase the number of users who have can send/receive mail on the server.



License Information

Licenses In Use	2
Total Licenses Available	10
	Check Latest Subscription Information



User Information

Username	Full Name	Options	Action
tim	Tim O'Reilly	📁 ✉ 🔒 FTP ▽ 🌐	Edit Delete
veruca	Veruca Salt	📁 ✉	Edit Delete

In the screenshot shown, user ***tim*** has access to all the available services while user ***veruca*** only has access to e-mail and the file server.

User Information

Every user must have the following information configured:

- ***Username*** - a username (lowercase only)
- ***First name*** - the user's first name
- ***Last name*** - the user's last name
- ***Password*** and ***Verify*** - a password

User Options

The following options are available in the user configuration. Note: the option will not appear if the related software is not installed on the system.

📁	File Server Folder -	access to home directory on the File Server
🖧	FTP Server -	FTP Server access
✉	Mailbox -	Mail Server - SMTP
🔒	access PPTP Server -	PPTP VPN
▽	access Proxy Server -	Web Proxy
🌐	access Web Server -	Web access for Flexshare

Note: Shell Access | If an administrator needs to enable Secure SHell (SSH) access for a user's account, this needs to be done at the command line in versions 4.0 and later.

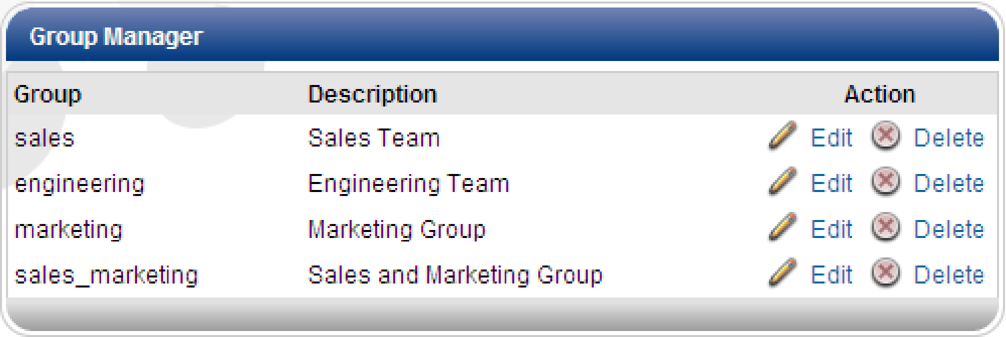
Groups

Group Manager Information	
Description	Tool to add and manage groups on the system.
Package Name	cc-users
Configuration Page	Account Manager All Accounts Groups

The group manager page allows you to add, delete and manage groups on the system.

Configuration

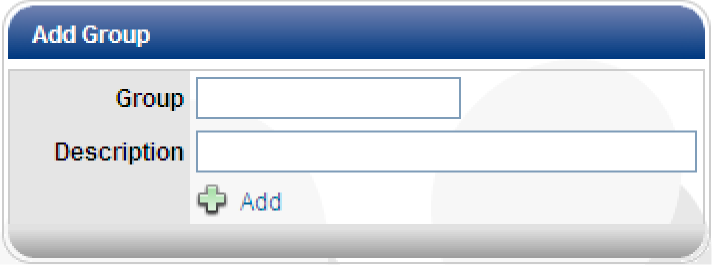
The first thing you will see on the group manager page is a summary of existing groups.



Group Manager

Group	Description	Action
sales	Sales Team	Edit Delete
engineering	Engineering Team	Edit Delete
marketing	Marketing Group	Edit Delete
sales_marketing	Sales and Marketing Group	Edit Delete

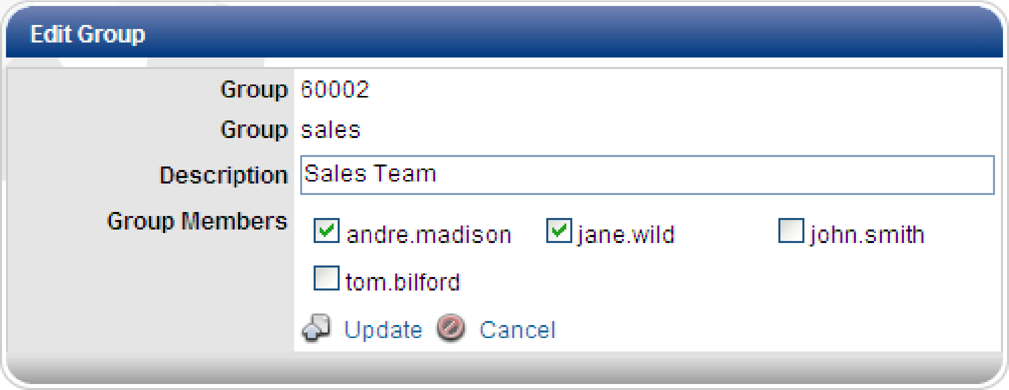
Use the "Add Group" form below the summary of existing groups to add a new group.



Add Group

Group	
Description	

Once you have added a new group, or if you click on the "Edit" link next to an existing group, a new form will appear providing information specific to the group you created/edited.



Edit Group

Group	60002
Group	sales
Description	Sales Team
Group Members	☑ andre.madison ☑ jane.wild □ john.smith □ tom.bilford

Use this form to make changes to the users belonging to the group and/or to change the description of the group name.

System Tools

Backup and Restore

Backup and Restore Information	
Description	A simple backup and restore tool for configuration files.
Package Name	cc-backuprestore
Configuration Page	System Settings Backup/Restore

The backup/restore feature lets you take a snapshot of all the configuration files and save them to a separate system for safe keeping. If a ClarkConnect system needs to be restored, you can reinstall the ClarkConnect system and then restore all the configuration settings from the backup.

Configuration

The backup/restore tool saves all the configuration information available through the web-based interface:

- Usernames and passwords (4.0 or higher)
- Network configuration
- Firewall configuration
- Software configuration (for example, content filter)

The backup/restore settings tool does ***not*** save user data, logs or mailboxes. Use the LAN/Backup and Recovery tool for backing up data. (or bmbackup)

Date

Date Information	
Description	Tool to set the date, time and timezone.
Package Name	cc-webconfig
Configuration Page	System Settings Date

The date configuration tool allows you to select your time zone as well as enable/disable automatic time synchronization.

Encrypted File Systems

Encrypted File System Information	
Description	Encrypted file system manager.
Package Name	cc-dmcrypt
Configuration Page	System Settings Encrypted File System

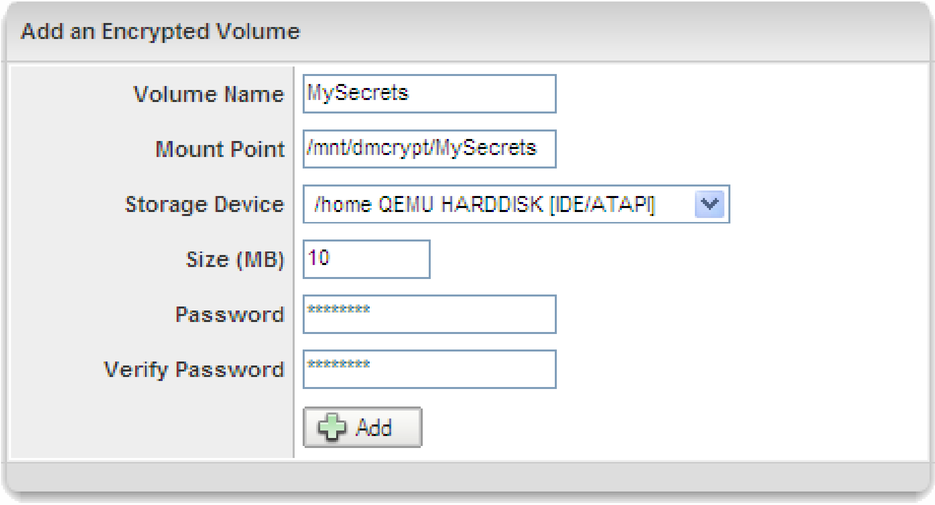
The encrypted volume module allows the creation of encrypted volumes that can be used to protect confidential data from unauthorized access in the event the server is physically removed from the premise or a portable mass storage device is lost/stolen while in transit.

Data is stored in an encrypted format when a volume has not been mounted. Mounting a volume requires the password. With a strong password, gaining access to the decrypted data (i.e. usable information) is impossible in the event the volume is unmounted. A volume is unmounted whenever a server is restarted (i.e. a shutdown, loss of power etc.) and must be mounted by an administrator having both Webconfig access and the volume password. It is important to note that this module does not provide protection against unauthorized access to data when a volume is mounted (i.e. the state the volume would normally be in during every day use). This module does not replace the need to maintain software updates, use of a properly configured firewall, IDS/IPS etc.

Configuration

Adding an Encrypted Volume

Any number of encrypted volumes can be created on the server - either on the local hard disk or an external mass storage devices. Volumes created on the local disk reside in parallel with other system/user data. By contrast, volumes created on unmounted devices (i.e. a USB attached hard disk) fill the entire physical disk size...formatting any/all data that may be on an existing file-system.



Add an Encrypted Volume

Volume Name	MySecrets
Mount Point	/mnt/dmcrypt/MySecrets
Storage Device	/home QEMU HARDDISK [IDE/ATAPI]
Size (MB)	10
Password	********
Verify Password	********

Volume Name

A unique name that describes the volume (i.e. ArchivedMail, ExternalUSB etc.)

Mount Point

The location the volume will be accessible. By default, the mount point is created in /mnt/dmcrypt/<VolumeName>

Storage Device

The physical device location.

Size

The size (in MB) of the encrypted volume. Keep in mind, encrypted volumes have an ***encryption***
overhead approximately equal to 1-5% of the total defined size of the volume.

Password

The password required to mount the encrypted volume.

Verify Password

Re-enter the password to verify.

Troubleshooting

What if I forget my password?

In a word: don't. If you forget a volume encryption password, there is absolutely no way to recover the data.

How can I auto-mount my encrypted volumes on bootup?

You cannot...this would defeat the purpose of creating an encrypted volume.

Language

Language Information	
Description	Tool to set the language and locale.
Package Name	cc-webconfig
Configuration Page	System Settings Language

You can change the language used by ClarkConnect from this configuration page.

Running Services

Running Services Information	
Description	A tool to view and manage services running on the system.
Package Name	cc-webconfig
Configuration Page	System Settings Running Services

This configuration page gives you a bird's eye view of the services (also known as "daemons") on your system.

Shutdown and Restart

Shutdown and Restart Information	
Description	A shutdown and restart tool for your system.
Package Name	cc-webconfig
Configuration Page	System Settings Shutdown/Restart

A tool to shutdown or restart your system.

E-Mail Notification/Alert (SMTP Relay)

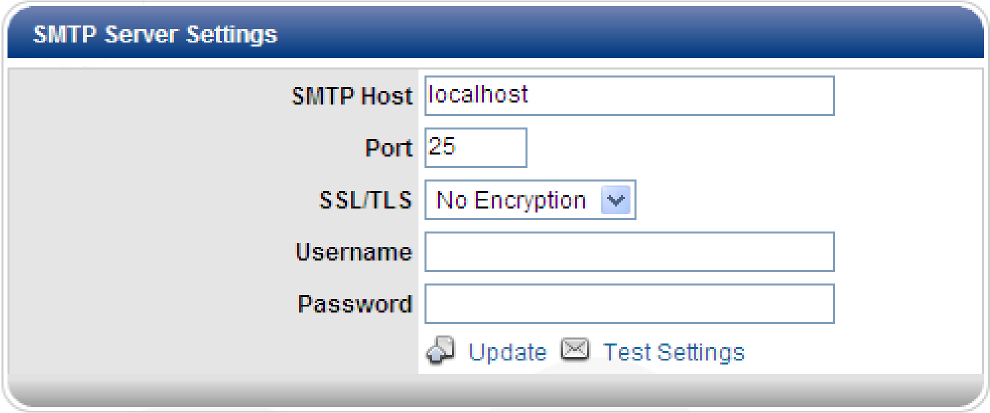
SMTP Relay/Notification Information	
Description	Allows applications to send reports, alerts, notifications etc. via email through the configured SMTP relay without having a local Mail Transport Agent (MTA).
Package	Name cc-mailer
Configuration	Page System Settings SMTP Relay
Keywords	Swift

Installation

This module is installed only when a module dependent on the Mailer class is installed. To install manually, run:

```
# apt-get update
# apt-get install cc-mailer
```

Configuration



SMTP Host	localhost
Port	25
SSL/TLS	No Encryption
Username	
Password	

Configuration of the SMTP relay is access under System Tools SMTP Relay.

SMTP Host

The hostname of the SMTP server to connect to.

Port
The port to used to send the initial connection request on. SMTP usually uses port 25.
SSL/TLS
Encryption protocol to use when connecting to the host server.
Username
A valid username to authenticate to the server.
Password
A valid password to authenticate to the server.

SSL Certificate Manager

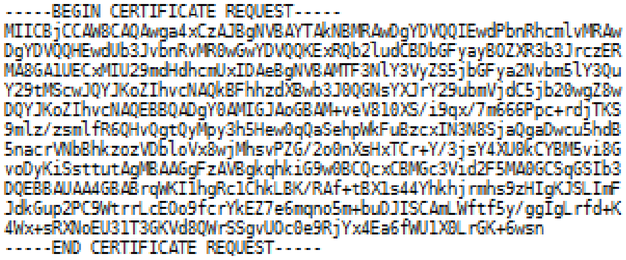
SSL Certificate Information	
Description	Allows the creation, signing, renewal and revocation of SSL certificates for implementing cryptography using SSL (v2/v3) and TLS (v1) protocols.
Package Name	cc-ssl
Configuration Page	System Settings SSL Certificate Manager

SSL certificates are the de-facto standard for encrypting information sent over a network and can also be used to provide authentication, as in the case of SMIME email signature signing.

This module provides an administrator with the ability to create a Certificate Authority (CA) which can then be installed as a trusted CA on any operating system, browser or mail client in order to encrypt/decrypt (and/or sign emails) communications between two computers. Creating your own CA and using it to sign certificates is termed "self-signing".

Self-signing of certificates is as secure as purchasing signed SSL certificates from a ***Trusted CA*** like Thawte or Verisign, where prices range from $US 50-300 per year. Self-signing is extremely convenient (and cost effective!) if you are providing access to known users (ie. employees, clients, vendors etc.). It is less convenient than a ***Trusted CA*** when dealing with unknown users such as website visitors using a browser to access your online store using HTTPS (HTTP over SSL), since the user will be prompted by their browser to trust the certificate that is presented to them.

The SSL Certificate Manager module can also create Certificate Signing Request (CSR) certificates. The contents of a typical CSR certificate are shown below:



```
-----BEGIN CERTIFICATE REQUEST-----
MIICBjCCAW8CAQAwga4xCzAJBgNVBAYTAkNBMRAwDgYDVQQIEwdPbnRhcmlvMRAw
DgYDVQQHEwdUb3JvbnRvMR0wGwYDVQQKExRQb2ludCBDbGFyayB0ZXR3b3JrczER
MA8GA1UECxMIU29mdHdhcmUxIDAeBgNVBAMTF3NlY3VyZS5jbGFya2Nvbm5lY3Qu
Y29tMScwJQYJKoZIhvcNAQkBFhhzdXBwb3J0QGNsYXJrY29ubmVjdC5jb20wgZ8w
DQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAM+veV810XS/i9qx/7m666Ppc+rdjTKS
9mlz/zsmlfR6QHvQgtQyMpy3h5Hew0qQaSehpWkFuBzcxIN3N8SjaQgaDwcu5hdB
5nacrVNbBhkzozVDbloVx8wjMhsvPZG/2o0nXsHxTCr+Y/3jsY4XU0kCYBM5vi8G
voDyKiSsttutAgMBAAGgFzAVBgkqhkiG9w0BCQcxCBMGc3Vid2F5MA0GCSqGSIb3
DQEBBAUAA4GBABrqWKIlhgRc1ChkLBK/RAf+tBX1s44Yhkhjrmhs9zHIgKJSLImF
JdkGup2PC9WtrrLcEOo9fcrYkEZ7e6mqno5m+buDJISCAmLWftf5y/ggIgLrfd+K
4Wx+sRXNoEU31T3GKVd8QWrSSgvUOc0e9RjYx4Ea6fWU1X0LrGK+6wsn
-----END CERTIFICATE REQUEST-----
```

Webconfig

Webconfig Information	
Description	Webconfig settings.
Package Name	cc-webconfig
Configuration Page	System Settings Webconfig

The Webconfig settings page allows you to change the look and feel of the web-based interface.

Database
MySQL

Database Information	
Description	MySQL relational database.
Package Name	cc-mysql
Configuration Page	Software Database MySQL Setup

The Webconfig UI for MySQL provides login configuration/management to the phpMyAdmin web interface...a separate UI that allows full control over your MySQL databases.

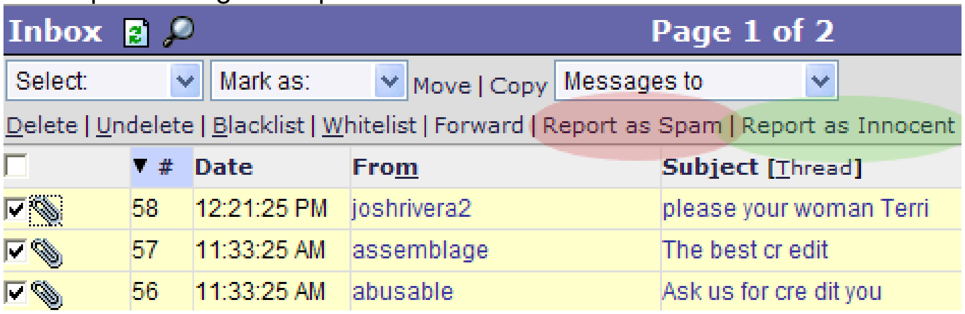
Email
Antispam

Antispam Information	
Description	Antispam for mail servers.
Package Name	cc-spamassassin
Configuration Page	Software Mail Antispam

The antispam software works in conjunction with your mail server. The software identifies spam using a wide range of algorithms on e-mail headers and body text. ClarkConnect also includes greylisting and additional blacklists -- both are effective tools that can be used to detect spam.

Webmail

Training the antispam system via webmail is simple and more effective. Simply select the messages that you wish to process and press either the ***Report as Spam*** or ***Report as Innocent*** buttons (see screenshot). You will then be shown a confirmation message before the actual processing takes place.


Inbox
Page 1 of 2
Select:
Mark as:
Move | Copy
Messages to
Delete | Undelete | Blacklist | Whitelist | Forward | Report as Spam | Report as Innocent

□	▼ #	Date	From	Subject [Thread]
☑	58	12:21:25 PM	joshrivera2	please your woman Terri
☑	57	11:33:25 AM	assemblage	The best cr edit
☑	56	11:33:25 AM	abusable	Ask us for cre dit you

Antivirus

Antivirus Information	
Description	Antivirus for mail servers.
Package Name	cc-clamav
Configuration Page	Software Mail Antivirus

The antivirus system scans mail messages as they pass through your mail server.

Mail Policies

When configuring the antivirus system, you must make some mail policy decisions. There are three types of policies available:

- ***Bounce*** bounce the e-mail
- ***Discard*** - silently discard the e-mail
- ***Pass Through*** - send e-mail with warning (original sent as an attachment)

Virus Detected Policy

When a virus is detected, you can choose to either discard the message, or pass the message through. We recommend discard mode for most installations.

Aliases

Aliases Information	
Description	Mail server aliases tool.
Package Name	cc-postfix
Configuration Page	Software Mail Aliases

Mail aliases allow you to route extra e-mail addresses (for instance sales@, info@, etc) to one or more e-mail addresses. This tool can also be used to create mail distribution lists - for example, staff@example.com can be used to send e-mail to all users on the system.

POP and IMAP

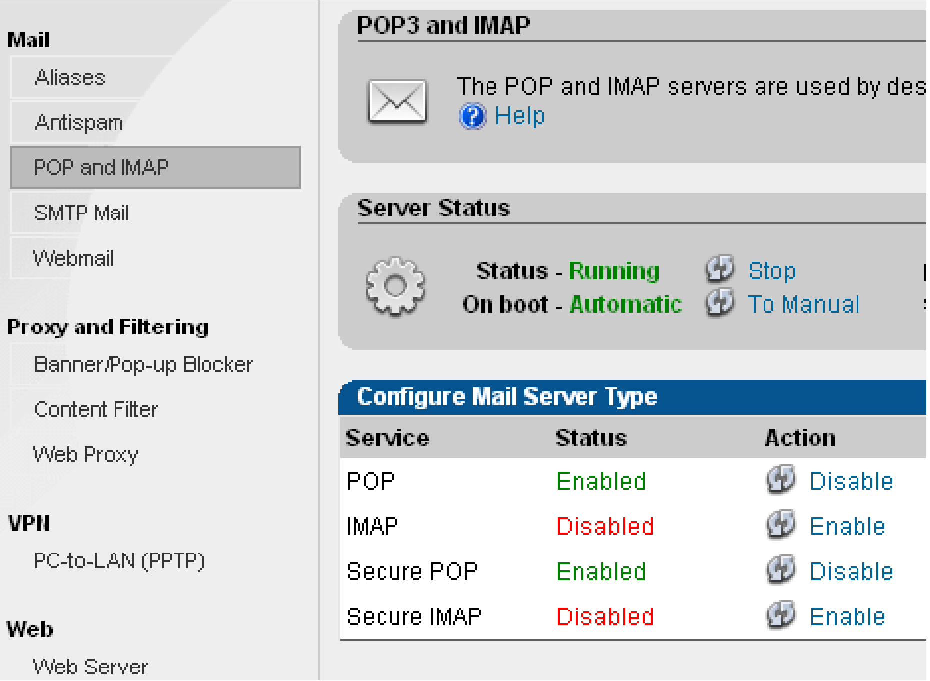
POP and IMAP Information	
Description	Mail access for desktop mail clients.
Package Name	cc-cyrus
Configuration Page	Software Mail POP and IMAP

ClarkConnect provides both POP and IMAP servers for providing mail delivery to desktop clients.

Mail Server Protocols

The mail server supports four different protocols (see screenshot):

- IMAP
- Secure IMAP
- POP
- Secure POP



POP3 and IMAP

The POP and IMAP servers are used by des

Server Status

Status - Running
On boot - Automatic

Configure Mail Server Type

Service	Status	Action
POP	Enabled	Disable
IMAP	Disabled	Enable
Secure POP	Enabled	Disable
Secure IMAP	Disabled	Enable

Mail Server - SMTP

Mail Server - SMTP Information	
Description	SMTP/MTA mail server.
Package Name	cc-postfix
Configuration Page	Software Mail SMTP Mail Server

You can manage your own mail server. There are a number of reasons this might be advantageous:

- Ability to have a customized user and domain name - ie. anyone@anydomain.com
- Mailboxes limited only by hard disk storage capacity and your own administration settings
- Alias support - i.e. sales@yourcompany.com can be sent to bob@yourcompany.com and joe@yourcompany.com
- No waiting around for new users to be added
- Custom antispam control
- Antivirus support
- Privacy
- Full control

Webmail

Webmail Information	
Description	Web-based mail system.
Package Name	cc-horde
Configuration Page	Software Mail Webmail

A web-based e-mail solution ideal for allowing users 'on the road' and without a mail client to access mail on the server using any computer connected to the Internet.

Accessing Webmail

- The webmail system runs on port 83 on the HTTPS protocol. To access the system type

https://192.168.1.1:83/ or https://yourdomain.com:83/
- If webmail access is required from the Internet, please allow connections to port 83 (webmail) on the firewall .
- Web-based mail requires the IMAP server to be running.
- Users will receive a pop-up warning in their web browser. This is normal and does not diminish the fact that the connection is encrypted and secure.

File Services

Flexshare

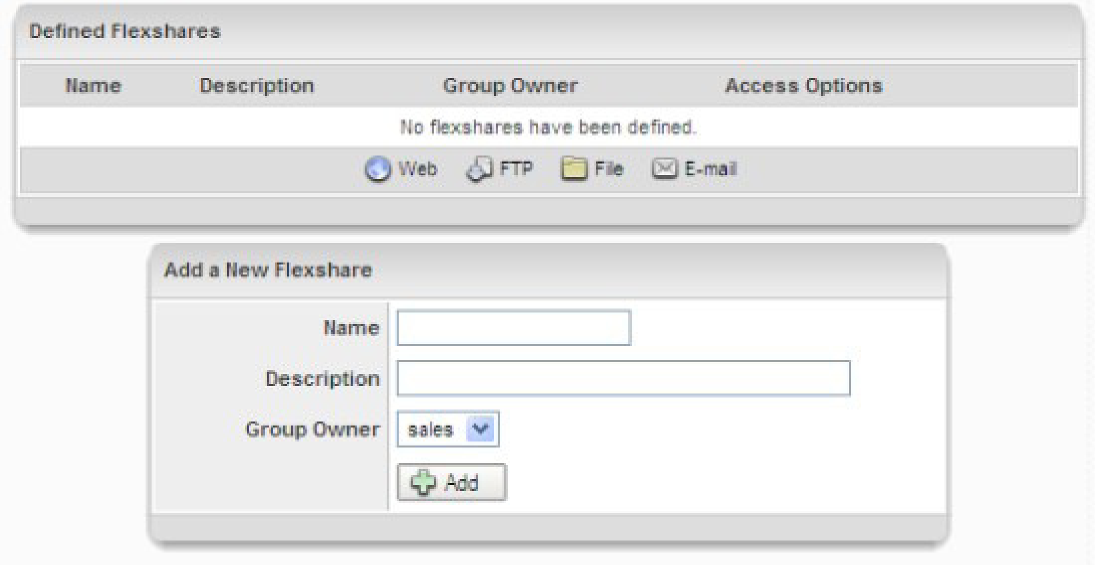
Flexshare Information	
Description	A file collaboration utility.
Package Name	cc-flexshare
Configuration Page	Software File Services Flexshare

Flexshare is a flexible and secure collaboration utility which integrates four of the most common methods of accessing files or content:
- Web (HTTP/HTTPS)
- FTP (FTP/FTPS)
- File Shares (Samba)
- E-mail (SMTP/MIME/SMIME)

You will also need to install one or more of the following modules to enable functionality for the following services:
- Web access - cc-httpd
- FTP access - cc-proftpd
- File access - cc-smbd
- E-mail upload - cc-postfix, cc-cyrus

Share Overview

Once the system user has been updated with the password provided, you will be presented with the Flexshare Overview.



Defined Flexshares

Name	Description	Group Owner	Access Options
No flexshares have been defined.			

Add a New Flexshare

Name	
Description	
Group Owner	sales

The first table lists the shares you have currently defined, allowing you to quickly view which access methods are enabled in addition to overall Flexshare status (either enabled or disabled).

You can ***Edit***, and ***Delete*** the status of each Flexshare using the ***Action*** links in the right hand column. Of course, if no Flexshares are defined, the ***Action*** links will not be visible.

The second table allows you to define (create) a new Flexshare. See Creating a New Flexshare below.

Creating a New Flexshare

To define a new Flexshare, fill out the ***Name*** and ***Description*** fields and select a Unix group to represent the share owner in the ***Add a new Flexshare*** form. A Flexshare template will be created (with no access and disabled by default). The Editing a Flexshare form will be displayed, allowing you to customize the share options and enable access options.

Editing a Flexshare

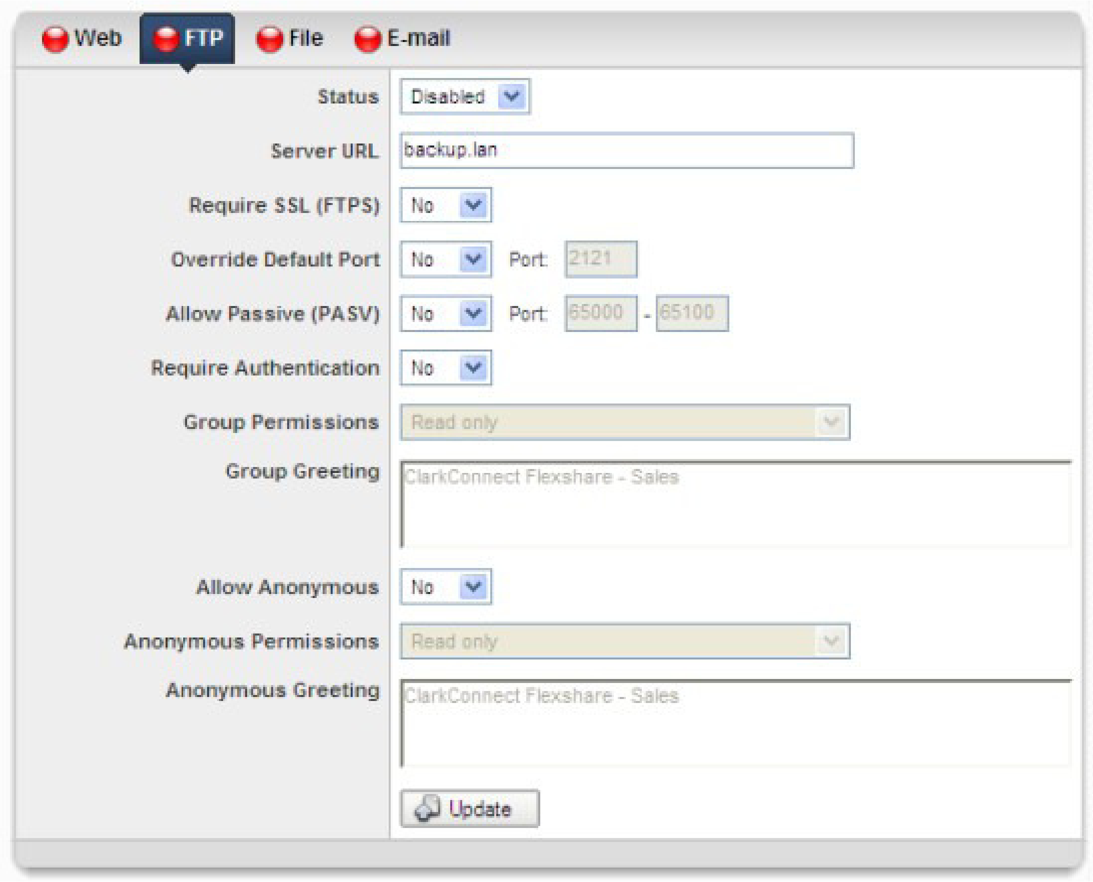
You can make edits/changes to any defined Flexshare at any time. A newly created Flexshare will have no access points enabled, so you will want to configure at least one service (Web, FTP, Filesharing or E-mail) to take advantage of the share you have created.

Configuring Flexshare's ***Web*** access enables anyone (or authorized users only) to use a web-browser to navigate to a website in order to view content, interact with a dynamic web page (for example - a PHP or CGI enabled online store) or download files from an index listing.

FTP

Configuring Flexshare's ***FTP*** access enables anonymous or authorized users only (or both) to use an FTP-client to connect via File Transfer Protocol in order to upload and/or download files to the server. The FTP protocol, while outdated, is still a prominent service today and is particularly useful for handling large files.

One of the downsides of the FTP protocol is that it uses separate ports to control data flow and transmit pay



Status	Disabled
Server URL	backup.lan
Require SSL (FTPS)	No
Override Default Port	No Port: 2121
Allow Passive (PASV)	No Port: 65000 - 65100
Require Authentication	No
Group Permissions	Read only
Group Greeting	ClarkConnect Flexshare - Sales
Allow Anonymous	No
Anonymous Permissions	Read only
Anonymous Greeting	ClarkConnect Flexshare - Sales

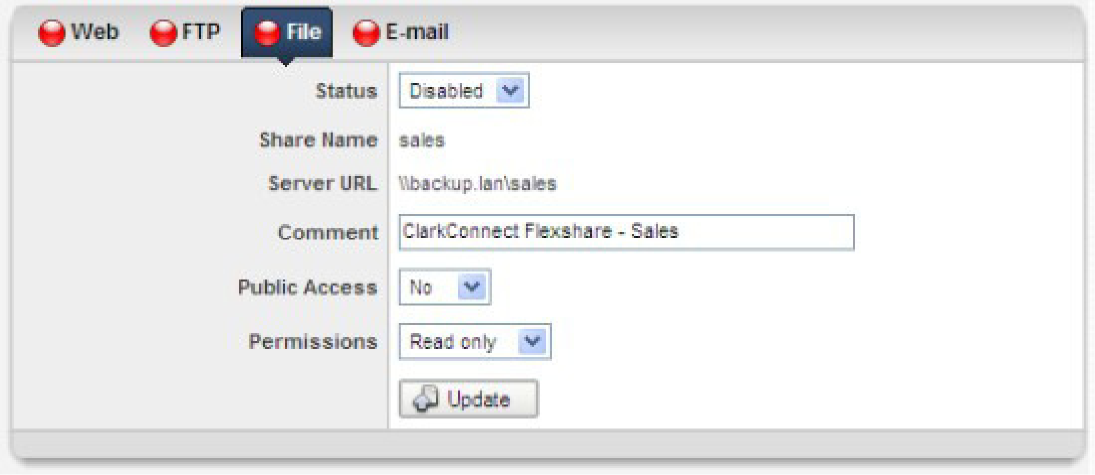
Enabled
Indicates the current status of the ***FTP Access*** for a Flexshare. Note, even though the FTP Access point is enabled, the overall Flexshare must also be ***Enabled*** in order to work.
Use the ***Enabled/Disabled*** link at the bottom of the form to toggle the status.

Require SSL (FTPS)
Determines the protocol to use - FTP or FTPS. If you have enabled authentication, you are advised to set this to ***Yes*** (use FTPS) since users will be required to provide their username/passwords to authenticate to the server. Using FTPS ensures this sensitive data is encrypted.

Override Default Port
Flexshare FTP/FTPS uses port 2121/2120 and 2123/2122 as the default ports (see bubble below for an explanation). You can override these standard ports by setting this parameter to ***Yes*** and entering the custom ports in the fields that will appear upon changing the override drop-down.
The options contained in each drop-down box contain three characters. The characters are defined as:

- Hyphen - No permissions
- r - Read
- w - Write
- x – Execute

Allow Anonymous
Allows anonymous FTP access. Users only have to provide the username ***anonymous*** and (usually) their e-mail address to gain access to the share. Use anonymous when you are not providing access to restricted files and you do not want/need to create individual accounts on your server to authenticate against.
File



Status	Disabled
Share Name	sales
Server URL	\\backup.lan\sales
Comment	ClarkConnect Flexshare - Sales
Public Access	No
Permissions	Read only

Configuring Flexshare's ***File*** access (SAMBA) enables public or authorized users only (or both) to connect via file sharing in order to move files from desktop to the server and vice-versa.
Enabled
Indicates the current status of the ***File Access*** for a Flexshare. Note, even though the File Access point is enabled, the overall Flexshare must also be ***Enabled*** in order to work.
Use the ***Enabled*/*Disabled*** link at the bottom of the form to toggle the status..

Public Access
Set ***Public Access*** field to ***Yes*** if you want to allow anyone on the Local Area Network (LAN) access to the Flexshare

FTP Server

FTP Server Information	
Description	A full-featured FTP server.
Package Name	cc-proftpd
Configuration Page	Software File Services FTP

Configuration
The default configuration for ClarkConnect system allows read-only anonymous FTP to the /var/ftp directory and full access to valid user accounts. Advanced configuration of the FTP server can be done in one of two ways:

- Creating and configuring a Flexshare (Version 4.0 and up only)
- Editing the /etc/proftpd.conf configuration file.

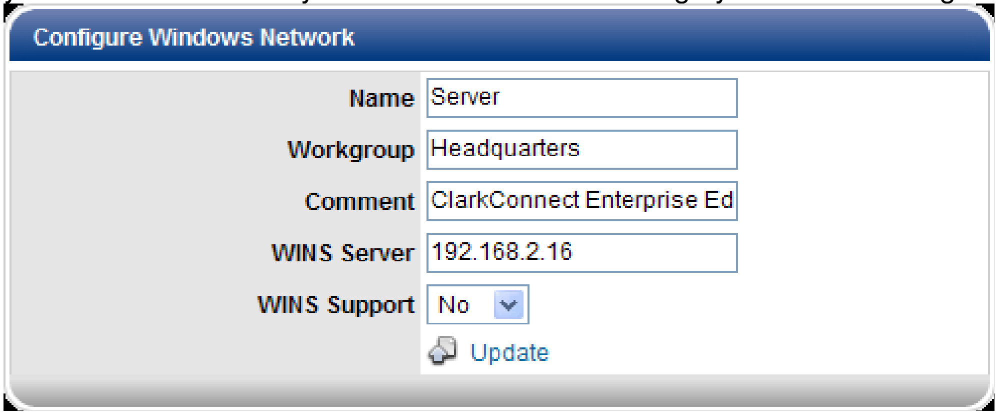
Windows-Samba

File Sharing / Samba Information	
Description	Samba file sharing system for Windows.
Package Name	cc-samba
Configuration Page	Software File Services Windows File Sharing

Your ClarkConnect system provides file serving capabilities for a Windows network. Among other tasks, you can use the software for backup file storage, and sharing printers.

Basic Configuration

The basic configuration for the Windows/Samba file server is straightforward -- at the very least, you will want to change the ***Name***, ***Workgroup*** and ***Comment***. If you are using Windows PCs, you will be able to see your ClarkConnect box through your Network Neighborhood.



Configure Windows Network

Name	Server
Workgroup	Headquarters
Comment	ClarkConnect Enterprise Ed
WINS Server	192.168.2.16
WINS Support	No

Name

The name of the system as it appears on Windows Networks.

Workgroup

The Windows Network workgroup. If you are configuring your system as the primary domain controller (PDC) then this is also the name of the domain.

Comment

The comment is a short description for the system.

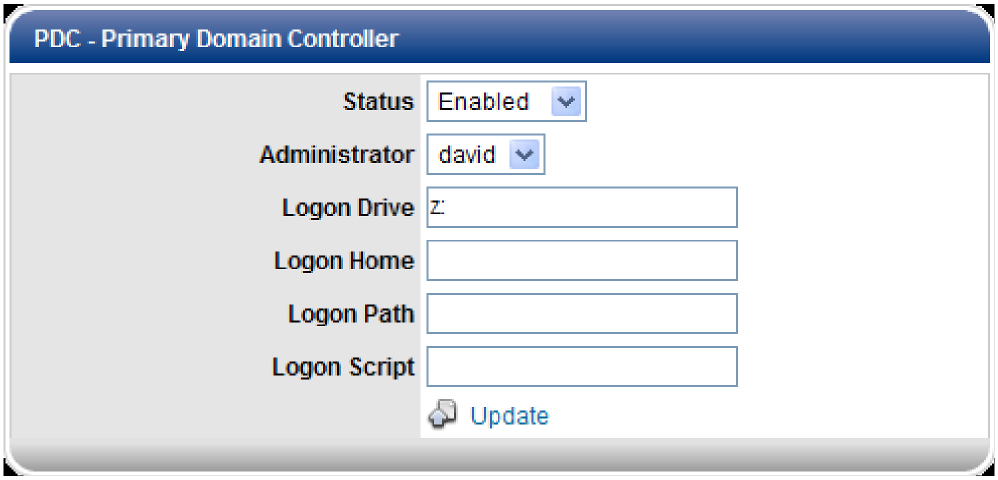
WINS Server / WINS Support

If you plan on using VPN or have more than two local networks, we strongly recommend that you enable a WINS server on your network. If you already have a WINS server, you can enter the IP address of the server in the ***WINS Server*** field. Alternatively, the ClarkConnect system can be configured as a WINS server on your network. Enable the ***WINS Support*** option. More information on WINS is available in this Howto.

PDC - Primary Domain Controller

If you would like your ClarkConnect system to act as a primary domain controller (PDC), you can configure the settings.

Note: You must be using version 4.1 or higher for PDC mode



PDC - Primary Domain Controller

Status	Enabled
Administrator	david
Logon Drive	Z:
Logon Home	
Logon Path	
Logon Script	
	Update

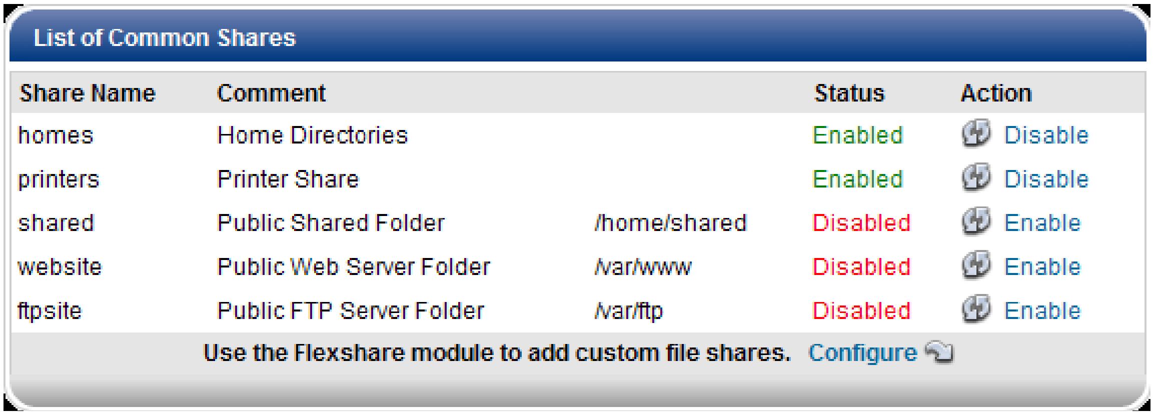
Status

Toggle this field to enable/disable PDC mode.

Administrator

Select a user account for PDC administration. This account will be used to add computers systems to the domain.

Common File Shares



List of Common Shares

Share Name	Comment		Status	Action
homes	Home Directories		Enabled	Disable
printers	Printer Share		Enabled	Disable
shared	Public Shared Folder	/home/shared	Disabled	Enable
website	Public Web Server Folder	/var/www	Disabled	Enable
ftpsite	Public FTP Server Folder	/var/ftp	Disabled	Enable

Use the Flexshare module to add custom file shares. Configure

- The ***homes*** folder contains private user folders.
- The ***printers*** icon will appear if you configure a shared printer.
- The ***shared*** folder is for public file sharing.
- The ***website*** folder contains the files for your web site.
- The ***ftpsite*** folder contains the files for your web site.

LAN Backup and Recovery

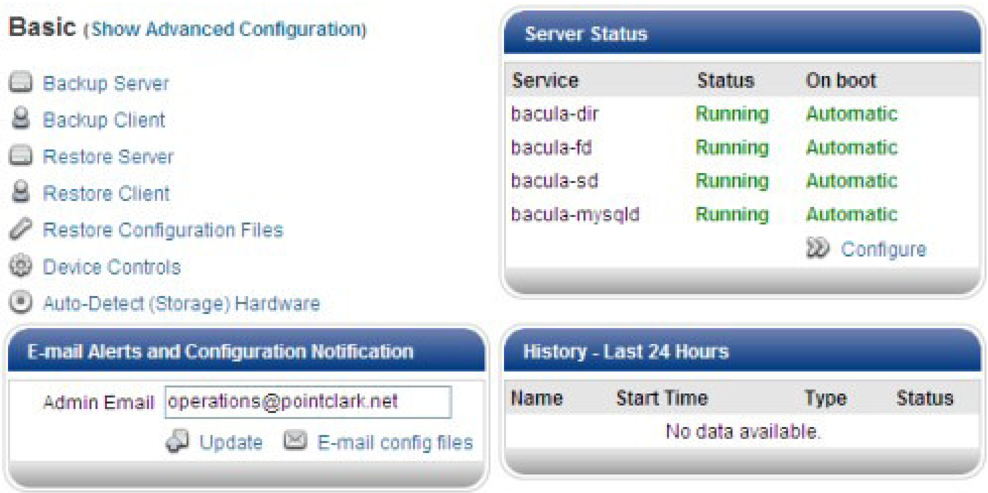
Description	Client/server backup and recovery.
Package Name	cc-bacula
Configuration Page	Software File Services LAN Backup/Recovery

Bacula is a network-based backup program. It allows an administrator to backup, recover and verify data on any number of systems on a local area network (and across VPN tunnels), on a variety of operating systems. Bacula supports various storage media devices, including file, tape, removable HDD.

Supported Media

ClarkConnect's implementation of the Bacula backup/restore software is customized to support a limited selection of hardware.

- The server's hard disk - obviously not recommended for server backup
- Iomega REV (35GB and 70GB) with the following interfaces:
- IDE/ATAPI
- USB
- SATA
- USB Mass Storage Device (USB drives, memory sticks etc.)
- Another workstation on the LAN
- DVD (beta)



Basic (Show Advanced Configuration)

- Backup Server
- Backup Client
- Restore Server
- Restore Client
- Restore Configuration Files
- Device Controls
- Auto-Detect (Storage) Hardware

Server Status

Service	Status	On boot
bacula-dir	Running	Automatic
bacula-fd	Running	Automatic
bacula-sd	Running	Automatic
bacula-mysqld	Running	Automatic

Configure

E-mail Alerts and Configuration Notification

Admin Email: operations@pointclark.net

Update   E-mail config files

History - Last 24 Hours

Name	Start Time	Type	Status
No data available.			

Print Server

Print Server Information	
Description	A print server.
Package Name	cc-cups
Configuration Page	Software Printing Print Server

ClarkConnect includes the Cups - the Common Unix Printing System - as well as a large set of printer drivers.

Configuration

Configuration of the printing system is done using the Cups web interface. You can access this interface via the ClarkConnect web-based interface.

As a security precaution, the Cups web interface is only accessible on a trusted (LAN) network. You can not access the web interface from a remote Internet connection.

Cups and Samba

When you configure a new printer with Cups, it will appear as a shared printer in Windows Network Neighborhood (if Samba is installed). However, you will need to restart the Samba service after adding a new printer.

Web Proxy
Access Control

Web Proxy Access Control Information	
Description	Time and user-based access control for the web proxy.
Package Name	cc-squid-acl
Configuration Page	Software Proxy and Filtering Access Control

Time-based Access Control allows an administer to enforce time-of-day web access to users or computers (IP or MAC address) using the web proxy.

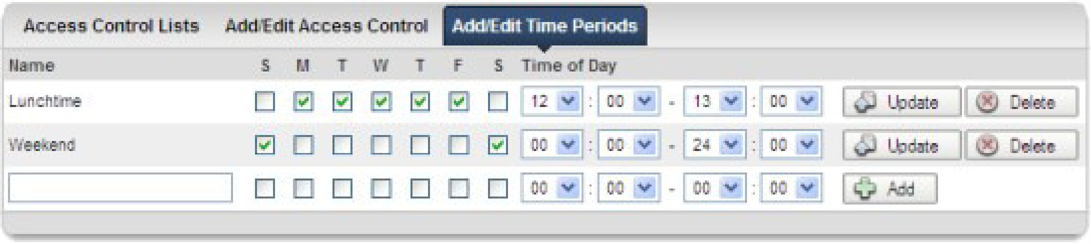
Adding Time Periods

Time periods define the day of week (i.e. Monday, Tuesday ...) and the time of day (i.e. 12:00 - 13:00) that an access control rule should apply. Select ***Add/Edit Time Period*** from the webconfig tab menu to:

- display and/or edit a currently defined time period
- add a new time period definition
- delete an existing time period definition

Note: Deleting a time period will delete any access control rule that depends on the time period definition being deleted.

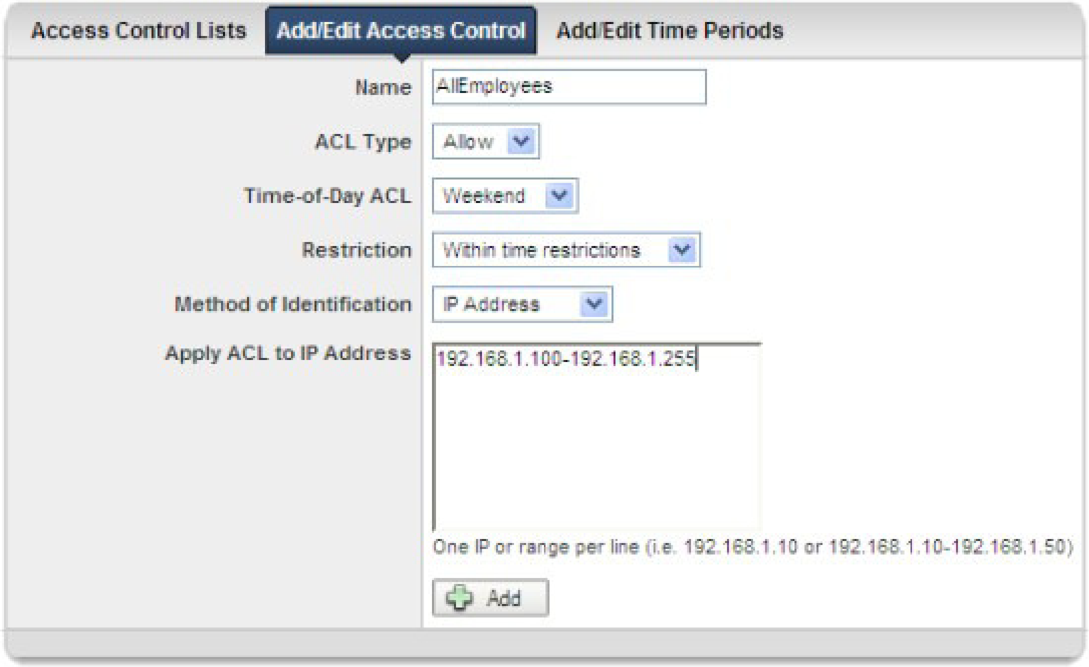
In the sample screenshot below, we have created two time period definitions. The first defines a lunch break on weekdays between 12:00pm and 1:00pm (13:00). The second covers the entire day over a weekend (Saturday and Sunday).



Name	S	M	T	W	T	F	S	Time of Day		
Lunchtime	☐	☑	☑	☑	☑	☑	☐	12 : 00 - 13 : 00	Update	Delete
Weekend	☑	☐	☐	☐	☐	☐	☑	00 : 00 - 24 : 00	Update	Delete
	☐	☐	☐	☐	☐	☐	☐	00 : 00 - 00 : 00	Add	

Adding Access Control Lists

An unlimited number of access control list definitions can be created to customize precisely how users or machines on the LAN should be given access to the web via the proxy server. In the example below, a rule to allow all machines on the LAN to have access to the web during the weekend is being created. By specifying an internal IP range of 192.168.1.100 to 192.168.1.255, the IP based identification will apply this rule to all computers on the LAN receiving a DHCP lease in this IP range.



Name: AllEmployees

ACL Type: Allow

Time-of-Day ACL: Weekend

Restriction: Within time restrictions

Method of Identification: IP Address

Apply ACL to IP Address: 192.168.1.100-192.168.1.255

One IP or range per line (i.e. 192.168.1.10 or 192.168.1.10-192.168.1.50)

Name
A unique name identifying the access control.

ACL Type
Sets the ACL rule type - allow or deny. ***Allow*** provides web access to the user/computer...***Deny*** forbids web access.

Time-of-Day ACL
References a unique time of day rule. The drop down menu will be empty and a link to create a new time period will be displayed if no time definitions have been created.

Restriction
Determines whether the ACL rule will apply to the time period defined or all time ***outside*** of the time period defined. For example, if you defined a time period name ***Lunchtime*** that was defined as 12:00 - 13:00 from Monday to Friday and you wanted a specific rule to apply during the lunch hour, select ***Within***. Conversely, if you wanted a rule to be applied for all hours outside of the lunch period, you would select ***Outside***.

Method of Identification
Depending on your proxy configuration, up to three different methods of user/machine identification are possible - username, IP address and MAC address.

Username
Username-based authentication is only available if you have User Authentication enabled. Users must provide login credentials *and* have access to the proxy server (as defined by the User Options configuration). Once logged into a proxy session, ACL rules based on username will apply.

IP Address
To restrict web access to a particular computer or multiple computers (i.e. a computer lab), IP address based identification can be used. A single IP address or a range of IP addresses (separated by a dash) can be added. Valid entry examples include:

- 192.168.1.100
- 10.0.0.121

- 192.168.1.100-192.168.1.150

The IP address represents the address of the machine connecting to the proxy. Since the computer is located on the LAN segment of the network, any IP address or range listed here should be restricted to an internal IP address or range.

MAC Address

A MAC address is a unique identifier originating from a computer's network card. MAC addresses can be a good alternative to IP addresses if an administrator does not lock down the network settings of a machine which might allow a savvy user to get around an IP address-based access control rule. A MAC address must be obtained from the machine and is dependent on the OS.

Banner Ad and Pop-up Blocker

Banner Ad and Pop-Up Blocker Information	
Description	The software blocks banner ads and pop-ups at the gateway.
Package Name	cc-privox
Configuration Page	Software Proxy and Filtering Web Proxy

The software filters cookies, ads, banners, pop-ups, and other unwanted Internet content.

Configuration

If you use ClarkConnect as a gateway, you can configure the banner ad blocker in transparent mode. In other words, it is not necessary to change the settings for all the web browsers on the PCs on your network.

- ***Step 1*** - Install the required Web Proxy server
- ***Step 2*** - From Web Proxy's web-based administration page, set the proxy to transparent mode.
- ***Step 3*** - From Banner Ad administration page, enable banner ad blocker integration.

Content Filter

Content Filter Information	
Description	A smart and robust web content filter.
Package Name	cc-dansguardian
Configuration Page	Software Proxy and Filtering Content Filter

The content filtering software blocks inappropriate websites from the end user. The software can also be used to enforce company policies; for instance, blocking personal webmail sites like Hotmail can decrease lost productivity at the office.

The filter engine uses a variety of methods including phrase matching, URL filtering and black/white lists. Although the filter works effectively 'out-of-the-box', for best results, we recommend subscribing to a service level includes the 'Content Filter Update' service (see Services link below). By keeping your blacklist up-to-date, you will be providing your LAN with the most effective blocking solution against the 'churn' of sites that change daily.

Installation

If you did not select this module to be included during the installation process, you must first install the module.

Configuration

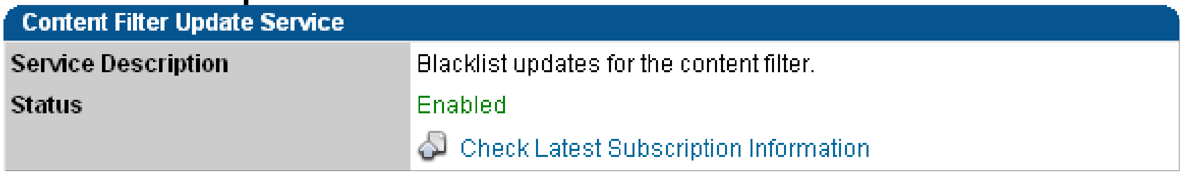
The web-based administration tool gives you access to a number of configuration settings. The filter ***must*** be run in parallel with the Web Proxy server.

It is important to understand the implications of running the content filter with a web proxy server configured to run in ***standard*** mode.

Standard Mode
In standard mode, the web proxy operates on port 3128 and the content filter operates on port 8080.

Transparent Mode
In transparent mode, all requests from the local network automatically pass through the web proxy cache. The settings for the local machines do not need to be changed. By-passing the proxy is not possible by changing browser settings on the local machine. Obviously, this is the preferred configuration.

Content Filter Update Service



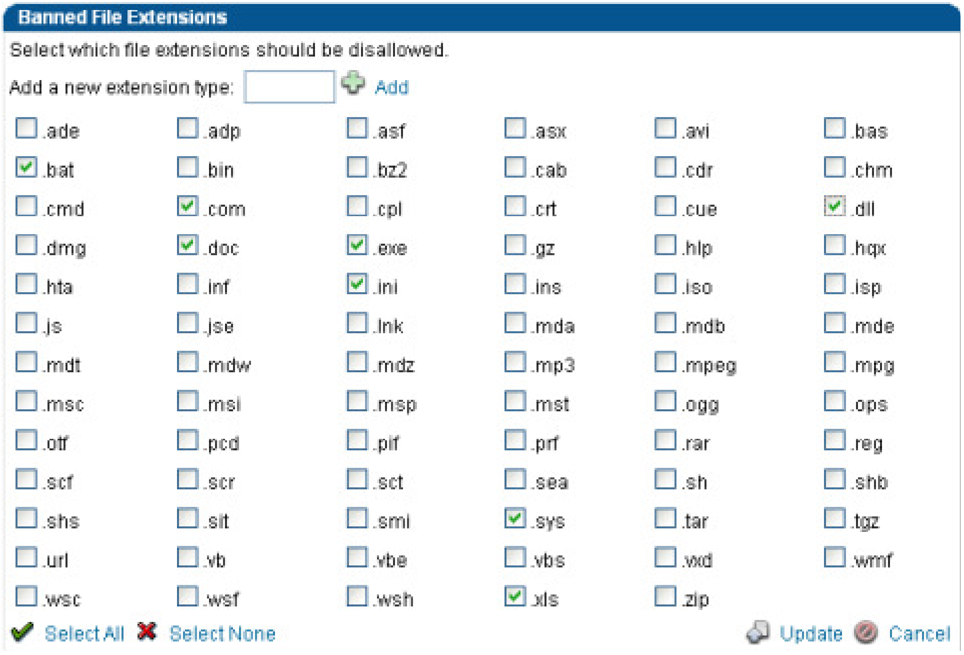
Content Filter Update Service	
Service Description	Blacklist updates for the content filter.
Status	Enabled
	Check Latest Subscription Information

If you have a subscription to the "Content Filter Blacklist Update" service (enabled through your ClarkConnect Gateway Service account) you can check to make sure the update service is active.
If the update service is activated, you will see a screen capture similar to that shown below.
Updates are pulled or pushed automatically from the ClarkConnect Gateway Service network approximately every week.

Configure Advanced Filtering

Banned File Extensions / Banned MIME Types

Banned File Extensions
Banning specific file extensions is a useful tool for limiting content available to users on the LAN. It can also greatly decrease the chances of users unwittingly downloading and running 'arbitrary' code downloaded from the Internet which could potentially contain viruses, spyware of other malicious code.



Banned File Extensions

Select which file extensions should be disallowed.

Add a new extension type: [ ] Add

□ .ade	□ .adp	□ .asf	□ .asx	□ .avi	□ .bas
☑ .bat	□ .bin	□ .bz2	□ .cab	□ .cdr	□ .chm
□ .cmd	☑ .com	□ .cpl	□ .crt	□ .cue	☑ .dll
□ .dmg	☑ .doc	☑ .exe	□ .gz	□ .hlp	□ .hqx
□ .hta	□ .inf	☑ .ini	□ .ins	□ .iso	□ .isp
□ .js	□ .jse	□ .lnk	□ .mda	□ .mdb	□ .mde
□ .mdt	□ .mdw	□ .mdz	□ .mp3	□ .mpeg	□ .mpg
□ .msc	□ .msi	□ .msp	□ .mst	□ .ogg	□ .ops
□ .otf	□ .pcd	□ .pif	□ .prf	□ .rar	□ .reg
□ .scf	□ .scr	□ .sct	□ .sea	□ .sh	□ .shb
□ .shs	□ .sit	□ .smi	☑ .sys	□ .tar	□ .tgz
□ .url	□ .vb	□ .vbe	□ .vbs	□ .vxd	□ .wmf
□ .wsc	□ .wsf	□ .wsh	☑ .xls	□ .zip	

By checking a box next to an extension, you are ***disallowing*** filtered users from accessing this file type. If you wish an extension to be blocked and it is not listed in the available list, add it to the list using the "Add a new extension type" form.

Banned Site List / Exempt Site List

Banned Site List

Sites entered in the "Banned Site List" will be banned, regardless of the site's content, or whether the site is on one of the blacklists.

Exempt Site List

Sites entered in the "Exempt Site List" will be allowed, regardless of the site's content. Use this form if content on a site triggers a 'false positive' that you wish to override.

Banned User IP List / Exempt User IP List

If you have some or all of your workstations configured to use static IP addresses, you can configure individual workstations' access to the web.

Banned User IP List

Here you can configure LAN IP addresses that will be completely blocked from accessing the web.

You can either add IP addresses individually or add groups as defined below.

Exempt User IP List

Here you can configure LAN IP addresses that will be granted ***completely unfiltered*** access to the web. You can either add IP addresses individually or add groups as defined below.

Groups

You can configure groups of IP addresses to simplify and organize workstation access to the web.

For example in an educational environment you can add all administrator/staff IP addresses to a ***Staff*** group and add them to the Exempt User IP List.

Weighted Phrasing

The content filter system uses phrase lists to calculate a score for every web page. You can fine tune your content filter scoring by specifying which phrase lists to use.
In general you will want the phrase lists you select here to correspond with the blacklists you are using. At a minimum you will want to include the ***proxies*** phraselist to prevent your users from bypassing the filter.

Blacklists

The content filter system uses black lists to block specific web sites. You can fine tune your content filter black lists by specifying which lists to use. Note that these lists are updated weekly by the ***Content Filter Update Service*** if you have subscribed to that service.

Configure Filter

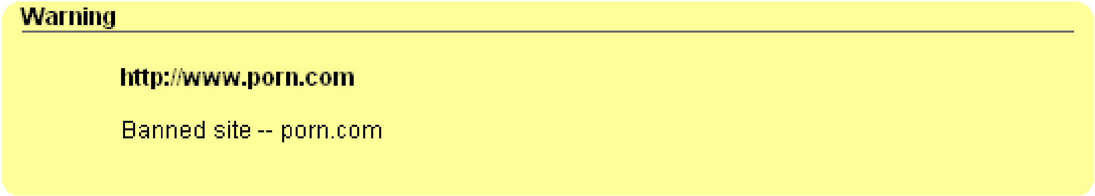
Language - If your native language is supported by the DansGuardian content filter, you can configure the filter to use your language when displaying block reports to your users and error messages.

Sensitivity Level - The sensitivity level is an arbitrary scale that allows 'coarse' adjustment of the phrase filter sensitivity. Increasing the sensitivity level means that fewer bad phrases/words will cause the filter to block the page.

PICS Level - An Internet standard for rating web content. This setting will prove to be of minor significance as sites self-administrate this parameter. As a general rule, the recommendation is to disable this setting.

Reporting Level - Five options are available to customize what a user 'sees' when the filter blocks a page:

- Stealth Mode - Site is not blocked...User's IP and site is logged (/var/log/dansguardian/access.log)
- Access Denied - User's browser will receive an 'Access Denied' in place of the web page.
- Short Report - A short error message 'bubble' will be displayed like the one below:



Warning

http://www.porn.com

Banned site -- porn.com

Full Report - Same as above, but the weighted limit and actual value will be displayed (useful for fine-tuning the system).

- Custom Report - Uses the customizable HTML template located at /etc/dansguardian/languages/[language] where language is the language you have selected in the setting above. The HTML template file is template.html and the default en_US language folder is /etc/dansguardian/languages/ukenglish.

Block IP Domains - Used to prevent users from circumnavigating the URL-based portion of the filter by using IP addresses instead of URL's. Pages will still be filtered based on the other filtering mechanisms: weightedphrases, mime types, file extensions etc

Blanket Block - Most restrictive setting. All sites will be blocked with the exception of those listed in the exempt list. Useful for kiosks/public terminals where a browser is used to access a company site etc.

Web Proxy

Web Proxy Information	
Description	Web proxy cache server.
Package Name	cc-squid

Configuration Page	Software Proxy and Filtering Web Proxy

Squid is a high-performance proxy caching server for web clients, supporting FTP, gopher, and HTTP. The software not only saves bandwidth and speeds up access time, but also gives administrators the ability to track web usage in the daily report.

General Settings

Maximum Cache Size

The maximum size on your hard disk to use for the proxy server cache.

Maximum Object Size

Any file (image, web page, PDF, etc) above the maximum object size will still go through the proxy but will not be cached. Large files (for instance, a movie file) can take up a lot of space in your proxy cache. If you have a cache size of 2 Gb and two people happen to download 1 Gb files at the same time, then these two files would replace everything else in your cache. You can limit the maximum object size to prevent this situation.

Maximum Download File Size

If you want to limit downloads of large files (for instance, movies) you can set a maximum size. Any file above this limit will get blocked.

Reset Cache

Use the ***reset cache*** button to delete all the files currently stored by the web proxy server.

Mode

The web proxy and content filter work together to filter web traffic on your network. The combination of these two applications can operate in several different modes.

Off

This mode is typically used to either temporarily disable the web proxy service or implement a custom proxy configuration file. Web traffic can still continue to flow un-proxied on port 80, while access to port 3128 (web proxy) and port 8080 (content filter) are also available.

Off + Content Filter

In this mode, all workstations on the local network ***must*** be configured to use port 8080 (content filter) as the proxy server. In other words, the only way a person can access the web is by configuring their web browser to go through the content filter.

On

This mode is typically used to take advantage of the improved bandwidth usage and speed of a proxy server. In ***transparent mode***, all web requests from the local network automatically pass through the proxy. No configuration changes are required on the workstations.

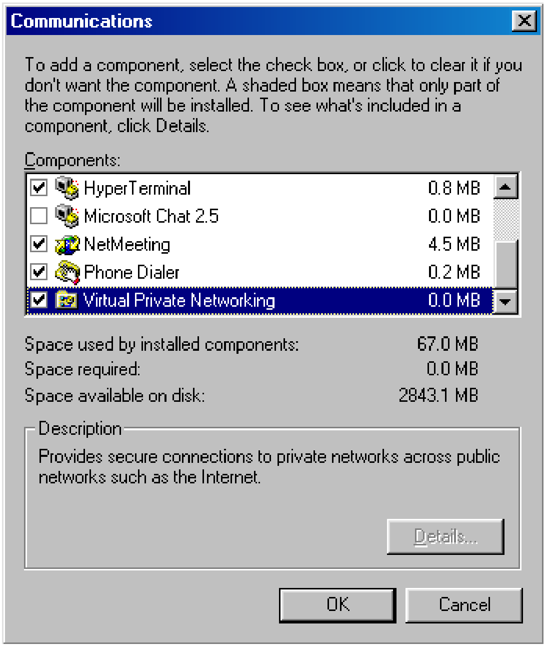
On + Content Filter

This mode is typically used to enforce content filtering without the need to make configuration changes on the workstations. As soon as you enable this mode, all web traffic going through your gateway goes through the content filter.

VPN

PPTP

VPN Server - PPTP Information	
Description	Virtual Private Network PPTP server.
Package Name	cc-pptp
Configuration Page	Software VPN PC-to-LAN



Communications

To add a component, select the check box, or click to clear it if you don't want the component. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.

Components:

☑	HyperTerminal	0.8 MB
□	Microsoft Chat 2.5	0.0 MB
☑	NetMeeting	4.5 MB
☑	Phone Dialer	0.2 MB
☑	Virtual Private Networking	0.0 MB

Space used by installed components: 67.0 MB
Space required: 0.0 MB
Space available on disk: 2843.1 MB

Description

Provides secure connections to private networks across public networks such as the Internet.

The PPTP server is a secure and cost effective way to provide road warrior VPN connectivity. The PPTP VPN client is built-in to Windows 98, ME, 2000, and XP. No extra software is required and ClarkConnect provides full password and data encryption.

Configuring the PPTP Server

Local IP and Remote IP

You must select a range of LAN IP addresses for the PPTP VPN connections. This range should be on the same network as your local area network. By default, the DHCP Server on ClarkConnect only uses IP addresses above x.x.x.100. All addresses below this number are reserved for static use. We strongly suggest you use this sub-100 static range for PPTP.

Encryption Key Size

Most PPTP VPN clients support the stronger 128-bit encryption key. However, some VPN clients (especially hand-held computers and mobile phones) can only support 40-bit encryption. Change the encryption key size to meet your needs.

Domain

The default domain used by the PPTP client.

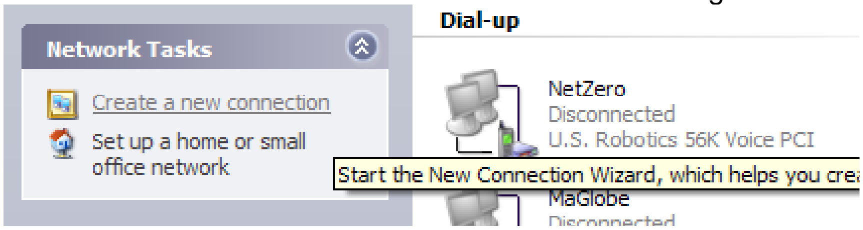
WINS Server

The Microsoft Networking WINS server used by the PPTP client. Depending on your network configuration, you may need to specify the WINS settings in VPN client configuration

Configuring Windows XP

The PPTP client is built-in to Windows XP.

- Go to the ***Control Panel***.
- Click on ***Network Internet Connections*** (this step may not be necessary.
- Click on ***Network Connections***.
- Click on ***Create a New Connection*** to start the configuration wizard (see screenshot).

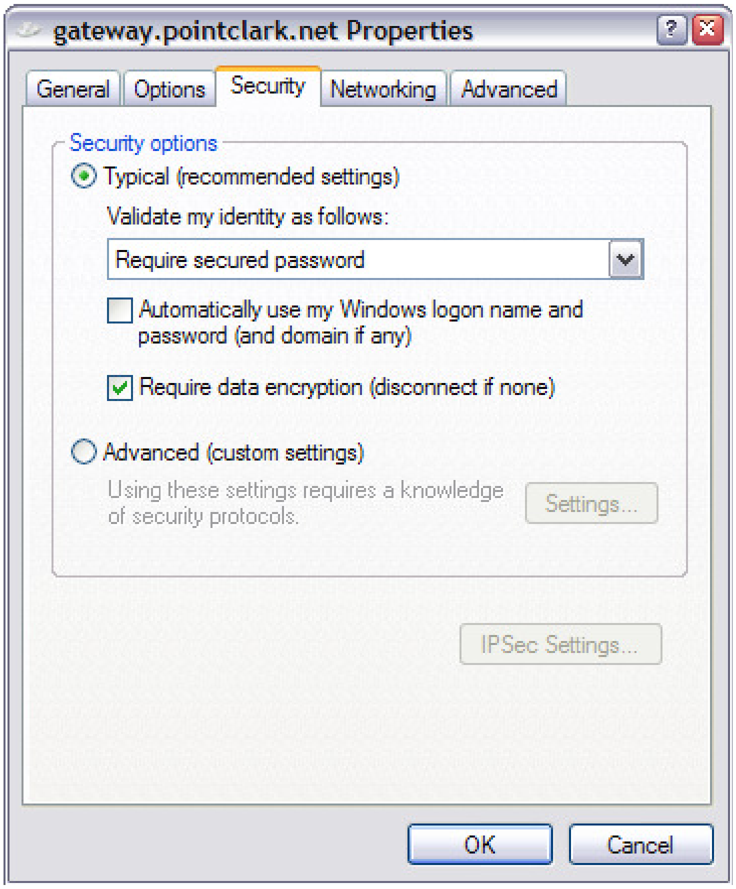


Start the New Connection Wizard, which helps you crea

- Select ***connect to the network at my workplace***.
- Select ***Virtual Private Network connection***.
- Add a connection name, and dial settings, and hostname.
- Click on the ***Properties*** button (or right-click on the new connection, and select ***Properties*** from the menu.

- Select the ***Security***

- Make sure ***Require data encryption*** is selected.


gateway.pointclark.net Properties

Security options

● Typical (recommended settings)

Validate my identity as follows:

Require secured password

□ Automatically use my Windows logon name and password (and domain if any)

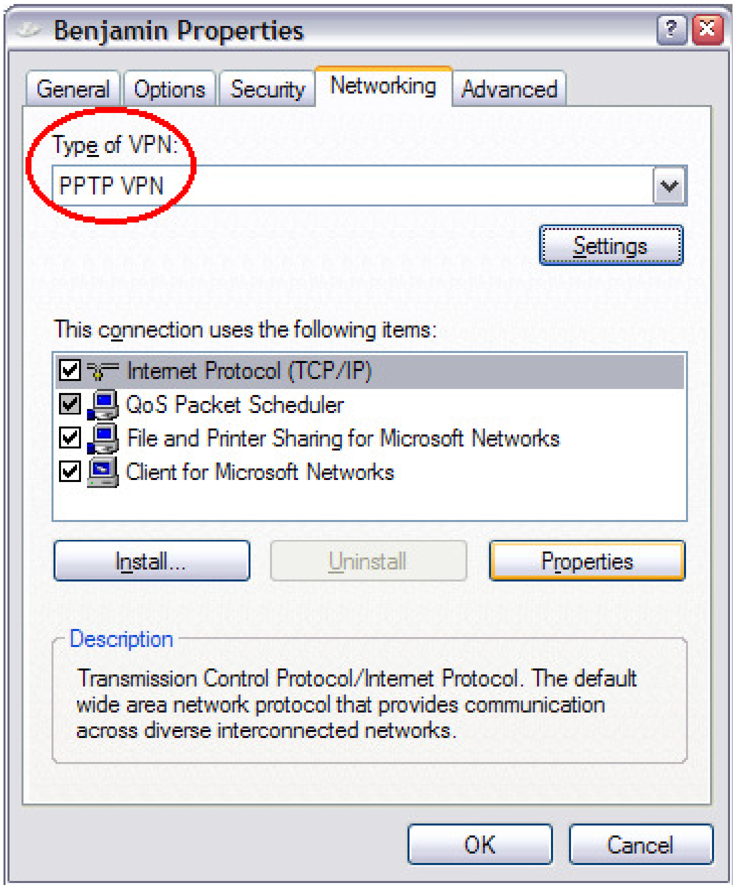
☑ Require data encryption (disconnect if none)

○ Advanced (custom settings)

Using these settings requires a knowledge of security protocols.

Select the ***Networking*** tab.

- From the ***Type of VPN*** drop box, select ***PPTP VPN***.



Type of VPN: PPTP VPN

This connection uses the following items:

☑ Internet Protocol (TCP/IP)
☑ QoS Packet Scheduler
☑ File and Printer Sharing for Microsoft Networks
☑ Client for Microsoft Networks

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

IPsec

VPN Server - IPSec Information	
Description	Virtual Private Network tools for LAN-to-LAN connections.
Package Name	cc-ipsec
Configuration Page	Software VPN LAN-to-LAN

You can use the web-based administration tool to create a connection with other ClarkConnect servers (on licensed systems, dynamic IP support is included).

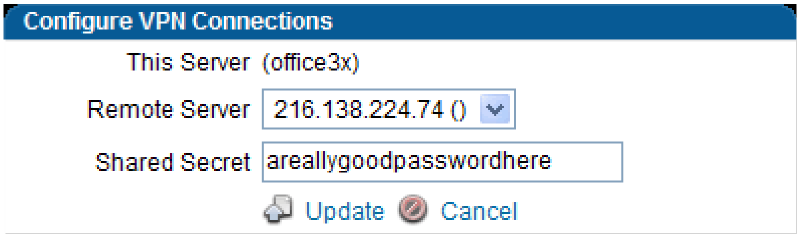
Configuring Connections with Managed VPN

Managed VPN support not only simplifies configuration, but also improves the up-time of the connections. In order to create a connection between to systems, you need to configure ***both*** ClarkConnect systems.

If you are configuring a VPN connection between your local gateway and a remote gateway, then configure the remote gateway ***first***. Once the VPN is started on the remote system it will only be accessible when the VPN connection is up. If run into trouble configuring the tunnel, you can use a dial-up or other location to access the remote location.

From the web-based administration tool, click on ***Create*** in the Managed VPN Connections box. You need to:

- Select the IP address of the remote connect
- Type in a pre-shared secret (password)



Configure VPN Connections

This Server	(office3x)
Remote Server	216.138.224.74 ()
Shared Secret	areallygoodpasswordhere

On the first connection or when an IP address changes, it may take a few minutes for the connection to synchronize.

The two LAN networks at either end of the VPN connection must not overlap! If you need to change the LAN IP address/network on your ClarkConnect server, please use the Administration Console.

Gather Network Information

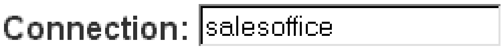
You must gather some network information for the IPsec server configuration, namely: the IP address, next hop (gateway), and network for both sides of the network. Make sure these settings are correct -- you will save many hours of pain and frustration. The information for the local ClarkConnect system is shown when you start to configure an unmanaged VPN connection.

The two LAN networks at either end of the VPN connection must not overlap! If you need to change the LAN IP address/network on your ClarkConnect server, please use the Administration Console

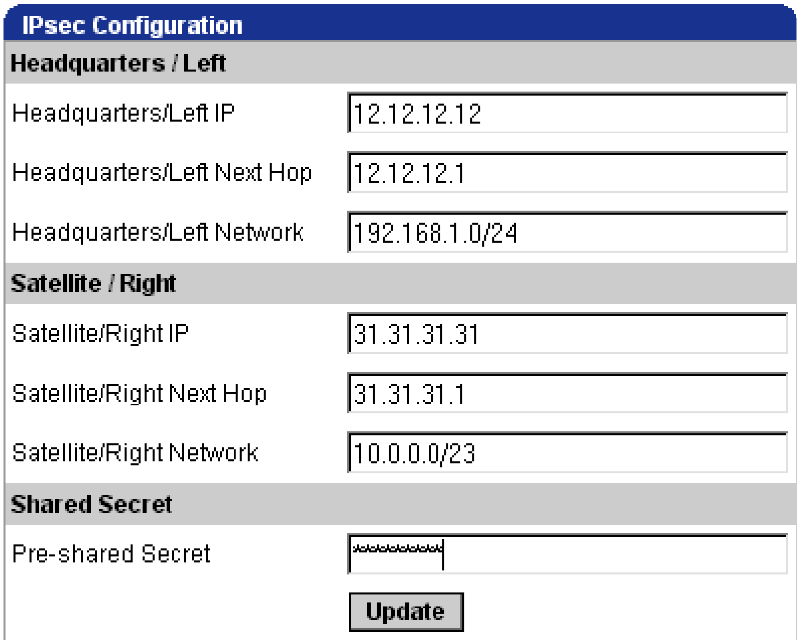
Select a Connection Name and Pre-Shared Secret

Once you have your network settings in hand, enter the information on both ends of the VPN connection. Enter a simple nickname for the connection along with a strong pre-shared secret.

When configuring the other end of the VPN connection, do not be tempted to swap the Headquarters and Satellite information! The configuration screens on both ends of the connection will look ***exactly*** the same.



Connection: salesoffice



IPsec Configuration

Headquarters / Left	
Headquarters/Left IP	12.12.12.12
Headquarters/Left Next Hop	12.12.12.1
Headquarters/Left Network	192.168.1.0/24
Satellite / Right	
Satellite/Right IP	31.31.31.31
Satellite/Right Next Hop	31.31.31.1
Satellite/Right Network	10.0.0.0/23
Shared Secret	
Pre-shared Secret	*********

Photo Gallery

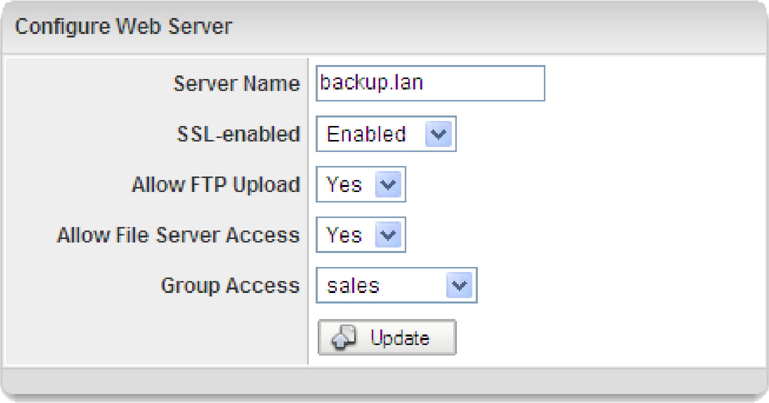
Photo Gallery Information	
Description	A web-based photo album.
Package Name	cc-gallery
Configuration Page	Software Fun Photo Gallery

Gallery is a web based photo album that provides you with the ability to create and maintain your own online photo collection via an intuitive web interface.

Web Server

Web Server Information	
Description	A powerful and popular web server.
Package Name	cc-httpd
Configuration Page	Software Web Web Server

ClarkConnect includes the Apache web server -- the same software that powers many of the world's largest websites.



Configure Web Server

Server Name	backup.lan
SSL-enabled	Enabled
Allow FTP Upload	Yes
Allow File Server Access	Yes
Group Access	sales

Configuration

General

Global

The basic set-up of the Apache web server is installed by default. In the main configuration, you need to specify two items:

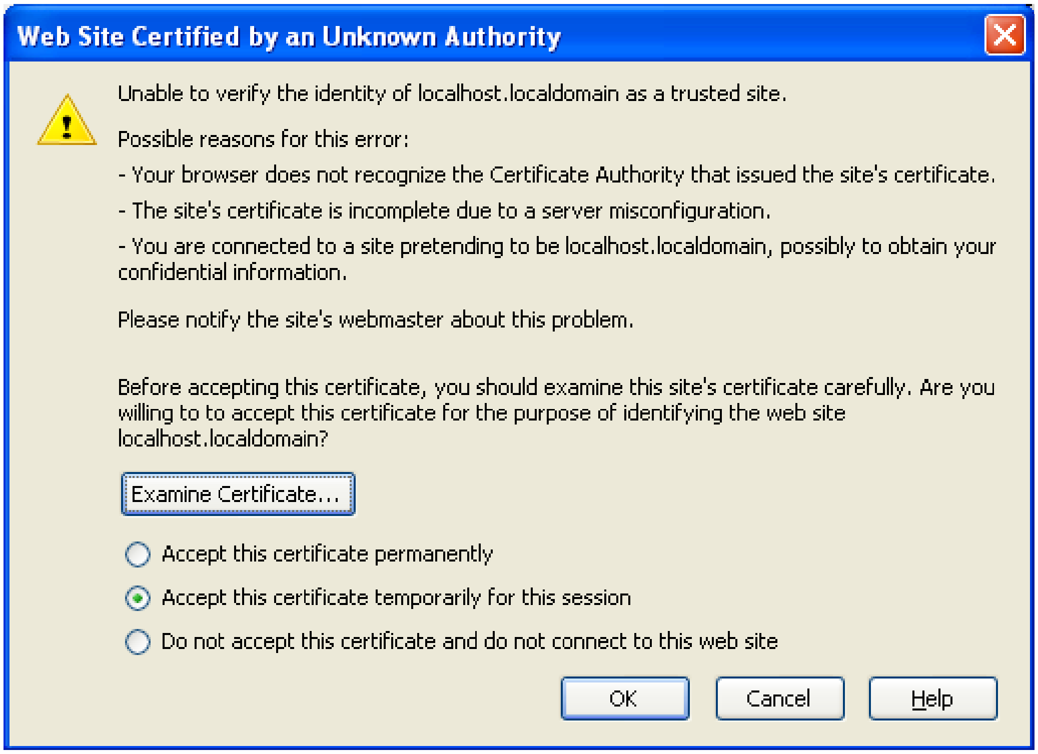
Server Name

The server name is a valid name (for example, www.example.com) for your web server. This name is used on some infrequently used error pages, so it is not all that important.

SSL-Enabled - Secure Site

The web server comes with built-in SSL encryption for enhanced security. If your website requires a username and password for login, then it is a good idea to use encryption. For instance, if you have the webmail or groupware solution installed, you should access their respective login pages via the secure web server. In your web browser, you should use the encrypted ***https://your.domain.com*** instead of the un-encrypted ***http://your.domain.com*** (https vs http). When enabled, all communication between the web server and user's web browser is encrypted using a 128-bit security key.

SSL encryption requires a web site certificate. ClarkConnect automatically generates a default certificate that is 100% secure. However, this certificate is not verified by one of the web site certificate authorities (it costs at least $100 per year to maintain a verified web site certificate). Your users will see the following warning (or similar) when connecting to the secure web server.



Web Site Certified by an Unknown Authority

Unable to verify the identity of localhost.localdomain as a trusted site.

Possible reasons for this error:

- Your browser does not recognize the Certificate Authority that issued the site's certificate.

- The site's certificate is incomplete due to a server misconfiguration.

- You are connected to a site pretending to be localhost.localdomain, possibly to obtain your confidential information.

Please notify the site's webmaster about this problem.

Before accepting this certificate, you should examine this site's certificate carefully. Are you willing to to accept this certificate for the purpose of identifying the web site localhost.localdomain?

○ Accept this certificate permanently

● Accept this certificate temporarily for this session

○ Do not accept this certificate and do not connect to this web site

Allow FTP Upload
Enables an administrator/user to upload or change content on the website via FTP. By default, the FTP uses a non-standard port of 2121. A user must be created on the server with FTP access in order to provide authentication credentials to login to the FTP server. Any user belonging to the group configured in the Group Access setting will have read/write access to the website directory.
You must use an FTP client (rather than a browser) if you would like to upload files to the server.

Reports

Current Status

Current Status Information Information	
Description	Disk load, system load, memory usage, and other system status.
Package Name	cc-status
Configuration Page	System System Information Current Status

Dashboard

Dashboard Information	
Description	The dashboard shows a big picture overview of your system.
Package Name	cc-webconfig
Configuration Page	Dashboard Overview

The dashboard page is a bird's eye view of your system.

Intrusion Detection

Intrusion Detection Information	
Description	A report displaying summary information on the intrusion detection system.
Package Name	cc-snort
Configuration Page	Reports Reports Intrusion Detection

The intrusion detection report provides a way to analyze hostile traffic arriving on your network interfaces.

Logs

Logs Information	
Description	Log viewer.
Package Name	cc-reports
Configuration Page	System System Information Logs

The log report page allows you to view and filter detailed log files on your system.

SMTP Mail

SMTP Mail Report Information	
Description	A report displaying summary information on the mail server.
Package Name	cc-postfix
Configuration Page	Reports Reports SMTP Mail

Statistics

System Statistics Information	
Description	Historical information on system performance.
Package Name	cc-mrtg
Configuration Page	Reports System Information Statistics