

Before you begin...

You will need:

- Microsoft Internet Explorer version 6, 7 or 8
- Mozilla Firefox version 3 or higher
- A hub or switch, or an Ethernet crossover cable.

Decide on your network configuration

The diagram to the right shows a typical deployment.

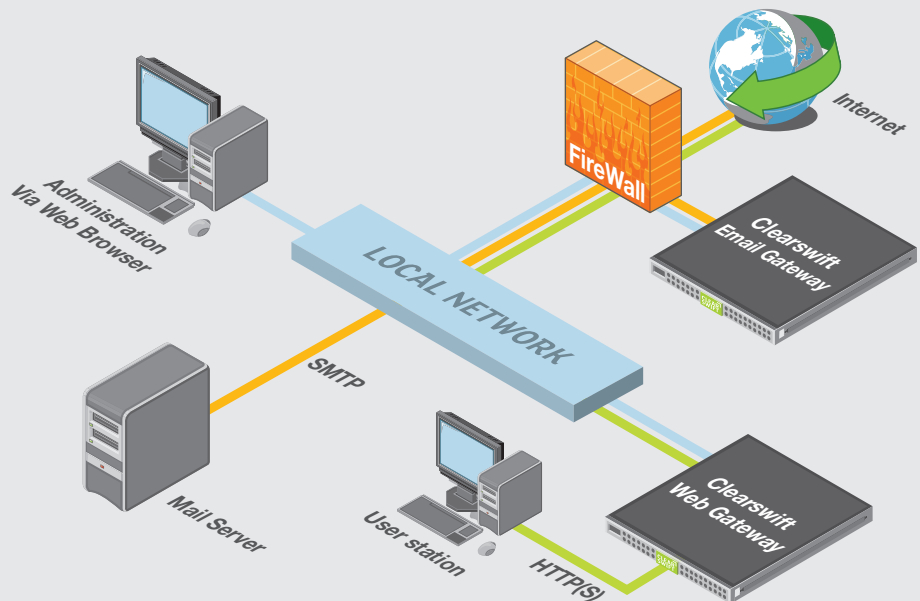
Gather basic system information

You will need to supply some basic information about your Clearswift Gateway and its network configuration for the setup wizard.

We recommend you gather the information listed in the attached setup wizard table before you start.

License information

You should have already received your product (or evaluation) License Key from your Catalyst Partner or Clearswift. Should you require confirmation of your License Key please contact your local sales office.



Routing Web Traffic

Configure client browsers to use the Clearswift Web Gateway(s) by changing their browser settings as necessary or use a PAC script.

The Clearswift Web Gateway can also be used in **transparent mode** in conjunction with a switch that supports routing HTTP traffic.

Routing Email Traffic

Change your organization's DNS MX record to route inbound email to the Clearswift Email Gateway.

Configure your corporate mail server to route outbound email to the Clearswift Email Gateway.

1. Connecting your Clearswift Gateway

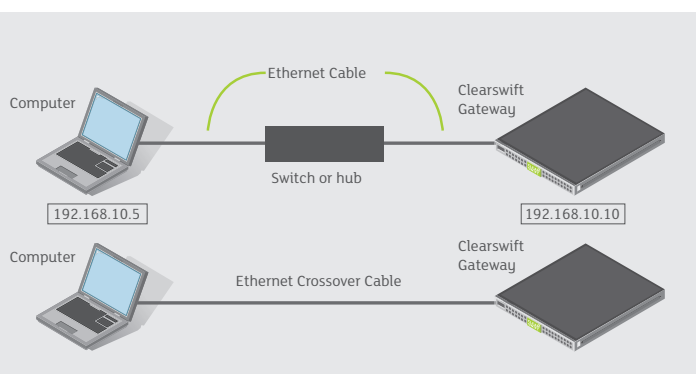
Do not install any of the Dell software from the supplied CD's unless instructed to by a Clearswift or Dell technician as the system comes pre-loaded.

- Install the Gateway in a system rack, if required
- Connect the Gateway to power, turn on and allow the system to configure itself.

This stage will take a maximum of 10 minutes and will cause the Gateway to automatically reboot itself.

2. Connecting your computer

1. The Clearswift Gateway NIC1 network interface card is set by default to IP address 192.168.10.10. To enable your computer to connect to the Gateway, configure the computer with these TCP/IP settings:
 - Static IP address: 192.168.10.5
 - Subnet mask: 255.255.255.0
2. Connect the computer to the NIC1 connector on the Clearswift Gateway, via a switch or hub, or directly through an Ethernet crossover cable.



3. Start the Setup wizard

Once the computer is connected to the Clearswift Gateway, type the following URL into Internet Explorer or Mozilla Firefox:

https://192.168.10.10 to complete the Gateway Setup wizard:



4. Connecting your Clearswift Gateway

Disconnect the computer you connected in Step 2, and connect the Gateway to your network using the NIC1 connector (and NIC2 if you configured the second NIC). Bridging mode for proxied web traffic, with one NIC internal facing and the other NIC external facing, is not supported.

5. Starting the Clearswift Gateway web interface

Reconnect to the Gateway using its new address given to it during the setup wizard, e.g. **https://ip_address**. Login to the system using the admin account and password.

If you are unable to access the system and are sure you have entered the correct credentials, then it is possible the setup wizard may still be running, wait for a minute and try again.

For suggested firewall settings please see the table on the next page.

6. Check your system

The Clearswift Gateways contain features within the *System Centre* that allow customers to check their system configuration and make necessary amendments to integrate into your infrastructure.

See the Clearswift Gateway online help for guidance on modifying the configuration and using the *Connectivity Test* feature to identify any mis-configurations or environmental problems.

7. Configuring your system

The Gateways are grouped into separate logical sections "*Policy*", "*Messages*" (Clearswift Email Gateway only), "*Reports*", "*System*", "*Health*" and "*Users*".

The *Policy* centre allows administrators to define their corporate policy. The *Message* centre is where quarantined messages are managed and messages can be tracked. The *Report* center is where reports can be run, modified and scheduled for automatic delivery. The *System* centre is where you configure the product into your infrastructure. The *Health* centre displays system health status and the *User* centre is where you define administrative users and grant them access rights so that they can perform their roles securely.

The install wizard will install a default policy to enable you to start using the product almost instantly, but you should review the policy configuration by going to the "*Policy Routes*" page which is within the "*Policy*" centre and use the "*Show Printable Version*" to view the configuration.

Suggested Firewall Settings				
Port	Protocol	Direction	Required for	
20	TCP	Out	FTP over HTTP.	
20, 21	FTP	In/Out	Backup & Restore, if using an FTP server located beyond the firewall.	
22	TCP	In	SSH access to the Gateway Console.	
25*	TCP	Out	Outbound SMTP. If your system uses an alternative port, open that instead.	
53	TCP, UDP	Out	DNS requests, if using DNS servers beyond the firewall. Only allow outbound requests to the specified DNS servers, & responses from those servers.	
80	TCP	Out	Required for General Web Access. HTTP access to the Clearswift Update Server app-patches.clearswift.net for fetching software upgrades and Kaspersky anti-virus updates from kav-update-8.1.clearswift.net, kav-update-8.2.clearswift.net, kav-update-8.3.clearswift.net	
88	TCP, UDP	Out	User Authentication using Kerberos.	
123	UDP	Out	NTP, if you use an NTP server and it is beyond the firewall. Allow responses from the NTP server.	
135, 137, 139, 445	TCP	Out	User Authentication using NTLM.	
389	TCP	Out	LDAP Directory access.	
443	TCP	In	HTTPS access to the Gateway Web Interface.	
443	TCP	Out	Required for General HTTPS Web Access. HTTPS access to the Clearswift Update Server applianceupdate.clearswift.com for license management.	
636	TCP	In/Out	LDAP and SSL Connection to a non global catalog port. If you use LDAP servers beyond the firewall	
3268	TCP	Out	LDAP connection to an active directory global catalog port. If you use LDAP servers beyond the firewall.	
8071	TCP	In	HTTPS Client communication with the Master. The port is only open on the Master.	
9000	UDP	In/Out	Distribution of information to peer Gateways.	

20, 21	FTP	In/Out	Backup & Restore, if using an FTP server located beyond the firewall.
22	TCP	In	SSH access to the Gateway Console.
25	TCP	In/Out	SMTP.
53	TCP, UDP	Out	DNS requests, if using DNS servers beyond the firewall. Only allow outbound requests to the specified DNS servers, and responses from those servers.
80	TCP	In	HTTP access to the PMM interface, if you are using PMM
80	TCP	Out	HTTP access to the Kaspersky Update Server kav-update-8.1.clearswift.net, kav-update-8.2.clearswift.net, kav-update-8.3.clearswift.net HTTP access to the Clearswift Update Server app-patches.clearswift.net HTTP access to the Clearswift Bulk Mail Detection Servers bulkmail1.clearswift.net, bulkmail2.clearswift.net, bulkmail3.clearswift.net, bulkmail4.clearswift.net, and bulkmail5.clearswift.net for the classification of messages.
123	UDP	Out	NTP, if you use an NTP server and it is beyond the firewall. Allow responses from the NTP server.
389	TCP	Out	LDAP directory access, if you use LDAP servers beyond the firewall.
443	TCP	In	HTTPS access to the Gateway Web Interface and for communications between peer Gateways.
443	TCP	Out	HTTPS access to the Clearswift Update Server applianceupdate.clearswift.com for license management, handling Managed Lexical Expression Lists and for communications between peer Gateways.
3268	TCP	Out	LDAP connection to an active directory global catalog port. If you use LDAP servers beyond the firewall.
3269	TCP	In/Out	LDAP and SSL connection to an active directory global catalog port. If you use LDAP servers beyond the firewall
8007	UDP	In/Out	Access to the Clearswift TRUSTmanager Reputations server.
19200	UDP	In/Out	Broadcasting of greylisting data to peer Gateways.

Building a Gateway policy

The Clearswift Gateway policies are created and managed in the "*Policy*" centre. There are a number of default *Content Rules* which have been created to perform a specific part of the policy, such as "Delete Virus". These *Content Rules* can be amended or new ones created based on customer requirements. *Content Rules* are constructed using elements taken from *Policy references*, such as *Lexical lists* which contain lists of words to check for. These references can then be re-used in multiple separate *Content Rules* to save recreating them

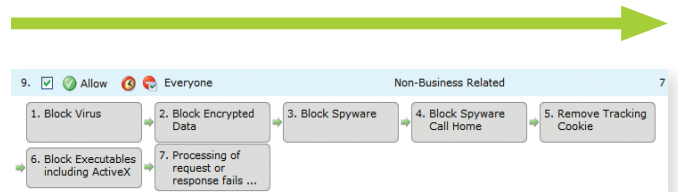
If you have the Clearswift Email Gateway and the Clearswift Web Gateway you can peer them together and share the **Content Rules** across both products. This allows you to define rules once that can apply to both of the Clearswift Gateway protocols.

Content Rules are applied to *Policy Routes* which define the direction of communication. For example, in the Clearswift Email Gateway: "*@mycompany.com" TO "Everyone", or in the Clearswift Web Gateway it could be "Everyone" TO "Social Networking Sites"

A company will define multiple *Policy Routes* to describe their communication rules. The ordering of routes is important as the list is evaluated from top to bottom to find the route that has the best match for the source and destination of the communication.

Action	From	To	Rules
1. Allow	Everyone	Trusted Sites	
2. Block	Everyone	Security Risk	7
3. Block	Everyone	Sexually Explicit	7
4. Block	Everyone	Violence/Offensive	7
5. Block	Everyone	Weapons	7
6. Block	Everyone	Drugs	7
7. Block	Everyone	Gambling	7
8. Allow	Product Management	Non-Business Related	7
9. Allow	Everyone	Non-Business Related	7
10. Allow	Everyone	Chat & Instant Messaging	7
11. Allow	Everyone	Web Mail	7
12. Allow	Everyone	Clearswift Web Threat Test	12
13. Allow	traffic that does not match another route		7

So if you were in the Product Management group, and accessing "Non Business Related" sites you would have the downloaded data checked against the rules that are defined in Route 8 - all other users would be processed against the rules of Route 9. Within each route the Content Rules are ordered in most significant order first.



In this example if someone has tried to download an executable virus, it would trigger against Rule 1 (Block Virus) and Rule 6 (Block Executables including ActiveX). As Rule 1 is the first rule, the product will perform the actions that have been defined for that rule.

Understanding these concepts will help you greatly to understand how to create rules and apply them to policy routes to form your Clearswift Gateway security policy.

Contact Clearswift

Standard support is available to any Clearswift customer (or during an evaluation).

Standard support




- 24/7 Phone and Email Support
- Knowledge Base Access
- Service feeds to update your deployment
- Service packs and patches

Japan only:
9-5 Monday to Friday Phone & Email Support

CLEAR SWIFT

Contact	Support
APAC	(+61) 2 9424 1210
Japan	0800-400 773
Germany	0800 1800 556
Europe	(+44) 0118 903 8200
US	1 856 359 2170
Email	support@clearswift.com
Online	kb.clearswift.com

Setup Wizard Settings

ITEM	YOUR VALUES	NOTES
Gateway license details		Please contact your Clearswift representative for your full license key. Evaluation licenses can be obtained from the Clearswift website: https://web2.clearswift.com/membercenter/licenses-smtpappliance.aspx OR https://web2.clearswift.com/membercenter/licences-webappliance.aspx
Company name:		
License key:		
Serial number:		
System Locale		This will affect the format used to display dates etc.
Time settings		If you elect not to use an NTP server you must specify the current date and time later, using the Gateway System center. The wizard provides a list of time zones to select from.
Timezone:		
NTP time server hostname or IP address:		
Network settings		If you configure only one network interface card, use NIC1.
Network details for NIC1		
IP address:		
Subnet mask:		
Default Gateway IP address:		
Network details for NIC2 (if using both)		If used, NIC2 must have a separate IP address.
IP address:		
Subnet mask:		
Default Gateway IP address:		
Static route (optional)		Define additional static routes to Gateways if required by your network environment.
Network:		
Subnet mask:		
Gateway:		
DNS settings		A fully qualified hostname has the format hostname.domain-name, for example: appliance1.your-companyname-here.com
Hostname		
Fully qualified hostname for the Gateway:		
IP addresses of up to 3 DNS servers		
Primary DNS server:		
Secondary DNS server:		Supply your DNS server IP addresses if you are using DNS.
Tertiary DNS server:		
 Names of up to 6 hosted email domains		Supply the domain name of at least one hosted domain. You can add others from the System center.
Hosted domain:		
Hosted domain:		
Hosted domain:		
Hosted domain:		
Hosted domain:		
Corporate mail server details		Enter the details of the mail server for your domain(s).
Host:		
Port number:		
 Mail server for external delivery		These details are only required if you are not using DNS to route mail for external delivery.
Hostname:		
Port number:		
System email addresses		The email address of the admin user account. Sender of messages such as alerts. Sender of messages such as non-delivery reports.
Main administrator email address:		
Gateway email address (Web Gateway only):		
Server email address (Email Gateway Only):		
Postmaster email address (Email Gateway Only):		
 Clearswift Web Gateway Proxy Settings		Choose the port on which the Gateways should listen for requests.
Port number:		
Proxy Settings		Provide these details if the Clearswift Gateway needs to use an HTTP proxy to access the Internet. (Web Gateway only) Use a HTTP proxy to connect to the upgrade server. (Email Gateway only)
Proxy host and port:		
User name and password:		
Initial system passwords		Supply passwords to be used for each of the standard Clearswift accounts.
Web User Interface (Admin):		
Console User (Console):		
System Administrator (System):		

