

LAKESIDE HOUSE
CAIN ROAD
BRACKNELL
BERKSHIRE
RG12 1XL

WWW.CW.COM

T0:

Cable&Wireless

GCSx Pre-connection Check list

Version: 1.3
Date 3rd November 2008

1 PRE-CONNECTION CHECK LIST

1.1 Document Purpose

This document provides a checklist for connection to the GCSx network, and qualification for on site support to be provided by a Vistorm Consultant.

Fulfilment of the pre-requisites detailed below will help to ensure connection to the GCSx network is made in the most time effective manner.

A check box is provided to confirm whether these pre-requisites have been met or not. Please tick the relevant check box, and supply other detail as necessary.

1.2 Pre-requisites

▶ Network Pre-requisites

- All routing to the GCSx network will be configured prior to the consultant arriving on site.
 - This includes all necessary internal routing to allow servers that will require communication to and from the GCSx network to be routed correctly.

Completed Scheduled Date / /

- Ensure that the core router (if used) is configured correctly to route GCSx specific traffic correctly to the GCSx network via the Firewall put in place between the Local Authority Network and GCSx Network.

Completed Scheduled date / /

- Please provide information as to whether any routers used for communication to the GCSx network use Network Address Translation

Router use NAT Routers do not use NAT

- All relevant static routes will be configured prior to the consultant arriving on site on all servers that require routing to the new Firewall.

Completed Scheduled date / /

- A dedicated network resource will be available at all times to configure/troubleshoot the Local Authority routers/switches as required to assist in any network troubleshooting.

Network resource will be available on the day?

- Vistorm need to be informed in advance whether any of the Local Authority equipment involved in the connection to GCSx is not managed by the Local Authority, i.e. outsourced to a managed service provider, and whether any of the equipment require a change control procedure, including the lead time for any such changes. Equipment can include, but is not limited to routers, switches, Firewalls and Servers.

Please tick if local authority agrees to this pre-requisite?

▶ Firewall pre-requisites

- Please confirm the model of Firewall that will be used between the Local Authority Network and the GCSx Network.

- Please confirm the version of the Firewall and Operating System the Firewall is running on, and the hardware model

-
- The Firewall will be fully installed and configured prior to the consultant arriving on site.
 - All firewall rules required to facilitate the connection to the GCSx network must be configured prior to the security consultant arriving on site. This includes all relevant HTTP, HTTPS, SMTP, NTP, LDAP and DNS rules as required with the necessary source, destination, action and comment columns configured, a table is provided in section 1.3 of this document.

Completed Scheduled date / /

- Vistorm will not be configuring any of the Firewall equipment, but will be available as a support resource to assist with any issues that may arise as a result of the connection to GCSx.

Please tick if local authority agrees to this?

- Any static routes and default gateways required on the Firewall to enable connection to GCSx will be pre-configured prior to the security consultant arriving on site.

Completed Scheduled date / /

- All relevant NAT rules will be configured on the Firewall, prior to the Security consultant arriving on site.

Completed Scheduled date / /

▶ Server Pre-requisites

- Server specific pre-requisites

- The email server that will host the GCSx mailboxes must be in place (this can be an existing email server or a dedicated GCSx one).

Completed Scheduled date / /

- Please confirm the type of Email Server that the Local Authority is running.

.....

- A decision has been made as to which users will be enabled for the GCSx service.

Completed Scheduled date / /

- All required mail server changes such as configuring new mailboxes and user accounts, assigning GCSx aliases to users, configuring new SMTP connectors and configuring an additional accepted domain can be made on the date of the site visit (i.e. no change control procedures are required or have already been put in place).

Completed Scheduled date / /

- Please confirm the type of DNS Server that the Local Authority is running.

.....

- All required DNS server changes such as configuring conditional forwarding to the GCSx domains can be made on the date of the site visit (i.e. no change control procedures are required or have already been put in place).

Completed Scheduled date / /

- All required proxy server changes such as configuring new rules to access the GCSx application sites can be made on the date of the site visit (i.e. no change control procedures are required or have already been put in place).

Completed Scheduled date / /

- A process for creating user accounts for access to the GCSx services has been determined.

Completed Scheduled date / /

- A decision has been made whether to use the GCSx provided time service and the relevant changes are made prior to the visit.

Completed Scheduled date / /

▶ Hours of Work

- Vistorm standard hours of consultancy are 9am – 530pm, if additional time is required contrary to the standard hours; Vistorm will require advance notice for out of hours work

Please tick if local authority agrees to this pre-requisite?

▶ Scope of Work

- All Network equipment routers and switches are the responsibility of the Local Authority

Please tick if local authority agrees to this?

- The CE router is the responsibility of Cable and Wireless.
- The Vistorm security consultant is responsible for assisting in troubleshooting of the Firewall in tandem with the Local Authority Firewall administrator with regards to the GCSx connection only.

Please tick if local authority agrees to this?

- The Vistorm IS consultant is responsible for assisting in configuring and troubleshooting of the relevant Microsoft Servers in tandem with the Local Authority Microsoft administrators with regards to the GCSx connection only.

Please tick if local authority agrees to this?

▶ Resource Pre-requisites

- Firewall
 - A dedicated Local Authority Firewall administrator responsible for the Firewall used for the GCSx connection will be available at all times as required by the Vistorm consultants.

Please tick if local authority agrees to this pre-requisite?

- Microsoft Servers
 - A dedicated Local Authority Exchange administrator will be available at all times as required by the Vistorm consultants.

Please tick if local authority agrees to this pre-requisite?

- A dedicated Local Authority Active Directory administrator will be available at all times as required by the Vistorm consultants.

Please tick if local authority agrees to this pre-requisite?

- A dedicated Local Authority Proxy Server administrator will be available at all times as required by the Vistorm consultants.

Please tick if local authority agrees to this pre-requisite?

- Network

- A dedicated Local Authority Network administrator responsible for the network switches and routers will be available at all times as required by the Vistorm consultants.

Please tick if local authority agrees to this pre-requisite?

- Testing

- A dedicated resource to aid in testing of the connection to GCSx will be available at all times to assist with connectivity testing.

Please tick if local authority agrees to this pre-requisite?

- ▶ Cancellation Policy

- In the event that the LA wishes to cancel the on-site consultancy within 7 days of the scheduled date then any rescheduled date will be on a chargeable basis*.

Please tick if local authority agrees to the cancellation policy

▶ Accuracy or Information

- Should the information given in this document prove inaccurate leading to the inability to confirm the GCSx services, any further consultancy to prove GCSx service availability may be on a chargeable basis*.

Please tick if local authority agrees to the accuracy of information agreement

* Cost will be as per the C&W standard Professional Services rate table.

1.3 Firewall rule base pre-requisites.

The table below shows the default GCSx firewall configuration.

The firewall MUST be configured as below to minimise the likelihood of successful attack against the network.

From	To	Protocol	Action	Comment
Your Internal Networks that require access to GCSx	GCSx Networks	HTTP (TCP/80) HTTP (TCP/8080) HTTPS (TCP/443)	Allow	Enable outbound access to applications in GCSx using HTTP & HTTPS
GCSx Networks	Your Applications/ Web Servers	HTTP (TCP/80) HTTPS (TCP/443)	Allow	Enable inbound requests from GCSx to your web servers/applications (if applicable add other protocols as required)
GCSx Mail Servers	Your Mail Server(s) allocated IP address in GCSx Network range	SMTP (TCP/25)	Allow	Enable inbound e-mail from GCSx central mail relays

Your Mail Server(s) allocated IP address in GCSx Network range	GCSx Mail Servers	SMTP (TCP/25)	Allow	Enable outbound e-mail to GCSx central mail relays
Your Internal DNS Server(s) allocated IP address in GCSx network range	GCSx DNS Servers	DNS (UDP/53) DNS (TDP/53)	Allow	Allow queries to GCSx DNS servers
Your NTP Server(s)	GCSx NTP Servers	NTP (UDP/123)	Allow	Allow queries to GCSx NTP servers
Your Internal Networks	GCSx LDAP Server	LDAP (TCP/389)	Allow	Access to GCSx LDAP Server (GC Directory)
Your Internal Networks	Public Address Space	HTTP (TCP/80) HTTP (TCP/8080) HTTPS (TCP/443)	Allow	Enable outbound access to applications on the Internet on HTTP & HTTPS (add other protocols as required)
Any	Any	ICMP	Allow	Temporarily Allow ICMP for connectivity testing
Any	Any	Any	Block	Clean-up Rule

All other traffic attempting to traverse the Firewall from the Local Authority network to the GCSx network, and vice versa must be dropped by the firewall.

1.4 NAT rule base pre-requisites.

The table below shows the default GCSx firewall configuration.

From	To	Translation type
Your Mail Server	Your allocated IP address in GCSx Network Range	NAT Static (one-to-one)
Your Proxy Server(s)	Your allocated IP address in GCSx Network Range	PAT (NAT overload)
Your DNS Server	Your allocated IP address in GCSx Network Range	NAT Static (one-to-one)
Your Edge Server	Your allocated IP address in GCSx Network Range	NAT Static (one-to-one)
All user traffic	Your allocated IP address in GCSx Network Range	PAT (NAT overload)
All user traffic	Your allocated IP address in GCSx Network Range	PAT (NAT overload)
All user traffic	Your allocated IP address in GCSx Network Range	PAT (NAT overload)
Your allocated IP address in GCSx Network Range	Your allocated IP address in GCSx Network Range	PAT (NAT overload)

In addition to this configuration, the firewall MUST also be configured to:

- set up an explicit default deny policy (packets must be dropped with no destination unreachable response sent back to the requestor, so that denied ports are 'stealthed'). Only those services that are explicitly required MUST be allowed;
- log all requests;

- deny inbound traffic that appears to come from internal addresses;
- deny outbound traffic that does not appear to come from internal addresses;
- deny all traffic with invalid source addresses (including broadcast and multicast); and
- deny all traffic with source routes or other IP options set.

1.5 *Contact and Address Details*

Please provide contact details of the site where the work will take place in advance.

- Site Address
- Primary Contact, Secondary Contact
- Contact Phone numbers
- Physical visit arrangements

Document Control

© Cable&Wireless 2008

The information contained herein is the property of Cable & Wireless and may not be copied, used or disclosed in whole or in part except with the prior written permission of Cable & Wireless.

Distribution Control & Change Coordinator

Version: 1.3

Author: Sukhvinder Bhangal, Radka Holinska, Mark Hulbert and Keith Hart

Title: GCSx Preconnection Check List