Active Circle
Technical Brief

Network Port & Routing Requirements

Active Circle 5.0 - November 2018

oodrive
LEADING BY TRUST

INDEX

1. Introduction

1.1. Scope of the document

This document describes the requirements for the Active Circle system in terms of network ports and routing.

The scope of this document is limited to version 5.0 and higher of Active Circle, used on IPv4 networks. Any changes to this functionality in future versions of Active Circle will be reflected in revised versions of this document.

1.2. Audience

This document is mainly intended for network administrators, as a helper for setting up a firewall on Active Circle nodes or the client machines running the Active Circle GUI applications.

1.3. Organisation of the information

This document is divided into two main parts. The first part gives an overview of the networking features of Active Circle and describes the general port and routing requirements of the system. The second part presents tables containing detailed information about incoming and outgoing ports for each feature, protocol and routing scheme. There is one set of tables for the nodes (servers) and one set for the applications.

Some technical terms, acronyms, abbreviations and references are explained at the end of the document, in a glossary and a section with table footnotes. An appendix describes Active Circle compliance with other network infrastructure standards.

1.4. For more information

You will find more information about how to manage the network features and ports in the Active Circle documentation:

- Active Circle Installation Guide
- Active Circle Administration Guide
- Active Circle Command Line Guide

You can find theses documentations in your online help website: https://activecircle-help.com.

To find out more, contact your Active Circle representative or send an e-mail to: customer-support@active-circle.com.

2. Active Circle Networking Overview

2.1. Network Overview

Active Circle is a clustered file storage solution with integrated file security. It provides a large set of features, such as file replication, versioning, hierarchical storage management, continuous data protection and a virtual file system. The system consists of multiple server machines, known as nodes, which together are called a Circle.

From a network point of view, the system acts mainly as a multi-service server. It provides access to stored files in the same way as network-attached storage (NAS), while adding inter-node discovery and synchronization capabilities.

Some features imply that Active Circle will sometimes act as a network client; for instance when interacting with user directory services for authentication purposes.

As Active Circle relies on several network services, careful consideration should be taken when setting up firewalls on server and client systems. This is to ensure sufficient security on the hosting platform without interfering with the distributed operating mode of Active Circle. To assist the administrator in these tasks, this document summarizes the network ports and routing configuration required by Active Circle nodes for both roles. It should serve as a reference for configuring a firewall on the system hosting the nodes.

2.2. Networking Features

The information presented in this document refers to the different network-related features provided by the node. This section contains a description of each feature.

2.2.1. Downloading Java applications

Through Java Web Start, the Active Circle GUI applications can be downloaded and run on any client system by connecting to a node's web server using a web browser.

2.2.2. Remote file access

Any node can be used as a file server providing CIFS (SMB), NFSv3 or FTP(S) access to the files stored on the Circle. No specific client software is needed on the client systems, as these protocols are supported by all major operating systems.

2.2.3. Node and client communications

- Service discovery: Each node supplies various services. Through the discovery mechanism, the other nodes become aware of the services offered and the applications can take advantage of them.
- Inter-node data transfer: This is a core feature of the Circle. Nodes transfer data between them to ensure functionality such as file replication, file availability on any NAS-enabled node, shared storage and tape management.
- Node-to-application data transfer: This allows the Active Circle applications to retrieve and exchange information with the nodes.

2.2.4. Node clustering

- High availability (HA) cluster services: Automatically assigns a unique addressing resource to a member node (called the leader), providing clients with access to remote files without having to provide a reference to a specific node. The HA cluster provides automatic failover and failback functionality which is transparent to the clients. The addressing resource can be a virtual IP address, a virtual DNS name, a virtual NetBIOS name or a script-based mechanism (such as OpenVPN).
- Lock manager & Policy management clusters: Nodes are organized in clusters for these advanced features.

2.2.5. User directory integration

Active Circle is supplied with an embedded user directory, as well as providing support for integration with external directories. The external directory functionality includes:

- Import: An initial snapshot of a third-party user directory can be captured.
- Synchronization: To ensure consistent and updated information.
- Authentication: When a client connects to a node through an Active Circle application or file access protocols, the user requesting access is authenticated.

2.2.6. Remote alerts

Active Circle nodes generate supervision notes to notify administrators about important events and errors. The notes are posted in the Administration application, and they can be sent to subscribed users or machines through SMTP e-mail and SNMP traps.

2.2.7. Supervision

Active Circle publishes a dedicated MIB, allowing to supervise the nodes with any SNMP-based supervisor (Nagios or alike).

2.2.8. API web service (option)

Active Circle offers a REST-based API with web services that can be provided by an external server or one of the nodes. It allows integration of Active Circle with third-party applications.

2.3. Active Circle Network Traffic

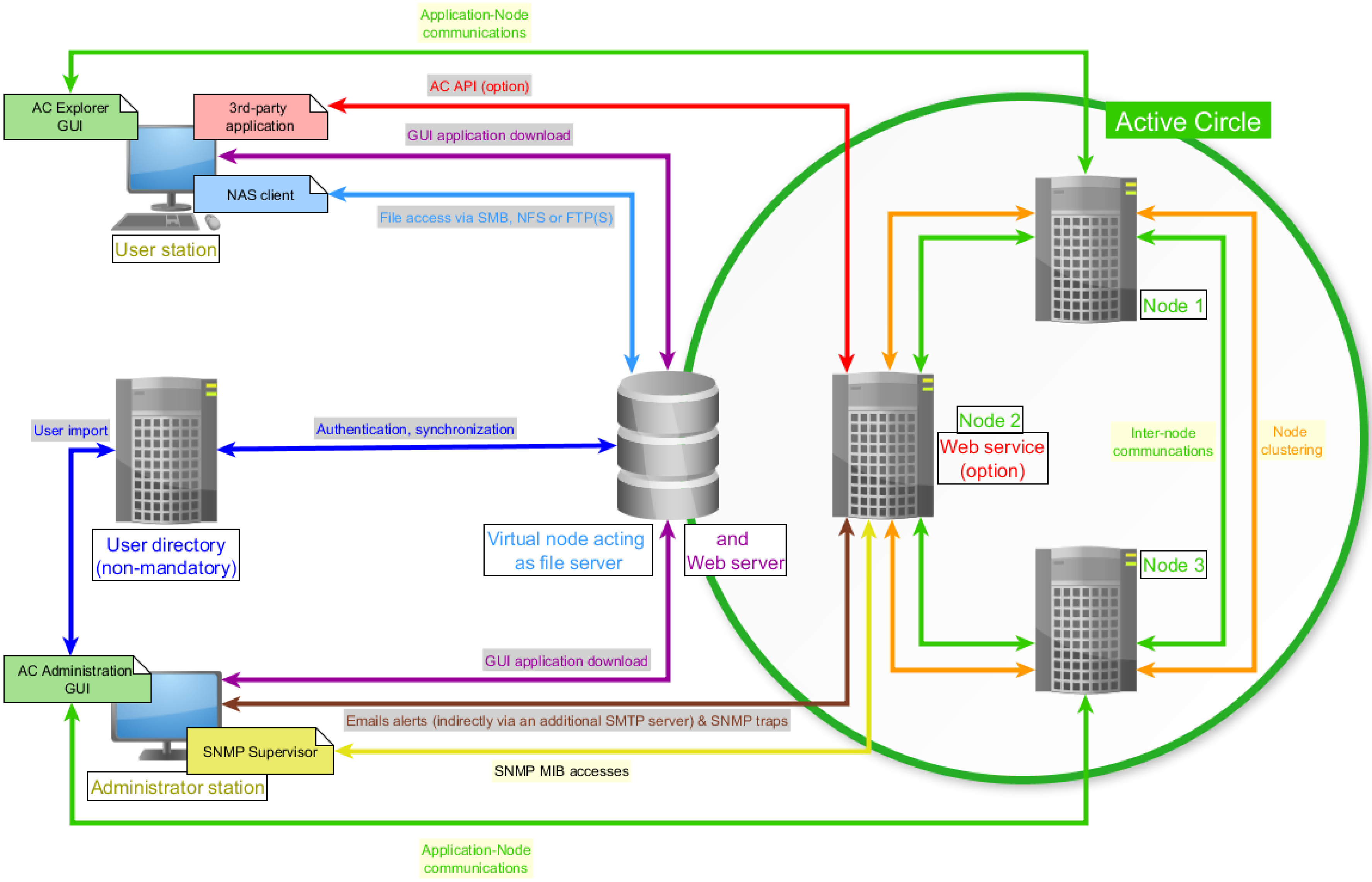
Introducing Active Circle in an enterprise network generates new network traffic of several kinds, involving different entities.

The entities generating the traffic are the Active Circle nodes, the virtual file servers (NAS) running on the nodes, internal and external user directories and multiple clients (administrators and users).

The induced traffic may be divided into the following types:

- Inter-node communications
- Client-Circle communications:
  - Client-NAS: Remote access through standard protocols
  - Client-Node: Active Circle Explorer and Administration applications
  - Client-Web service: Running external applications using the Active Circle API.
  - Alerts by SMTP email, SNMP traps.
  - Client-SNMP server: Access to the values described in the MIB.
- Communication with external user directories:
  - User authentication and synchronization
  - Importing a user directory using the Active Circle Administration tool.

The network traffic is summarized by the figure on the next page.


Application-Node communications
AC API (option)
GUI application download
File access via SMB, NFS or FTP(S)
AC Explorer GUI
3rd-party application
NAS client
User station
Active Circle
Node 1
Node 2
Web service (option)
Inter-node communcations
Node clustering
Node 3
User import
Authentication, synchronization
User directory (non-mandatory)
Virtual node acting as file server
and Web server
GUI application download
AC Administration GUI
Emails alerts (indirectly via an additional SMTP server) & SNMP traps
SNMP Supervisor
SNMP MIB accesses
Administrator station
Application-Node communications

3. Port and Routing Requirements

3.1. Routing

3.1.1. Nodes

The network routing configuration must allow each node to:

- reach all the other nodes of the Circle,
- reach any third-party user directory,
- reach the configured SMTP server (if any),
- reach the network management systems collecting SNMP traps (if any).

Note that this does not mean that all the systems must belong to the same sub-network.

3.1.2. Client Applications

The network routing configuration must allow the system running the client application to:

- reach at least the virtual node acting as file server (the leader of an HA cluster),
- reach the user directories to be imported.

Note that this does not mean that all the systems must belong to the same sub-network.

3.2. Routing Schemes

The nodes and applications rely on the following routing schemes:

- Local broadcast (nodes only),
- Unicast in both TCP and UDP,
- Multicast on the *jini-announcement* and *jini-request* registered addresses, along with configurable addresses picked from the *Organization-Local Scope* range. These addresses are listed in the IANA IPv4 Multicast Address Space Registry document. Enabling multicast routing is not mandatory (see next section).

3.3. Multicasting and Locators

Two main node features rely on multicasting:

- Service discovery
- HA (high availability) cluster services

Client applications rely on multicasting only for service discovery.

As multicasting is usually disabled by default on routers, Active Circle provides a *Locators* mechanism that allows service discovery to continue to work even if nodes are in different sub-networks. The *Locators* feature allows the administrator to specify the IP addresses of each node of the Circle. In such a configuration, service discovery is done using a unicast addressing scheme.

For more information, see the *Active Circle Installation Guide*.

As opposed to this, HA cluster services require either that all member nodes are in the same sub-network, or that multicasting is enabled on the routers used to reach each node.

Locators are also used by other, non-HA clusters. The Lock manager and Policy Management clusters use them to force their traffic to use the corresponding network interface, while any interface can be used when no locators are defined.

4. Ports for Nodes

The tables in this section indicate the ports used by Active Circle nodes.

Data transfers between the nodes rely on the common client-server model, in which one node acts a server while the other acts as a client. Client or server roles are not associated with any given node; each node performs both roles depending on the tasks being processed.

The first table applies to nodes when acting as a server. This can be used as a reference for configuring filtering for *incoming* traffic for the platform hosting the node.

The second table applies to nodes in client mode. This can be used to configure filtering for *outgoing* traffic for the platform hosting the node.

Ports and bindings shown are default values. Most can be changed using the Active Circle Administration application or the configuration files. Values on blue background cannot be modified. Features with yellow background are provided by the operating system, information about changing those values can be found in the operating system documentation.

Note:
The tables in this section are mainly provided to help setting up filtering on the operating system hosting the node. For security reasons, we recommend defining filtering rules only for the features that are used in your environment.

4.1. Ports for incoming traffic:

Blue = Automatic / Cannot be modified ● Yellow = Provided by operating system ● DAP = Dynamically Allocated Ports

Feature			Application protocol		Routing scheme	Transport protocol	Default ports for incoming traffic	Bound interfaces by default
Downloading applications in a browser			**HTTP / HTTPS**		unicast	TCP	80[i] / 443[ii]	all[iii]
Remote file access (NAS servers)			**NFSv3**		unicast	TCP	111, 2049, 35032, 35033[3]	all[3]
						UDP	111, 2049, 35032, 35033[3]	all[3]
			CIFS (SMB1)		unicast	TCP	139, 445	all[3]
					unicast & local broadcast	UDP	137, 138	all[3]
			FTP / FTPS	"Legacy" mode: control connection	unicast	TCP	21[3] / 990	all[3]
				Passive mode: control connection	unicast	TCP	21[iv] / 990	all[3]
				Passive mode: data connection	unicast	TCP	DAP	auto-detection[v]
Inter-node communications	**Service discovery**		**Jini**	Automatic discovery	multicast on 224.0.1.84	UDP	4160	all
				Locator-based discovery	unicast	UDP	4160	all
				Service requests	unicast	TCP	4160	individually on each physical interface
	Inter-node data transfer		**Active Circle**		unicast	TCP	[30000-30199][vi] (minimum 50 ports)	individually on each physical interface[vii]
Node clustering	**HA cluster services**	**Management**	**Active Circle**		multicast on 239.255.1.1[viii]	UDP	40000[7]	auto-detection[4]
		OpenVPN	**OpenVPN**		unicast	TCP/UDP[8]	1194[ix]	all[8]
	Lock manager & Policy management		**Active Circle**		unicast	UDP	40001[x]	auto-detection[4]
SNMP supervision			**SNMP (v1, v2c, v3)**		unicast	TCP/UDP	161	all

Active Media Connector (AMC) API Web service **Standard mode** (only for the node hosting the Web service)	**HTTP / HTTPS**		unicast	TCP	8081[xi] / 8443	all[10]
	PostgreSQL		unicast	TCP	5432[xii]	Localhost[11]
Active Media Connector (AMC) API Web service **Cluster mode**	**HTTPS**		unicast	TCP	8443[xiii]	all[10]
	PgPool II	virtual PSQL port, internal use for Tomcat and monitoring scripts	unicast	TCP	9999	all[10]
		watchdog port, internal use between PgPool nodes	unicast	TCP	9000	all[10]
		heartbeat port, internal use between PgPool nodes	unicast	UDP	9694, 60545	all[10]
		PgPool command administration port (PCP)	unicast	TCP	9898	all[10]
	PostgreSQL	PSQL port, internal use between PgPool and PostgreSQL	unicast	TCP	5432[xiv]	all[10]
	SSH	SSH port, internal use between PgPool nodes	unicast	TCP	22	all[10]
OS-provided remote access (optional, but recommended)	**SSH**		unicast	TCP	22	all

4.2. Ports for outgoing traffic:

Blue = Automatic / Cannot be modified ● Yellow = Provided by operating system ● DAP = Dynamically Allocated Ports

Feature			Application protocol		Routing scheme	Transport protocol	Ports for outgoing traffic		Server port targeted
Remote file access (NAS servers) (when acting as clients)			**CIFS** (SMB1)		unicast & local broadcast	UDP	137,138		137,138
			FTP / FTPS	"Legacy" mode: data connection	unicast	TCP	20[xv] / 989	DAP	protocol-negotiated
Inter-node communications (client side)	**Service discovery**		**Jini**	Automatic discovery	multicast on 224.0.1.85	UDP	DAP		4160
				Locator-based discovery	unicast	UDP	DAP		4160
				Service requests	unicast	TCP	DAP		4160
	Inter-node data transfer		**Active Circle**		unicast	TCP	DAP		[30000-30199][5] (minimum 50 ports)
Node clustering	**HA cluster services**	**Management**	**Active Circle**		multicast on 239.255.1.1[7]	UDP	DAP		40000[7]
		DNS-based clustering	**Dynamic DNS**		unicast	TCP	DAP		53
	Lock manager & Policy management		**Active Circle**		unicast	UDP	DAP		40001[9]
User directory integration: Synchronization and authentication (only with external user directories)			**LDAP / LDAPS** (incl. Active Directory)		unicast	TCP	DAP		389[xvi] / 636
			NIS (ypserv v2)		unicast	TCP	DAP		111, registered port[xvii]
					unicast	UDP	DAP		111, registered port[6]
Remote alerting	**Email alerts**		**SMTP**		unicast	TCP	DAP		25[xviii]
	SNMP traps		**SNMP (v1, v2c, v3)**		unicast	UDP	DAP		162[xix]
OS-provided host name resolution (for all features)			**DNS**		unicast	UDP	DAP		53
OS-provided clock synchronization			**NTP**		unicast	UDP	123		123

5. Ports for GUI Applications

This section lists the ports required by the Active Circle **Administration** and **Explorer** applications when executed on a client station. Both are Java applications, therefore they can be run from any client operating system with a web browser.

Ports and bindings shown are default values. Some can be changed using the Active Circle configuration files. Values on blue background cannot be modified. Features with yellow background are provided by the operating system, information about changing those values can be found in the operating system documentation.

The specifications for transfers from node to application are similar to those that apply to inter-node data transfers, except that the minimum number of ports needed by an application is 20 (as opposed to 50 for a node), provided that each application has its own, distinct, range.

Note:

The tables in this section are mainly provided to help setting up filtering on a client system running Active Circle GUI applications. For security reasons, we recommend defining filtering rules *only* for the features that are used in your environment.

5.1. Incoming traffic (server mode)

The following table applies to communications with the nodes when acting as a server. It can be used as a reference for configuring filtering for *incoming* traffic on the client system running the application.

Blue = Automatic / Cannot be modified ● Yellow = Provided by operating system

Feature	Application protocol	Routing scheme	Transport protocol	Default ports for incoming traffic	Bound interfaces by default
Service discovery	**Jini**	multicast on 224.0.1.84	UDP	4160	all
“Administration”: Node-to-application data transfer	**Active Circle**	unicast	TCP	[30200,30219][xx] (min. 20 ports)	individually on each interface
”Explorer”: Node-to-application data transfer	**Active Circle**	unicast	TCP	[30300,30319][xxi] (min. 20 ports)	individually on each interface

5.2. Outgoing traffic (client mode)

The following table applies to the applications in client mode. This can be used to configure filtering for *outgoing* traffic on the client system running the application.

Blue = Automatic / Cannot be modified ● Yellow = Provided by operating system ● DAP = Dynamically Allocated

Feature		Application protocol	Routing scheme	Transport protocol	Ports for outgoing traffic	Server port targeted
Downloading applications in a browser		**HTTP / HTTPS**	unicast	TCP	DAP	80[1] / 443
Communications with the nodes	**Service discovery**	**Jini**	unicast	TCP	DAP	4160
			multicast on 224.0.1.85	UDP	DAP	4160
	Application node data transfer	**Active Circle**	unicast	TCP	DAP	[30000-30199][5] (min. 50 ports)
User directory integration: import (ports needed only at import time)		**LDAP / LDAPS** (incl. Active Directory)	unicast	TCP	DAP	389[13] / 636
		NIS (ypserv v2)	unicast	TCP	DAP	111,registered port[14]
			unicast	UDP	DAP	111,registered port[14]
Remote alerting		**SNMP MIB**	unicast	TCP	DAP	161
			unicast	UDP	DAP	161
OS-provided host name resolution (for all features)		**DNS**	unicast	UDP	DAP	53

6. Glossary

CIFS: *Common Internet File System*, also know as *Server Message Block* (SMB). It is an application layer network protocol used by the Microsoft Windows platform, and is implemented in Unix/Linux through the *Samba* protocol.

Circle Property: Allows you to configure the behavior of the Active Circle nodes on several levels of the system. The property settings are available in the Active Circle *Administration* application and from the Active Circle *command line interface*. For more information, see the Active Circle documentation.

DAP: Short for *Dynamically Allocated Port*. These ports are allocated by the operationg system. Also called Ephemeral ports. On Linux, the expected default range is [32768,61000], but it can change depending on the Linux distribution or its preloaded configuration.

HA: *High Availability* is implemented as a model for clusters of nodes in Active Circle, to ensure continuous service availability.

Java Web Start: Allows users to start Java applications directly through a web browser. Used by the Active Circle *Explorer* and *Administration* applications.

Jini: A service-oriented architecture based on Java technology for constructing secure, distributed systems. Also called *Apache River*.

LDAP: *Lightweight Directory Access Protocol*.

MIB: *Management information base*, a computing information repository used by the Simple Network Management Protocol.

NAS: *Network-attached storage* on a file level, operating as a file server.

NFSv3: *Network File System* version 3. A distributed file system protocol.

NIS: *Network Information Service* is a client–server directory service protocol.

NTP: The *Network Time Protocol* is a networking protocol for clock synchronization.

OpenVPN: An open source software application which can be used with scripted HA clusters in Active Circle.

PostgreSQL: An object-relational database management system used by the Active Circle API.

REST: *REpresentational State Transfer* is a Web service design model used by the Active Circle API.

SNMP: The *Simple Network Management Protocol* is a protocol for managing devices on IP networks.

SSH: *Secure Shell* is a network protocol for secure remote command execution.

7. Appendix: Compliance with standards

7.1. IPv6

The current version of Active Circle is not compliant with **IPv6**, and must therefore be used only on IPv4 networks.

7.2. NAT Traversal

NAT traversal is the capability to work properly with network address translation devices.

For some of its features, Active Circle is not able to work properly with such devices, when some nodes of the Circle are "hidden" behind the devices. Indeed, these features embed IP addresses in transmitted packets, thus ignoring the translation done by the NAT device.

7.3. Link-local Auto-configuration

Link-local auto-configuration (also called AutoIP, APIPA or a part of ZeroConf) allows systems connected to the local sub-network to configure themselves automatically.

For the same reasons as with NAT-traversal (embedded IP addresses), Active Circle will not work properly when used in environments relying on link-local auto-configuration.

[i] Can be modified using the c*ircle property* **`httpd.port`** (implies node restart).

[ii] Can be modified using the c*ircle property* **`httpd.httpsPort`** (implies node restart).

[iii] Can be modified using the c*ircle property* **`httpd.bindAddress`** (implies node restart).

[iv] Can be modified under *Shares/Protocols* in the “Administration” client application.

[v] Corresponds to the interface the request was received on.

[vi] Range defined by the `TCP_PORT_RANGE` variable in the **`/activecircle/.localvars`** configuration file (implies node restart).

[vii] Can be restricted to specific interfaces, using the `SERVICE_INTERFACES` and `NETWORK_INTERFACES` variables in the **`/activecircle/.localvars`** configuration file.

[viii] Value defined at HA cluster creation time in the “Administration” client application.

[ix] Can be modified in the configuration file generated upon VPN setup, located in `/etc/openvpn`.

[x] Value defined in the *Advanced* view of the “Administration” client application, under *Policy Management* or *Lock Manager*, respectively.

[xi] Can be modified in the *Apache Tomcat* configuration files.

[xii] Can be modified in the *PostgreSQL* configuration files.

[xiii] Can be modified in the *Apache Tomcat* configuration files.

[xiv] Can be modified in the *PostgreSQL* configuration files.

[xv] The value for the server port less 1, automatically modified when modifying the server port. Assigned to the first outgoing connection, other concurrent connections are assigned dynamically allocated ports.

[xvi] Can be modified under *Users/External Directories* in the “Administration” client application.

[xvii] Port registered by the NIS server against its local port mapper. Modify in NIS server configuration files.

[xviii] Can be modified under *Advanced/Outgoing SMTP Server* in the “Administration” client application.

[xix] Can be modified using the *Supervision* interface in the “Administration” client application.

[xx] Range defined by the `CLIENT_GUI_ADMIN_PORT_RANGE` variable in the **`/activecircle/.localvars`** configuration file (implies node restart).

[xxi] Range defined by the `CLIENT_GUI_EXPLO_PORT_RANGE` variable in the **`/activecircle/.localvars`** configuration file (implies node restart).