

Port Settings for SRC Components

If you use firewall software within your internal network, ensure that firewall settings allow traffic to and from components in your SRC environment. Table 1 on page 1 lists the default port settings for SRC components.

For information about default port settings for applications in the SRC application library, see [Reviewing SRC Port Settings for SRC Applications](#).

Table 1: Default Port Settings for SRC Components

Component	Type of Communication	Default Port Setting
Applications, such as portals, that use the SAE Common Object Request Broker Architecture (CORBA) remote application programming interface (API)	CORBA remote API connections to the SAE.	TCP 8801
Cable modem termination system (CMTS) devices	Connection requests.	TCP 3918
Sample residential portal with Tomcata	Starting Tomcat server.	TCP 8005
	Apache JServ Protocol (AJP) requests for Tomcat.	TCP 8009
	Responses to incoming HTTP requests from Tomcat.	TCP 8080)
	This port is an alternative to port 80.	
JBossb	Remote method invocation (RMI) requests.	TCP 1099
	Communications for the Java Naming and Directory Interface (JNDI).	TCP 1100
License server	Messages from SAEs to the license server.	TCP 9000
	All SAEs in a configuration must be able to reach the license server.	
LDAP	Communications between LDAP and other components in an SRC environment, such as the SAE, NIC, and SNMP.	TCP 389
Network information collector (NIC)	Communications between the NIC host and components, such as portals, that use the NIC.	TCP 8810
	All components that use NIC resolution must be able to reach the NIC host.	

Table 1: Default Port Settings for SRC Components *(continued)*

Component	Type of Communication	Default Port Setting
RADIUS	Communications between RADIUS and the SAE.	UDP 1812
	Communications between RADIUS and the SAE for RADIUS accounting.	UDP 1813
Redirect engine	Redirection requests.	TCP 8800
SAE	Common Open Policy Service (COPS) connection from JUNOS routers.	TCP 3288
	Blocks Extensible Exchange Protocol (BEEP) connection from JUNOS routers.	TCP 3333
	BEEP with Transport Layer Security (TLS)	TCP 3434
	Session store data replication.	TCP 8820
SAE Web Admin	Secure HTTP.	TCP 8443
SNMP agent	SNMP communications between SNMP subagents and the master SNMP agent.	UDP 8030
	SNMP get and set messages.	UDP 161
	SNMP traps.	UDP 162

In addition, we recommend that TCP port 123 be open for the Network Time Protocol (NTP). We recommend that you configure NTP to synchronize time on the network. See the documentation for the NTP server for your system.

Related Topics ■ Securing Connections Between a C-series Controller and Remote Hosts