

Safe Place® and Code Alert®

Customer Information Technology Requirements – Series 10.x Software

Contents

This page intentionally left blank

Introduction

This document lists the minimum computer hardware and software requirements for the installation of RF Technologies (RFT) Safe Place/Code Alert Systems. RF Technologies makes no claims, whether stated or implied, to the operation of other software applications installed on customer-supplied hardware not listed in this document.

RF Technologies will supply the appropriate Server hardware and software with all Safe Place/Code Alert System installations. This document lists applicable Server configuration requirements. Customers may supply their own Client computers if desired. This document lists applicable Client hardware and software configuration requirements, whether the computer is provided by the Customer or by RF Technologies.

NOTE: The following requirements are pursuant to the RF Technologies, Inc. Terms and Conditions (PN 0510-0290) and may not be altered without written approval.

Microsoft Critical Updates

It is RF Technologies' policy that customers are responsible for Microsoft Critical Updates and believe all our products work correctly with the latest Microsoft Critical Updates. Although we formally qualify our products with specific Operating Systems and Service Packs, we do not formally qualify individual Microsoft Critical Updates. Microsoft Critical Updates are installed on all equipment within our Engineering and Qualification groups where we confirm our software performs as expected with the patches applied. To the best of our knowledge, no Microsoft Critical Update has caused the failure of RF Technologies' software products.

It is recommended that customers apply Microsoft Critical Updates as they become available and then confirm that the RF Technologies software products continue to operate correctly. Applying these patches will not invalidate any warranty or service contract in place at the time. If incorrect operation occurs, it is recommended that the customer remove the patch (if possible) and notify the RF Technologies Customer Support immediately.

Java Updates

Java updates on the Server and Client are high risk and should never be done. The Client and Server software is Java-dependent, and Java updates will likely cause adverse effects. The software is designed to use the particular version of Java that is installed as part of the installation and Automatic Java updates should remain DISABLED.

Antivirus

It is RF Technologies' policy that customers are responsible for the security and protection of their networks. Customers are responsible for maintaining current virus protection and robust firewalls. If a customer have defects in their network security, it is possible for their RF Technologies products to become infected. Antivirus updates should be applied as required the Customer's security policy.

Server Requirements

Physical Server

RF Technologies offers three physical server options. These options have been tested and validated to meet performance expectation that your life safety security system requires.

	Desktop (0910-0228)	Mid-Range (0910-0218)	Enterprise (0910-0219)
OS	Microsoft Windows Server 2012 R2		
CPU	Dual-core 2.9 GHz	Quad-Core Xeon 2.4+ GHz ≥4MB L3 Cache	Quad-Core Xeon 3.3+ GHz ≥4MB L3 Cache
Main Memory	4 GB	4+ GB	32 GB
HDD	250 GB 2.90 GHz SATA 7,200 RPM	2+146GB 15k RPM drives RAID1	3+146GB 15k RPM drives RAID5
Network Adapter	10/100 Base-T or faster	2 1Gb Ethernet w/TCP/IP Offload Engine	4 1Gb Ethernet w/TCP/IP Offload Engine
USB	Minimum 4 USB 2.0		
Graphic	Integrated 32 MB Video Standard		
Serial Ports	None	1 Serial Port, dedicated to HP iLO	
Power Supply	350+ W	Redundant 800W, 90+% efficiency	
Media Drive	CD-RW/DVD-R combo drive		
IP Address	Static		
VPN	Required for remote support		

NOTE: The Server Name should not be changed unless agreed to prior to installation. The RFT supplied Server is configured with a unique RFT provided Server name that identifies it to the rest of the Safe Place/Code Alert system as a Server. Before you consider changing this, please understand that RFT's ability to effectively service each system is degraded when the Server name is changed.

Virtual Server

RF Technologies has tested and validated these virtual server specifications to ensure they meet performance expectation that your life safety security system requires.

RF Technologies strongly recommends that no other 3rd party applications be installed on the Safe Place/ Code Alert Server.

	Minimum Requirement
VMWare vSphere	5.0 and higher
OS	Microsoft Windows Server 2012 R2
Feature	.Net Framework 3.5 (includes .Net 2.0 and 3.0) SNMP Services Telnet Client
CPU	Dual-core 2.4GHz
Main Memory	4 GB
HDD	60 GB, thin-provisioned
Network Adapter	10/100 Base-T or faster (Integrated 1 GbE Ethernet)
Graphic	Integrated Intel HD 32 MB Video Standard
IP Address	IPv4 static
Remote	VPN & Remote Desktop with Network Level Authentication
Media Drive	Virtual Clone Drive

Server Rack

RFT recommends that rack-mount Servers are located in a 4-post rack with at least 1U of available space and access to the rear panel. RFT will need access into the Server room in order to mount the Server, unless the Server will be mounted by the facility.

Server Database Backups

Real-time backups of RF Technologies Safe Place/Code Alert software are not supported.

In order to perform cold backups of RF Technologies Safe Place/Code Alert software, all RF Technologies processes must be stopped, the data then backed up, and the Server processes restarted. This can be done manually or with a script. A “Server Missing” alarm will display on all Client PCs during this process

Client Requirements

Requirements

RF Technologies has thoroughly tested and validated these client specifications to ensure they meet performance expectation that your life safety security system requires. Clients are available from RF Technologies, or software may be loaded upon customer-supplied clients that meet or exceed the recommended requirements listed below.

Computer	Recommended Requirement
OS	Win7 Enterprise or Professional, 32 or 64-bit with SP1 Win8.1 Enterprise or Professional, 32 or 64-bit with Update (KB2912355) Win10 Enterprise or Professional, 32 or 64-bit Win10 Anniversary Edition, Enterprise or Professional, 32 or 64-bit
CPU	1.67 GHZ or greater
Main Memory	1 GB or greater RAM
HDD	200 MB or greater available space
Network Adapter	10/100 Base-T or faster
USB	Minimum 4 USB 2.0
Sound	soundcard and speakers
Adobe Acrobat	Adobe Acrobat Reader 8.x or later
Internet	Internet Explorer 8,9,10 or 11
Monitor	**Recommended Requirement**
Resolution	1280x1024
Size	17" or greater
Touchscreen	Not required if using keyboard/mouse

Client Computer Configuration

The following configurations must be done to ensure proper operation of the client computers.

Data Entry & Reporting Mode

- Drive mapped to images share on Safe Place/Code Alert Server when logged in
- DHCP or static IPv4 Address
- Must resolve name of Safe Place/Code Alert Server to valid IP address
- Following installation, “Unit Monitored” and “Supervise This Client” options will need to be configured. Configuration details can be found in the Series 10 Administration Guide (0510-1129)

Safety & Security Mode

- All configuration settings listed above for ‘Data Entry & Reporting Mode” must be met
- Computer always Powered On and Logged In
- Safe Place/Code Alert Client Application must be running at all times to display alarms
- Screen Saver is DISABLED
- Power Saving Settings are DISABLED
- Sound and speaker volume must not be muted
- Requires UPS Power
- Windows taskbar option “Keep the taskbar on top of other windows” must be disabled
- Safe Place/Code Alert Client must be configured with “Supervise This Client”. Configuration details can be found in the Series 10 Software Administration Guide (0510-1129)

NOTE: All configured units need to be monitored by at least 1 client computer configured in Safety & Security Mode as defined in the previous section.

Network Requirements

Requirements

The RF Technologies Safe Place/Code Alert Systems require an Ethernet data link to enable communications between device hubs and the Server, and between the Server and the Clients. When this link is supplied by others (typically the customer's IT department) it must be designed and configured to meet the requirements in this document.

Each facility will have its own characteristics, but this document outlines the guidelines and requirements for the infrastructure to support the Safe Place/Code Alert systems.

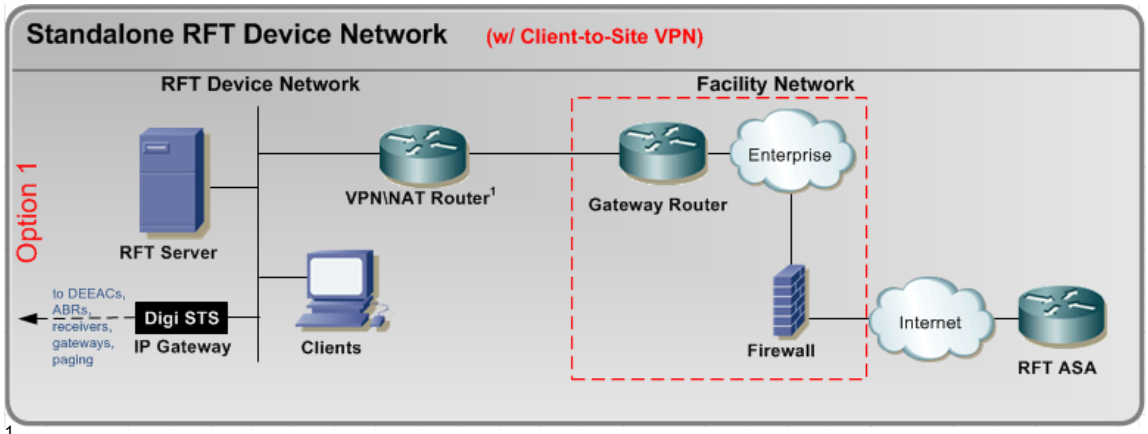
It is possible to use an Ethernet infrastructure installed in the facility as the Safe Place/Code Alert network. When this is done, the customer, network installer, and network administrator must be aware of the system requirements for this network. This approach ensures the performance of the monitoring system. Also, all CAT 5 wiring used must follow the standard Ethernet wiring rules for distance and separation.

Integration

There are three options for integrating the Safe Place/Code Alert system with a customer network. These include:

Standalone

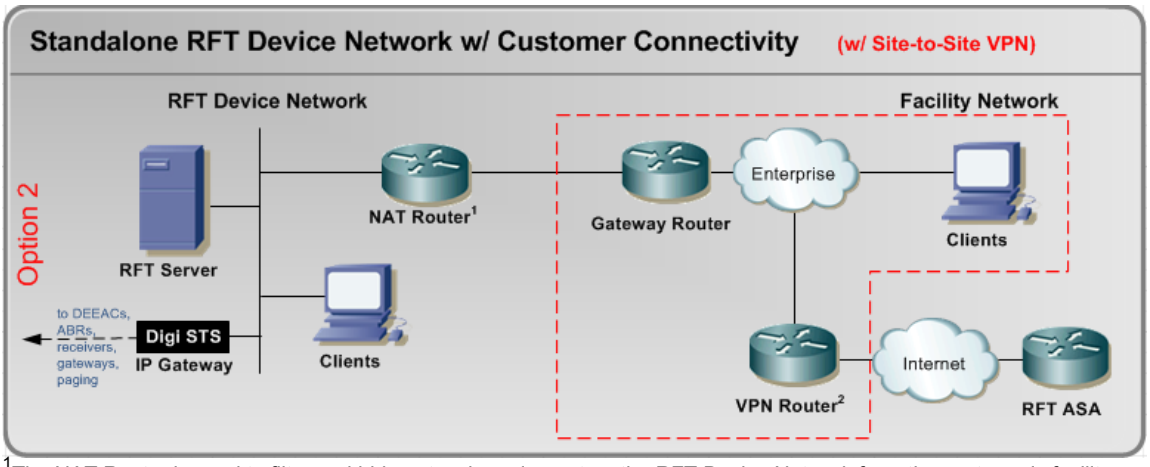
Device And Client Network supplied by RF Technologies with a VPN router connection through the customer's network to facilitate remote service support (if a VPN is used, reference the RFT VPN Access Infrastructure Planning Guide, 0510-0265)



[1]VPN Router is locked down and by default will only communicate with the RFT Server on the inside network and with the RFT ASA Servers on the outside network. The VPN Router automatically establishes VPN communications with the RFT ASA Servers when an Internet connection with UDP ports 500 & 4500 are open

Customer Supplied Client Connectivity

Device Network supplied by RF Technologies and Client Network supplied by customer with a VPN router connection through the customer's network to facilitate remote service support.

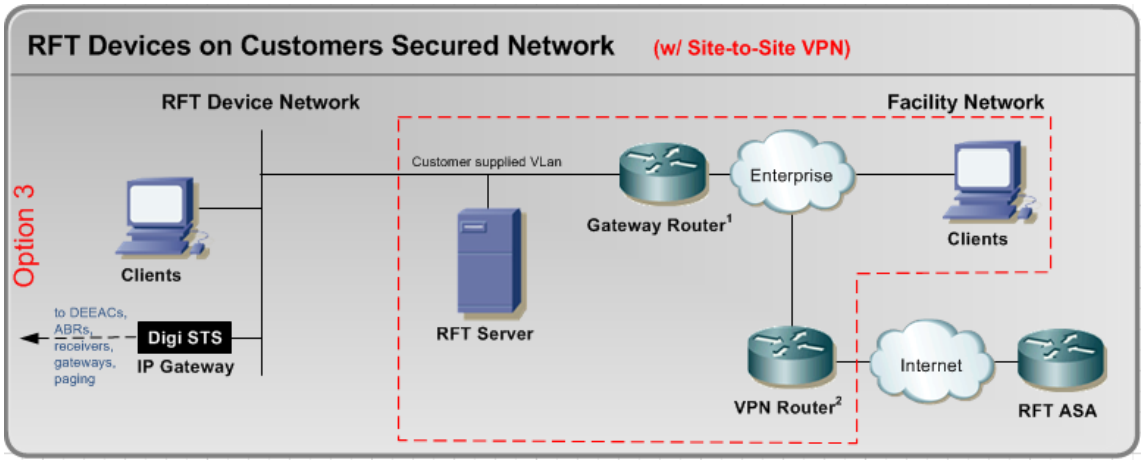


[1]The NAT Router is used to filter and hide network equipment on the RFT Device Network from the customer's facility network. VPN management and Client traffic is permitted through the NAT Router to reach the RFT Server. The NAT Router can also be used to provide remote VPN connectivity back to RFT if a site-to-site VPN is not required or feasible.

[2]A site-to-site VPN tunnel can be established between RFT and the customer's VPN hardware. NATing is used to limit what addresses are routed between networks.

Secured VLAN

Use of a customer supplied VLAN to allow both device and Client system communication across the customer supplied network.



[1]The customer provided Gateway Router is used to filter and hide RFT network equipment on the Customer supplied VLAN from the rest of the facilities network. If required, VPN mgmt and Client traffic is permitted through the Gateway Router to reach the RFT Server.

[2]A site-to-site VPN tunnel is established between RFT and the customer's VPN hardware. NATing is used to limit what addresses are routed between networks.

[3]The RFT Server and IP Gateway need to reside on the same subnet.

Customer Supplied Networks

Network Support Disclaimer

It is the responsibility of the customer to ensure the reliability and security of any networking components supplied by the customer. When the network is supplied by the customer, RF Technologies cannot be held responsible for Safe Place/Code Alert system downtime that results from network downtime.

The network used to communicate between RF Technologies equipment is utilized as a control and a data network. Control networks require more predictable and consistent response times. Increased traffic from corporate intranet data can greatly affect these response times.

Network reliability impacts the collection of data from the Safe Place/Code Alert systems. This data is used to generate reports and to assess the system health. Network reliability also impacts control functions

RF Technologies recommends that the customer employ qualified network support personnel that will maintain the reliability and health of the network post-occupancy. These network support personnel should have industry-recognized certifications to configure and support the installed network.

Customer Responsibilities

When a customer supplied network is utilized:

- Customer will provide primary support for Client computers installed on customer's network.
- Customer will provide 24x7 contacts for network and Client troubleshooting. Personnel will be available and provide access to RF Technologies support personnel if requested. Lack of support may require scheduling additional RF Technologies service visits at an additional charge.
- Remote VPN connection to Safe Place/Code Alert System will be configured only with customer assistance.
- Customer takes responsibility for applying RF Technologies approved antivirus and operating system updates.
- Prior to customer planned network outages, the Safe Place/Code Alert Client application must be shut down on all Client computers and the customer must institute a manual monitoring program if the RFT network equipment and/or Server will be affected.
- Customer is responsible for performing system backups as required.

Equipment Requirements

All RF Technologies equipment connected to the network will have a static IP address and must all be on the same subnet. Multiple subnets can be used if the appropriate routers/gateways are configured to ensure connectivity between all RF Technologies equipment on the network.

Network communications between RF Technologies equipment must not rely on wireless technology.

All network equipment ports connected to RF Technologies Servers and device hubs must be configured to 100 MB/sec or higher data speeds.

NOTE: RFT **strongly** recommends that each Smartphone be assigned a static IP address, or have a reserved IP address on the wireless network for reliable alarm notifications.

System Start-Up

When the network is supplied by others the customer must ensure that the network is operational before the RF Technologies install team arrives on site for system start-up. The system start-up cannot be completed without reliable connectivity between the system components. If start-up cannot be completed because the network is not installed or because any networking equipment required to ensure connectivity between system components is not operational and properly configured, the customer will be required to schedule an additional service visit at an additional charge.

Site and Network Access

RF Technologies Install and Service personnel must have access to all network equipment required to ensure communication between system components on the network. They must be able to connect to any portion of the network utilized by the Safe Place/Code Alert system and employ Ethernet network analysis tools for the purpose of system verification and/or troubleshooting. If access to network equipment and/or use of network analysis tools is not permitted, the customer must ensure that qualified network support personnel are on site and available to support the RF Technologies service engineers during the commissioning process. Lack of support may require scheduling additional field service visits at an additional charge.

Primary Communications

The following tables list the communication configuration requirements for the RF Technologies network. These must be maintained for all network configurations.

Server to Client - Inbound

The server must be able to receive these connections.

Service	Protocol	Inbound Port	Description
Clients	TCP	4007,7142	Primary client communication
SafeServe	TCP	The server's dynamic port range. **Default**: 49152-65535	If the server's Windows Firewall is enabled, SafeServe.exe may instead be configured to accept inbound and outbound connections instead of opening the full dynamic port range.
Server Status/Config	TCP	9185	Status and configuration application Cisco Phone notifications and updates RFT Cares app notifications and updates
MS SQL	TCP	1433	Reporting
Netbios/SMB	TCP	137, 138, 139, 445	Mapped drive to shared image folder on Server
Ping	ICMP	Echo-reply	

Client to Server - Outbound

The client must be able to initiate these connections.

Service	Protocol	Outbound Port	Description
Clients	TCP	4007,7142	Primary client communication
Server Status/Config	TCP	9185	Status and configuration application
MS SQL	TCP	1433	Reporting
Netbios/SMB	TCP	137, 138, 139, 445	Mapped drive to shared image folder on Server
Ping	ICMP	Echo-reply	

Hardware to Server

Service	Protocol	Port	Description
9500 Series Staff Alert Panel	UDP	63125, 63185	Configuration and status messages between device and server.
Digi Port Server	TCP	771	Communication between server and RF hardware

Outbound Messaging

License	Protocol	Port	Description
Email	TCP	25	SMTP/ESMTP only Port number is fixed Secure SMTP (SMTPS) is not supported SMTP servers requiring full address for login (i.e., user@domain) are not supported
Cisco Phone	TCP	9185	Phones must be able to connect to the server via this port
Smartphone	TCP	9185	Phones must be able to connect to the server via this port

VPN to Server

Service	Protocol	Port	Description
Server Status/Config	TCP	9185	Status and configuration application
Clients	TCP	4007,7142	Primary client communications
SNMP Agent	UDP	3125	Monitoring of hardware alarms
MS SQL	TCP	1433	Reporting
ScreenConnect	TCP	8041	Remote control and file sharing
Ping	ICMP	Echo-Reply	

VPT to Server Lights-Out Card

Service	Protocol	Port	Description
https	TCP	443	Hardware status and backup remote control

Revision History

Revision	Change
A	Release
B	**Added**: Java Updates section
C	**Added**: Software version 10.2 added Windows 10 support as a client. **Added:** Recommendation that each Smartphone be assigned a static IP address
D	**Updated:** SafeServe.exe firewall requirements in the Server to Client – Inbound table
E	**Updated:** Port usage and firewall recommendations for client/server communications in the Server to Client – Inbound table

3125 North 126th Street, Brookfield, WI 53005
Phone 800.669.9946 fax 262.790.1784
www.rft.com

0510-0524-E
Release Date: 8/2017