

InfraStruXure® Central Server v5.x: Security

Introduction

This Application Note explains the security associated with APC InfraStruXure Central Server v5.x, providing details on the various security layers within APC InfraStruXure Central as well as discussing the built-in firewall, access levels, and various network ports.

Authentication and Encryption

From InfraStruXure Central to the user

InfraStruXure Central is a server appliance, which is accessed remotely from client workstations via the InfraStruXure Central console, a Java application that is installed on the user's Windows® or Linux workstation. Communications between the InfraStruXure Central server and the system running the InfraStruXure Central console application can be secured (at the user's discretion) via a Secure Sockets Layer (SSL) 168 bit Triple-DES (Data Encryption Standard) encoded connection. This connection encrypts the data three times, using three different 64 bit keys, providing a more secure connection compared to the standard DES algorithm, which encrypts the incoming data once with a single 64 bit key. In addition, communications between the InfraStruXure Central server and other servers (such as LDAP and SMTP mail server) can be encrypted as well.

From InfraStruXure Central to the NetBotz® Appliance

For each NetBotz appliance, the InfraStruXure Central server will, if configured to do so, authenticate the network and security settings over a secure SSL connection. These include username and password. Communication to devices on the customer's LAN public network occurs through a front-end HTTP or HTTPS connection. In order to increase security, the HTTP or HTTPS connection and the HTTP or HTTPS port can be configured for each NetBotz device and for the InfraStruXure Central server using the Advanced View or the InfraStruXure Central console.

Access levels for InfraStruXure Central

InfraStruXure Central comes preconfigured with one administrator account (user name and password are set to "apc" by default). You can configure additional user accounts, each of which can be individually configured to permit varying levels of access to functionality, ranging from View Only access (which enables the user to view information about monitored and managed appliances, but permits no management or control capabilities) to Administrative access (which permits complete access to all monitoring and management capabilities). Each user account has its own unique log-in user name and

password. An administrator has full access to all InfraStruXure Central's functionality. There is no specified limit to the number of user accounts that can be configured for use on an InfraStruXure Central server.

Access levels for individual devices

Individual NetBotz devices use a user name and password for access level verification. By default InfraStruXure Central's "NetBotz Appliance Credentials" option is preconfigured to provide the "netbotz" user name and password when accessing NetBotz appliances on your corporate network and the "apc" user name and password when accessing NetBotz appliances on the InfraStruXure Central private network. InfraStruXure Central can also be configured to display user-specified user names and passwords as necessary. The individual device user name and password must be listed with the user name and password specified in InfraStruXure Central's "Settings -> Server Administration Settings -> NetBotz Appliance Credentials" option in order to be monitored by InfraStruXure Central. If the user name and password do not correspond InfraStruXure Central is unable to monitor the device. For SNMP devices, the SNMP community names must be specified in the discovery entry in the "Edit -> Add Devices" option.

Physical access

Physical access to the connection ports on InfraStruXure Central allows you to remove a network cable, disabling communication. Therefore, as with all critical InfraStruXure components, APC strongly encourages that InfraStruXure Central is placed in a physically secure location to minimize this risk.

Network Ports Used

Only the network ports used by InfraStruXure Central are enabled by default. The table below provides an outline of the network ports used.

Table 1 – *InfraStruXure Central network port information*

Description	Network Access	Port Number	Transmission	Protocol
HTTP Server	Public & Private	80	Incoming & Outgoing	TCP
HTTPS Server	Public & Private	443	Incoming & Outgoing	TCP
SNMP	Public & Private	161, 162	Incoming & Outgoing	UDP
NTP	Public & Private	123	Outgoing	UDP
APC Proprietary Communication Protocol, for use with AP76xx Outlet Strips and Gen. 1 PDU on private LAN	Private	6000	Incoming & Outgoing	UDP
SMTP (optional)	Public	User-specified	Outgoing	TCP
NFS (optional)	Public or Private	2049	Outgoing	UDP
SMB (optional)	Public or Private	139	Outgoing	TCP
LDAP (optional)	Public	User-specified	Outgoing	TCP

File system access

InfraStruXure Central is a server appliance running a Linux platform as its operating system. Access to the server's console through the ports on the server is reserved for use by authorized service personnel. In addition, the Telnet and SSH protocols are disabled by default in InfraStruXure Central to prevent access to the server. SSH can be enabled if desired via the console application, but this feature is intended for use only by APC support personnel when troubleshooting device issues.

Firmware updates

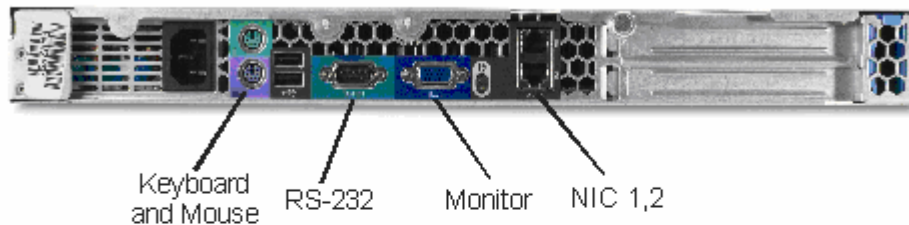
InfraStruXure Central provides the ability to perform firmware updates to managed devices as well as to the server appliance itself. There are three different update processes used by InfraStruXure Central: product update, NetBotz device firmware

update, and APC SNMP device firmware update. All three of these update file types can be downloaded by the user from the APC website, and loaded through the InfraStruXure Central client. The APC and NetBotz firmware updates can also be downloaded to the server from the APC update server, through the InfraStruXure Central client. All files are transferred to the server via HTTP/HTTPS. NetBotz firmware updates are transferred to the devices via HTTP/HTTPS, and APC SNMP firmware updates are transferred to the devices via FTP.

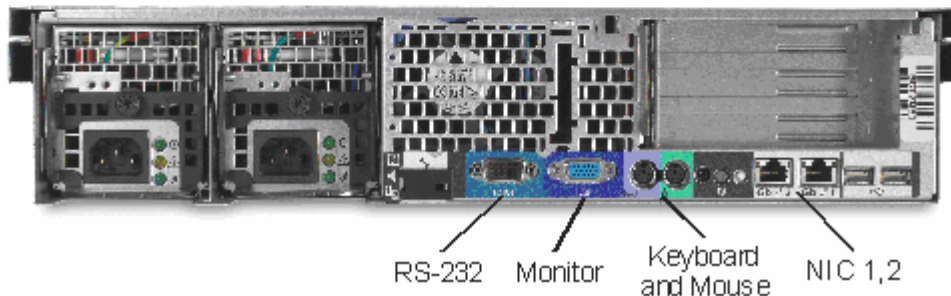
Ports

InfraStruXure Central communication ports are opened solely for communications with NetBotz devices. Refer to the diagrams below to identify the physical connection ports on the InfraStruXure Central server. Please note that the diagrams provided may be different than the actual hardware.

Basic or Standard Edition (rear view):



Enterprise Edition (rear view):



- RS-232 – This service port is used only by support personnel to retrieve low level diagnostic information. Access to the server via this service port requires a user name and password.
- Monitor, Mouse and Keyboard – The monitor, mouse, and keyboard ports are used by APC trained service technicians to access diagnostic information.
- Dual NIC Connections (1 and 2): These Ethernet ports provide connections to your corporate network, and enable you to also connect the InfraStruXure Central server to a private LAN.

Conclusion

InfraStruXure Central is designed with various layers of network and user management security providing a high level of protection from both unauthorized external and internal access to the managed devices, using various methods of user authentication. InfraStruXure Central has incorporated configurable user authentication and device access within the user interface of the server appliance, makes use of the added security features available in SNMP v3, and supports SSL encrypted communications between all monitored and managed devices and the server and management consoles. The combination of these features result in a robust “security-first” solution. Customers from many levels of government and the military, as well as a vast array of private and financial institutions trust the combination of InfraStruXure Central, NetBotz, and APC devices to help protect their valuable assets while increasing uptime, product lifespan, and resource efficiency.