DIGI INTERNATIONAL
11001 Bren Road East
Minnetonka, MN 55343
952-912-3444 tel
952-912-4991 central fax

To: Digi Hardware Customers
From: Donald Schleede – Digi International Inc., Information Security Officer
Date: January 20th, 2016
Subject: Customers looking for recommended configuration settings

At Digi, we understand that many of our customers are concerned about the security of the devices on their network. Additionally, many of Digi's customers need to make sure that they meet certain security guidelines and frameworks. The intent of this document is to describe the recommended steps for increasing the security of a Digi device on a network.

This document outlines the recommended steps for securing a Digi device. The appropriateness of these steps may vary with your application and use. As this is a general document, we are giving general "good practices" recommendations. However, depending on your specific application and network configuration, a recommended setting may create a conflict and affect your application. In some instances, the recommended settings may result in your device becoming unreachable and unmanageable. Digi highly recommends you thoroughly test your configuration before implementing these settings on a production system.

Specific Command References
The information provided below does not specify exact commands and processes to help secure every Digi devices. Please consult the user manuals for your device for that information.

Preparation

Update Firmware
The first step towards securing a device is to make sure you have the most up to date firmware for that device. Please visit the Digi Support website to check your firmware revision, and if necessary for the procedures required to update your firmware.

Note that if you are using Device Cloud (discussed later), the Device Manager functions will allow you to update several devices at once.

Disable Services

DIGI INTERNATIONAL
11001 Bren Road East
Minnetonka, MN 55343
952-912-3444 tel
952-912-4991 central fax

Overview

To increase the overall security of any device, it is recommended that you disable and turn off any unused services or "listening" ports that are not being used in your solution. Each service that is enabled adds to the "threat surface", or the overall threat, that a device exposes to an attacker. If a device will be connected directly to the Internet, or to a public APN on a cellular network, we highly suggest disabling any device administrative interfaces or services on the public interface.

If using Device Cloud, we suggest managing your devices through Device Manager functions. By using the Device Manager functions, the remote management services like telnet and SSH services can be turned off, as all configuration and management can be done through Device Manager functions. Disabling these administration services significantly reduces the exposed risk by the device.

NOTE: Some services, however, are critical to the function that the device is performing. Security is always a tradeoff between security and use. It is ultimately up to the end user to decide where this tradeoff needs to be established. Below are the recommended services on most Digi devices that should be disabled whenever possible.

Disable ADDP service/protocol

The ADDP protocol is used to discover and configure a device from the local area network. It's a great tool especially for initial network set up, but after initial set-up it is a good idea to disable the service. If you disable this service, the device will no longer respond to the local network device discovery tools that Digi publishes, or other third party tools that rely on the ADDP protocol. Digi suggests disabling this service only after it is registered with Device Cloud or the IP address has been set statically and information has been recorded in a safe place.

Disable Telnet / SSH / HTTP / HTTPS

The Telnet/SSH services provide access to the admin command line interface that is used to manage a device. HTTP/HTTPS are services that provide admin Web Interface access that is used to manage a device. It is recommended to disable as many of these services as possible. If the device is to be managed locally it is recommended to disable the telnet and HTTP services, and use either the SSH service for command line configuration, or HTTPS for web GUI configuration.

DIGI INTERNATIONAL
11001 Bren Road East
Minnetonka, MN 55343
952-912-3444 tel
952-912-4991 central fax

If the devices are managed through the Device Cloud's management function, Digi recommends turning off all of these services locally on the device to force all administration to occur through Device Cloud's management functions.

NOTE: If all services are disabled along with all other management interfaces it could cause you to lose the ability to manage the device. If this occurs, the only way to regain access to the device is to reset the device to factory specifications.

Disable SNMP

The SNMP service is used to remotely monitor and manage devices using common Simple Network management Protocol (SNMP) management tools. This service should be disabled if SNMP management tools will not be used. If SNMP management tools will be used, we suggest changing the public and private community names in the device.

Disable TCP and UDP ECHO

The TCP and UDP ECHO services are used typically for connectivity testing. These services should, by default, be turned off.

Change Device Parameters

Set a static IP address/netmask gateway

It is recommended that gateways installed on the network have a static IP address, static DNS server IP address, and DHCP disabled, including a failback to DHCP.

Please validate the parameters used below with your network administrator. If these parameters are not correct, you will lose connectivity to your device after a reboot of the device.

NOTE: In many instances, disabling the DHCP configuration may not be ideal, particularly in a private or home setting. For corporate settings, it is highly recommended not to use DHCP.

Set an NTP server for proper time stamping of logs

An NTP server is required to accurately report information within the device logs. You may want to discuss this setting with your network administrator, as they may have a preferred or internal NTP time server.

DIGI INTERNATIONAL
11001 Bren Road East
Minnetonka, MN 55343
952-912-3444 tel
952-912-4991 central fax

Set a login admin password on the device

Some Digi devices are shipped with a default user id and password. When a device is initially installed, a new user id and password should be set on the device. Once this is configured, the device will require this information to gain access to the device remotely through the remote telnet/SSH/HTTP/HTTPS sessions.

If using Device Cloud, it is recommended that this admin password be used only in an emergency. For device parameter changes, we suggest using the Device Manager functions. Settings to a device through Device Cloud can be tracked back to an individual user and all actions are logged.

NOTE: Digi suggests not using "admin" (or something similar) as your user id or password.

Setting a password for the "admin" and other configured users

Password will be required if you need to SSH/Telnet/HTTP/HTTPS into the device. When choosing a password, we recommend following proper password choosing processes. This consists of using passwords that are not based on a dictionary word, that are at least 8 characters long, contain upper and lower case characters, number, and have some level of complexity. Alternatively, all enabled services Telnet/SSH/HTTP/HTTPS need to require a password prior to getting access to any admin functions. If your device supports a TACACS or RADIUS server, we highly suggest configuring your device to use these remote identification services. When TACACS or RADIUS is configured, we recommend using local accounts only for a failsafe mechanism if communication to the identification server fails.

If you are using Device Manager functions within Device Cloud, this user id and password should be a password of last resort. It should only be used in case of an emergency.

Use encrypted interfaces

When you need to use a device service to transfer data from serial devices connected to the Digi end device, especially when data transfer is happening over the public Internet, it is important to configure and use encrypted services and interfaces. This includes accessing the serial port on the Digi device via SSH, SSL, or an Encrypted RealPort connection.

Final Steps

Enable device backup

DIGI INTERNATIONAL
11001 Bren Road East
Minnetonka, MN 55343
952-912-3444 tel
952-912-4991 central fax

Perform a backup of the device. This will ensure that you have a configuration saved which can be used to restore the device in the event of a factory reset.

Restart the device and enable all settings

To apply all of the settings, it is recommended that you restart the device.

Validation

To validate that your settings have taken hold and that a device threat has been reduced, we suggest the use of scanning tools to verify that services are disabled or the live services are properly configured.

The use of these tools is not covered in this document. Digi also suggests that a trained professional review any installation where the controlling devices or data are of a critical nature.

Below are examples of security scanning tools.

- Nmap – Port Scanning tool
- Nessus – "Free" vulnerability scanning tool
- Paros Proxy – OWASP provided Web application scanning tool
- BuRP – Web application scanning tool

Using Device Cloud to Manage Devices

For devices connected to the public Internet, it is highly recommended that you use Device Manager functions within Device Cloud to manage the overall security of your devices. With Device Manager, many of the security requirements (such as configuration control, Role Based Access Control (RBAC), logging) can be applied to your devices in a simple fashion.

If you are using Device Manager functions to manage your devices, you can significantly reduce security risk by effectively turning off all remote admin functions on the device, and using Device Cloud exclusively for management. It is important to note that implementing these steps may lock your device down so that management of the device cannot be done locally.

DIGI INTERNATIONAL
11001 Bren Road East
Minnetonka, MN 55343
952-912-3444 tel
952-912-4991 central fax

If you intend to use Device Cloud to manage your security, please validate that you have registered your device in the system and that your device is connected to it. We recommend that you setup Device Cloud user accounts so that management of devices does not require shared passwords or accounts. With these accounts, you can setup role based access controls to restrict what is needed to manage your gateways.

Set a device password for Device Cloud

To ensure that your device can't be copied and have fake data sent to Device Cloud, your device and Device Cloud can share a password that identifies the specific device. Once this password is set, it only allows your specific device and password to send data to Device Cloud.

Set the connection to a secure method (SSL)

Enabling this feature will make the connection to Device Cloud encrypted using the industry standard Internet encryption protocol. The encryption uses TLSv1 or SSLv3 or above with AES256-SHA, AES128-SHA or RC4-128-SHA encryption. This connection is made to Device Cloud via TCP port 3199 (unencrypted traffic uses TCP port 3197).

Disclaimer

This document is for informational purposes only, and is meant as a general guide to help our customers implement best practices security on a Digi device. It is ultimately the customer who must certify that a device is compliant with their own specific framework. Digi does not make any guarantees about the following information, or state that following this guide will guarantee that the device will meet your specific requirements. If a customer would like additional recommendations on device configurations, a professional services group can be engaged to help with your specific scenario to help secure and configure your devices in the safest possible way.

Thank you for your concerns on our products.

Donald Schleede - Digi Information Security Officer
Donald.schleede@digi.com 952-912-4951