AnywhereUSB

User Guide

Revision history—90001085

Revision	Date	Description
R	December 2019	Added information about the unique password on the device label, used to access the web UI.
S	February 2020	Updated instructions for enabling the encrypted AnywhereUSB network service.
T	May 2020	Updated SNMP configuration section. Updated encrypted network service information.
U	March 2021	Updated the Network Settings section.
V	September 2021	Added information: X.509 Certificate/Key Management Updated: Install the driver software

Trademarks and copyright

Disclaimers

Information in this document is subject to change without notice and does not represent a commitment on the part of Digi International. Digi provides this document “as is,” without warranty of any kind, expressed or implied, including, but not limited to, the implied warranties of fitness or merchantability for a particular purpose. Digi may make improvements and/or changes in this manual or in the product(s) and/or the program(s) described in this manual at any time.

Warranty

To view product warranty information, go to the following website:

www.digi.com/howtobuy/terms

Send comments

Documentation feedback: To provide feedback on this document, send your comments to techcomm@digi.com.

Customer support

Digi Technical Support: Digi offers multiple technical support plans and service packages to help our customers get the most out of their Digi product. For information on Technical Support plans and pricing, contact us at +1 952.912.3444 or visit us at www.digi.com/support.

Contents

AnywhereUSB User Guide

Get started

Initial AnywhereUSB configuration

Connect a host computer to AnywhereUSB

AnywhereUSB Remote Hub Configuration Utility

Configure AnywhereUSB encryption

Discover AnywhereUSB devices on other subnets

Hardware specifications

Multi-host connections

Configure from the web interface

Configure from the command line

X.509 Certificate/Key Management

Troubleshooting

Regulatory and safety information

Appendix A: AnywhereUSB permitted device list

Appendix B: Understanding hubs

Appendix C: Firewall support

AnywhereUSB User Guide

The AnywhereUSB is the first remote networking solution to utilize USB over IP® technology. Since the host computer or server may be located remotely, you can deploy AnywhereUSB devices in harsh or non-secure environments, making it ideal for point-of-sale, kiosks, surveillance, industrial automation, or any mission-critical enterprise application. This Ethernet-attached solution provides two, four, five, or fourteen USB ports to connect peripheral devices such as USB license dongles, barcode scanners, receipt printers, as well as Digi Watchport®/V2 or Watchport®/V3 USB Camera and Watchport Sensors.

The AnywhereUSB product line consists of the following models:

- AnywhereUSB/5 (first generation) components
- Second generation AnywhereUSB models

  The second generation AnywhereUSB devices provide a built-in web server and a command line interface (CLI) for additional configuration options.

  - AnywhereUSB/2 components
  - AnywhereUSB/5 (G2 and M models) components
  - AnywhereUSB/5 (G2 and M models) components
  - AnywhereUSB/14 components
  - AnywhereUSB/TS44 components

Configurable features

This section provides an overview of configurable features for the following products:

- AnywhereUSB/2
- AnywhereUSB/5 (G2)
- AnywhereUSB/5 M
- AnywhereUSB TS44
- AnywhereUSB/14

User Interfaces

There are several user interfaces for configuring and monitoring the AnywhereUSB family, including:

- Digi Device Discovery Utility, used to configure IP settings
- Web user interface (UI) for advanced configuring, monitoring, and administration
- AnywhereUSB command line interface (CLI)

- Simple Network Management Protocol (SNMP)
- AnywhereUSB Configuration Utility, used to connect/disconnect host computers

IP address assignment

There are several ways to assign an IP address to an AnywhereUSB:

- **Static IP**: Assign a specific IP address to a device, through the Digi Device Discovery Utility, the web UI, or the CLI.
- **Dynamic Host Configuration Protocol (DHCP)**: This is enabled by default. Use DHCP to automatically assign IP addresses, to deliver TCP/IP stack configuration parameters, such as the subnet mask and default gateway, and to provide other configuration information.
- **Auto Private IP Addressing (APIPA), also known as Auto-IP**: A standard protocol that will automatically assign an IP address from a reserved pool of standard Auto-IP addresses to the computer on which it is installed. The device is set to obtain its IP address automatically from a DHCP server. But if the DHCP server is unavailable or nonexistent, Auto-IP will assign the device an IP. If DHCP is enabled or responds later or you use ADDP, both will override the Auto-IP address previously assigned.

Security

Security-related features in AnywhereUSB include:

- Secure access and authentication to the web UI and CLI.
- One password, one permission level.
- Selectively enable and disable network services such as ADDP, HTTP/HTTPS, SSH, SNMP, and telnet.
- Encrypted AnywhereUSB traffic: An optional setting that allows a host computer to confirm the AnywhereUSB device authenticity and to encrypt USB-over-IP traffic.

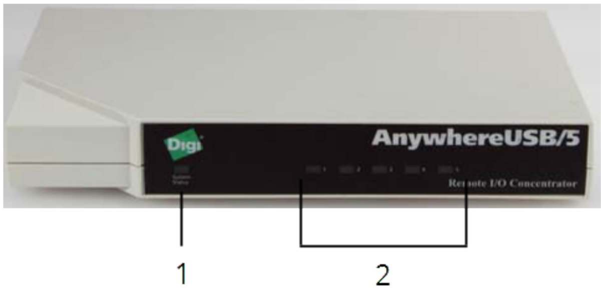
Configuration management

After an AnywhereUSB is configured and running, periodically perform any necessary configuration-management tasks, such as:

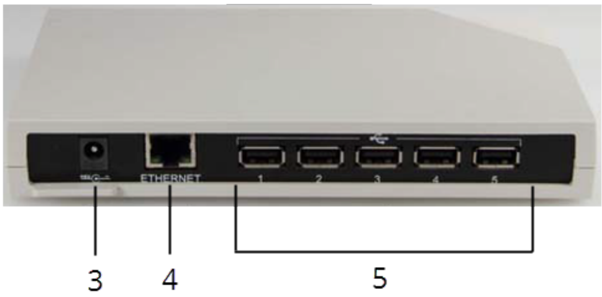
- Upgrade firmware
- Upgrade device driver
- Back up device configuration
- Reset to factory default settings
- Restart the device

AnywhereUSB/5 (first generation) components

Front panel



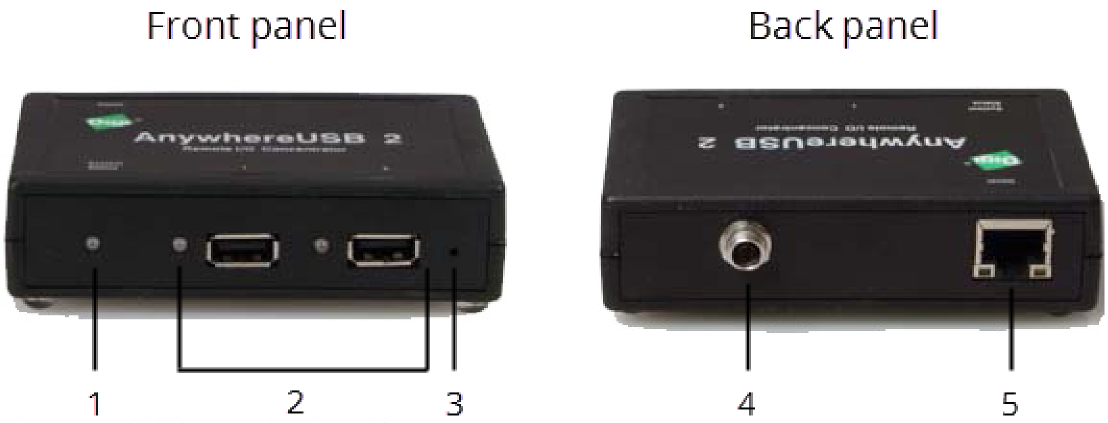
Back panel



Item	Name	Description
1	System Status LED	On initial power-up, the System Status LED is orange for two seconds while the system initializes and then blinks slow green. If you have enabled DHCP d and the device is booting up, the System Status LED is orange while the AnywhereUSB searches for a DHCP server. If it cannot find a DHCP server, it returns to the default configuration to allow the Configuration Utility to assign a static IP address. If the System Status remains red for an extended period of time, contact Digi Technical Support.
2	USB LEDs	Five USB LEDs; note the following LED patterns: ■ Green hunting pattern across all 5 USB LEDs: Not connected to a host computer. ■ Orange alternating on ports 1-3-5 and 2-4: Updating image in Flash. Do not remove power from AnywhereUSB while flash is being updated. Doing so damages your AnywhereUSB. ■ Solid green: The USB ports are connected to a host computer. ■ Green over red hunting pattern: Contact Digi Technical Support.

Item	Name	Description
3	Power connector	Use the included power adapter. **Note** The first generation AWUSB/5 uses a center-negative power supply which is different than the newer AWUSB/5 (G2) and AWUSB/5 M devices. Power-supplies are NOT interchangeable; use only the power supply that is provided with the device.
4	Ethernet connector	The left Ethernet LED is green when connected to a network and the right Ethernet LED blinks orange when there is data transmission activity on the port. Use a standard Ethernet cable.
5	USB ports	Five USB ports to connect USB devices.

AnywhereUSB/2 components



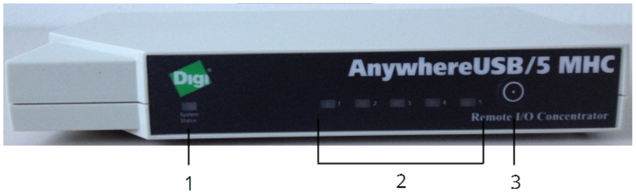
Item	Name	Description
1	System Status LED	When the device is powered on and during normal operation, the System Status LED blinks slow green. If the System Status light blinks red for an extended period of time, contact Digi Technical Support.
2	USB LEDs and ports	Two USB ports with two USB LEDs. The USB LEDs are solid green when any of the USB ports are connected to a host computer. The USB LEDs are off when any of the USB ports are not connected to a host computer.
3	Reset button	Use this button to either restart the device or reset its configuration to factory defaults.
4	Power connector	Use the included power adapter.

Item	Name	Description
5	Ethernet connector	The left Ethernet LED is green when connected to a network and the right Ethernet LED blinks orange when there is data transmission activity on the port. Use a standard Ethernet cable.

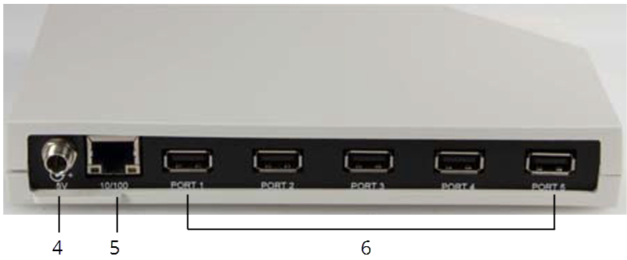
AnywhereUSB/5 (G2 and M models) components

The AnywhereUSB/5 (G2) and AnywhereUSB/5 M models have the same controls, ports, and connectors, as shown in the following image of an AnywhereUSB/5 M.

Front panel



Back panel

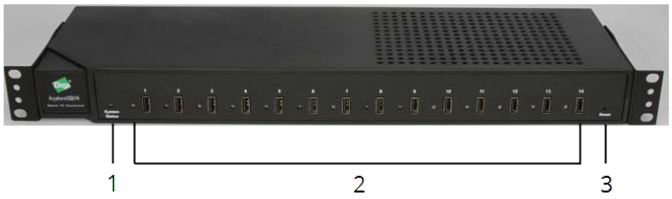


Item	Name	Description
1	System Status LED	When the device is powered on and during normal operation, the System Status LED blinks slow green. If the System Status light blinks red for an extended period of time, contact Digi Technical Support.
2	USB LEDs	Five USB LEDs. A USB LED is solid green when its USB port is connected to a host computer. A USB LED is off when its USB port is not connected to a host computer.
3	Reset button	When pressed, the Reset button either restarts the device or resets its configuration to factory defaults.

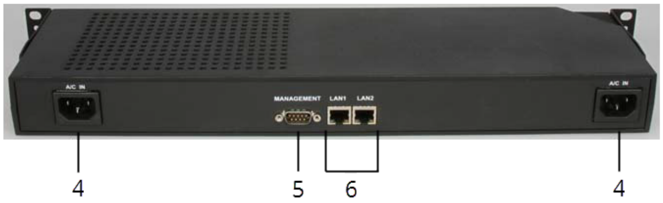
Item	Name	Description
4	Power connector	Use the included power adapter. **Note** The second generation AWUSB/5 (G2 and M) uses an improved center-positive power supply with a locking barrel connector, which is different than first generation AWUSB/5 devices. Power-supplies are NOT interchangeable; use only the power supply provided with the device.
5	Ethernet connector	The left Ethernet LED is green when connected to a network and the right Ethernet LED blinks orange when there is data transmission activity on the port. Use a standard Ethernet cable.
6	USB ports	Five USB ports to connect USB devices.

AnywhereUSB/14 components

Front panel



Back panel

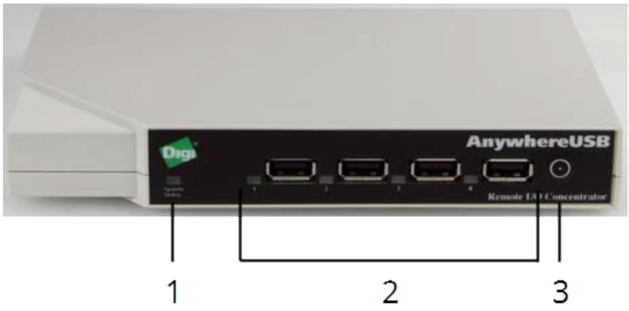


Item	Name	Description
1	System Status LED	When the device is powered on and in normal operation, the System Status LED blinks slow green. If the System Status light blinks red for an extended period of time, contact Digi Technical Support.
2	USB LEDs and ports	Fourteen USB ports with corresponding LEDs. A USB LED is solid green when a USB port is connected to a host computer. A USB LED is off when a USB port is not connected to a host computer.
3	Reset button	Use this button to either restart the device or reset its configuration to factory defaults.

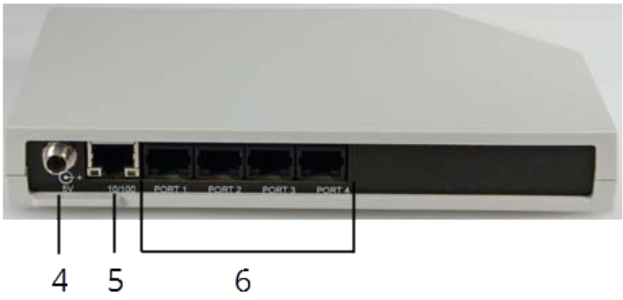
Item	Name	Description
4	Power connector	The AnywhereUSB/14 has two power connectors. When using only one power cable, you can use either of the power connectors. Use the included power cables.
5	RS-232 DB9 serial port	Use these serial ports when using RealPort or for console access to the AnywhereUSB device.
6	Ethernet connector	The AnywhereUSB/14 has two Ethernet connectors for redundancy. The left Ethernet LED is green when connected to a network and the right Ethernet LED blinks orange when there is data transmission activity on the port. Use the ports as follows: ■ LAN1 is the primary Ethernet port. Use this port when connecting only one Ethernet cable or as the main Ethernet connection when connecting both Ethernet ports. ■ LAN2 is the secondary Ethernet port and is used only for redundancy. Only connect an Ethernet cable to this port when you are already using LAN1. Use a standard Ethernet cable.

AnywhereUSB/TS44 components

Front panel



Back panel



Item	Name	Description
1	System Status LED	When the device is powered on and in normal operation, the System Status LED blinks green. If the System Status light blinks red for an extended period of time, contact Digi Technical Support.
2	USB LEDs and ports	Four USB ports and corresponding LEDs. A USB LED is solid green when its USB port is connected to a host computer. A USB LED is off when its USB port is not connected to a host computer.
3	Reset button	Use this button to either restart the device or reset its configuration to factory defaults.
4	Power connector	Use the included power adapter.
5	Ethernet connector	The left Ethernet LED is green when connected to a network and the right Ethernet LED blinks orange when there is data transmission activity on the port. Use a standard Ethernet cable. **Note** The AWUSB/14 has one network interface that supports one IP address. For more information, see AnywhereUSB/14 redundancy features in detail Knowledge Base article at knowledge.digi.com.
6	RS-232 RJ45 serial ports	Use these serial ports when using RealPort or for console access to the AnywhereUSB device. For more information about compatible Digi cables and cable adapters, see Serial Cables on www.digi.com.

RealPort software

The AnywhereUSB TS44 and AnywhereUSB/14 use RealPort COM port redirection for Microsoft Windows environments. RealPort software provides a virtual connection to serial devices, no matter where they reside on the network. The software is installed directly on the host computer and allows applications to talk to devices across a network as though the devices were directly attached to the host. Actually, the devices are connected to a Digi device somewhere on the network.

RealPort is unique among COM port re-directors because it is the only implementation that allows multiple connections to multiple ports over a single TCP/IP connection. Other implementations require a separate TCP/IP connection for each serial port. Unique features also include full hardware and software flow control, as well as tunable latency and throughput.

Encrypted RealPort

AnywhereUSB/14 and AnywhereUSB TS 44 supports RealPort software with encryption. Encrypted RealPort offers a secure Ethernet connection between the COM port and an AnywhereUSB device. Encryption prevents internal and external snooping of data across the network by encapsulating the TCP/IP packets in a Secure Sockets Layer (SSL) connection and encrypting the data using Advanced Encryption Standard (AES), one of the latest, most efficient security algorithms.

The Digi RealPort with encryption driver has earned Microsoft's Windows Hardware Quality Lab (WHQL) certification.

Drivers are available for a wide range of operating systems. It is ideal for financial, retail/point-of-sale, government or any application requiring enhanced security to protect sensitive information.

You can enable or disable access to the Encrypted RealPort service.

For details, see the *RealPort Installation User Guide* on www.digi.com.

Get started

This chapter explains what comes with each AnywhereUSB model, how to connect the hardware, and installing the necessary software.

What’s in the box?

All AnywhereUSB models include the following hardware in the box:

- AnywhereUSB device
- Power supply

  Note AnywhereUSB/14 domestic orders include two power cords.

Note A loose label sticker that includes the unique device password may be included in the box. Retain this label sticker with your hardware records. This default password will be needed if the device is factory reset and you want to access the web UI on the device or register the device with Digi Remote Manager®. If the device was already registered with Remote Manager at the time of the factory reset, you do not need the unique password to access the device in Remote Manager.

Connect the hardware

You need a standard Ethernet cable, your AnywhereUSB device and power supply to complete these steps.

1. Connect a standard Ethernet network cable to the Ethernet port on the back of the AnywhereUSB device and the other end to the Ethernet port on a switch.
2. Connect the power supply or power cord (AnywhereUSB/14) to the power connector on the back of the AnywhereUSB device and the other end into a power outlet.

   For the AnywhereUSB/14, you can use either power connector on the back on the device.

Before using the AnywhereUSB, you need to install the driver software, configure the IP address, and set up security (optional).

Install the driver software

You need a Microsoft Windows computer (host computer) to download and install the AnywhereUSB driver software from the Digi International Support website. The driver software includes the AnywhereUSB Remote Hub Configuration Utility.

After the driver software installs, the AnywhereUSB Remote Hub Configuration Utility opens. The utility automatically discovers AnywhereUSB devices on the local subnet and displays configuration information, including the DHCP address for a device.

Before you begin

Before you begin, you must uninstall any existing older AnywhereUSB driver (AnywhereUSB Remote Hub Configuration Utility) before you can re-install the driver software.

- You must perform the uninstall as a Windows Administrator.
- When the uninstall process is complete, reboot Windows once.

⚠ Only a Windows Administrator can perform the software install. If you are logged in as a non-Windows Administrator user and you attempt to install the software, you will be required to enter Windows Administrator login credentials to be able to complete the installation process.

Download and install the driver

1. Navigate to the AnywhereUSB support page.
2. Click the **Product Resources** tab. This should be selected by default.
3. From the **Drivers & Patches** section, click the **OS Specific Drivers** link.
4. From the list box, select the appropriate operating system option. A list of drivers for that OS displays.
5. Click the **download** link for the driver option that you want to install.
6. When the download is complete, right-click on the file and choose **Open** to start the install process.
7. When the installation is complete, reboot Windows once.
8. Repeat this process for each host computer.

Note “Host computer” refers to a Microsoft Windows-based computer that you use to connect to the AnywhereUSB. In a virtual environment, the host computer is the Windows-based virtual machine. You do not need to install the AnywhereUSB drivers on the physical server running the virtual machine (sometimes called host).

Initial AnywhereUSB configuration

After connecting the hardware and installing the software, you can connect the device to the network and configure additional options, such as a static IP address, USB port groups, and encryption.

Configure the IP address

When successfully connected to a network, each AnywhereUSB device gets an IP address. The first generation AnywhereUSB/5 model has a default static IP address and the second generation AnywhereUSB/2/5/5M/14/TS44 models have dynamic IP addresses. You can make changes to the IP address, such as assigning a static IP. Make sure you follow the instructions for your AnywhereUSB model.

Note The host computer running Digi Device Discovery Utility and the AnywhereUSB device must be on the same subnet.

AnywhereUSB/5 (first generation)

AnywhereUSB (second generation)

AnywhereUSB/5 (first generation)

By default, first generation AnywhereUSB/5 models support DHCP, but have static IP addresses.

Default IP address configuration:

- IP address: 192.168.254.222
- Subnet mask: 255.255.0.0

To configure a static IP address:

1. Open the **AnywhereUSB Remote Hub Configuration Utility**, which is included in the driver software you previously downloaded and installed. See Get started.
2. Select your **AnywhereUSB/5** from the list on the left.
3. Click **Configure**.
4. Type the IP address, subnet mask, and default gateway.
5. Click **Update**.

AnywhereUSB (second generation)

DHCP is enabled by default on all second generation AnywhereUSB models.

Second generation AnywhereUSB models include:

- AnywhereUSB/2
- AnywhereUSB/5 (G2)
- AnywhereUSB/5 M
- AnywhereUSB TS44
- AnywhereUSB/14

The host computer connects only by using the AnywhereUSB IP address. If the AnywhereUSB IP address changes, the connection is lost. We recommend assigning a static IP address to make sure your device always has the same IP address and remains connected to the host computer. You can use either the web UI or the Digi Device Discovery Utility to configure the IP address.

- Configure the IP address with Digi Device Discovery Utility
- Configure the IP address with the web UI

Configure the IP address with Digi Device Discovery Utility

Use the Digi Device Discovery Utility to:

- View the IP address of an AnywhereUSB device.
- Configure a static IP address when the AnywhereUSB does not obtain an IP address from a DHCP server (such as when there is no available DHCP server).

Note You must run the Digi Device Discovery Utility from a computer on the same subnet as the AnywhereUSB. If discovery fails, make sure that the Microsoft Windows Firewall is off. For additional troubleshooting help, visit the Digi Knowledge Base at knowledge.digi.com.

To configure a static IP address using the Digi Device Discovery Utility:

1. Download and install the Digi Device Discovery Utility:
   a. Go to www.digi.com/support#support-tools.
   b. From the **Support Downloads** section, click **Drivers**.
   c. Find and select **Device Discovery** from the product list.
   d. From the **Diagnostics, Utilities and MIBs** drop-down list, select your operating system.
   e. Download the utility for your operating system and install it.
6. Open the **Digi Device Discovery Utility**.
7. Right-click your AnywhereUSB device and select **Configure network settings**.
8. Type the IP address, subnet mask, and default gateway.
9. Click **Save**.

Configure the IP address with the web UI

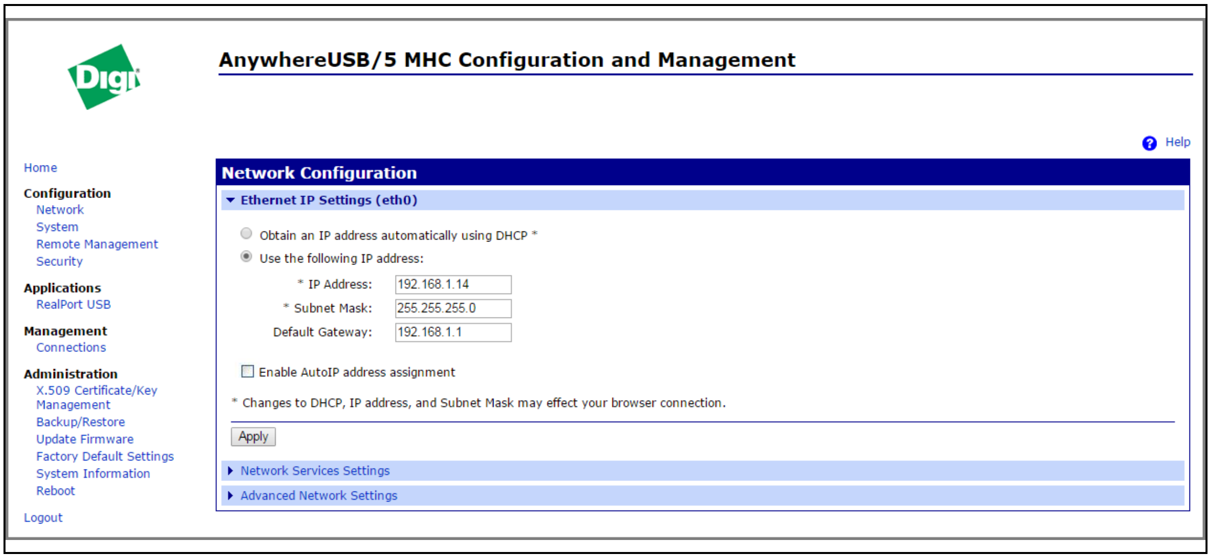
Use the AnywhereUSB Configuration and Management web UI to configure the AnywhereUSB with a static IP address.

To configure a static IP address using the web UI:

1. Open a web browser and type the AnywhereUSB IP address in the URL field. If you do not know the device IP address, use the Digi Device Discovery Utility or the AnywhereUSB Remote Hub Configuration Utility to get the IP address or connect directly to the web UI.
2. Log in to the web UI.
   - **User name**: **root**
   - **Password**: The unique, default password printed on the device label. If the default user name and password does not work, they may have been changed. Contact your system administrator for help.

Note If a password is not printed on the label, or the log in screen does not display, password authentication has not been enabled. See Security settings or contact your system administrator for help.

3. Select **Configuration > Network**.
   a. Select **Use the following IP address**.
   b. Type the IP address, subnet mask, and default gateway.
3. Clear the **Enable AutoIP** address assignment check box.
4. Click **Apply**. The network settings are updated and the web UI refreshes.



○ Obtain an IP address automatically using DHCP *
● Use the following IP address:

* IP Address: 192.168.1.14
* Subnet Mask: 255.255.255.0
Default Gateway: 192.168.1.1

□ Enable AutoIP address assignment

* Changes to DHCP, IP address, and Subnet Mask may effect your browser connection.

Connect a host computer to AnywhereUSB

This section explains how to configure the host computer to establish a connection to the AnywhereUSB device using the AnywhereUSB Remote Hub Configuration Utility.

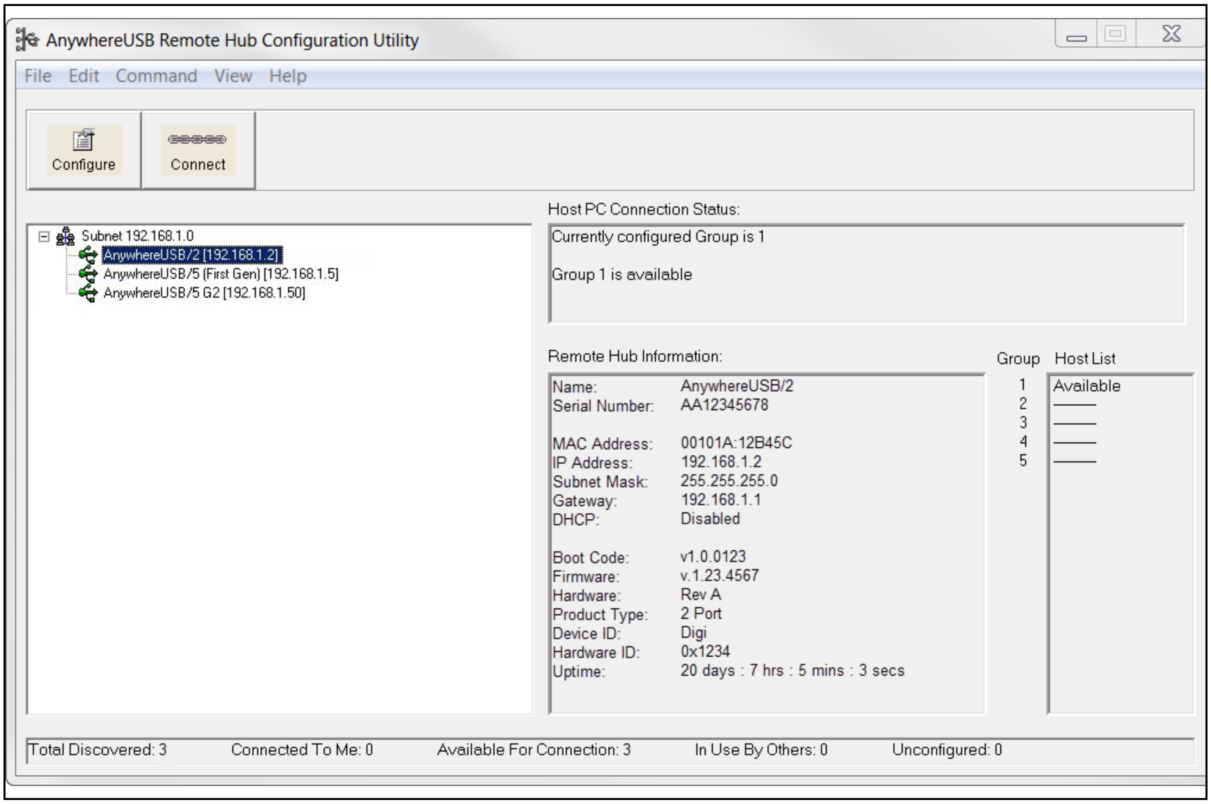
Connect to the AnywhereUSB

To use the USB devices that are attached to the AnywhereUSB, the host computer must first establish a connection to the AnywhereUSB.

Note For AnywhereUSB/5M and AnywhereUSB/14 multi-host models, assign groups before connecting to the host computer through the AnywhereUSB web UI. For details, see Multi-host connections.

1. Log in to a Microsoft Windows computer with an account that has administrative privileges.
2. Select **Start > Programs > AnywhereUSB > AnywhereUSB Remote Hub Configuration Utility**.

   The utility displays a list of all AnywhereUSB devices on your local subnet and on any subnet configured in the Discovery List.


AnywhereUSB Remote Hub Configuration Utility
File Edit Command View Help
Configure
Connect

Subnet 192.168.1.0
AnywhereUSB/2 [192.168.1.2]
AnywhereUSB/5 (First Gen) [192.168.1.5]
AnywhereUSB/5 G2 [192.168.1.50]

Host PC Connection Status:

Currently configured Group is 1

Group 1 is available

Remote Hub Information:

Name:	AnywhereUSB/2
Serial Number:	AA12345678
MAC Address:	00101A:12B45C
IP Address:	192.168.1.2
Subnet Mask:	255.255.255.0
Gateway:	192.168.1.1
DHCP:	Disabled
Boot Code:	v1.0.0123
Firmware:	v.1.23.4567
Hardware:	Rev A
Product Type:	2 Port
Device ID:	Digi
Hardware ID:	0x1234
Uptime:	20 days : 7 hrs : 5 mins : 3 secs

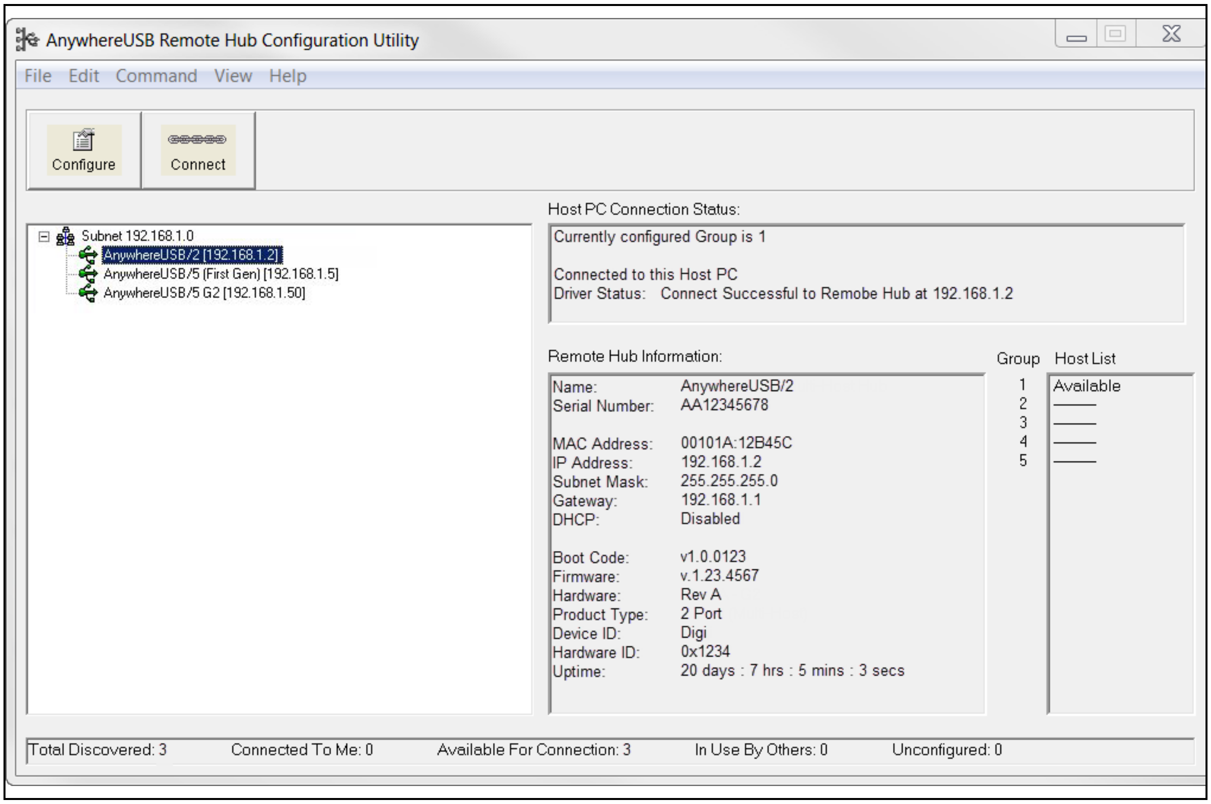
Group	Host List
1	Available
2	———
3	———
4	———
5	———

Total Discovered: 3 Connected To Me: 0 Available For Connection: 3 In Use By Others: 0 Unconfigured: 0

3. Select an AnywhereUSB device from the device list in the AnywhereUSB Remote Hub Configuration Utility and then do one of the following:
   - Click **Connect**.
   - Right-click and connect to a group.

   The host computer then attempts to connect to the AnywhereUSB.

   The Connection Status now says **Connected to this Host PC**.


AnywhereUSB Remote Hub Configuration Utility
File Edit Command View Help
Configure
Connect

Subnet 192.168.1.0
AnywhereUSB/2 [192.168.1.2]
AnywhereUSB/5 (First Gen) [192.168.1.5]
AnywhereUSB/5 G2 [192.168.1.50]

Host PC Connection Status:

Currently configured Group is 1

Connected to this Host PC
Driver Status: Connect Successful to Remobe Hub at 192.168.1.2

Remote Hub Information:

Name:	AnywhereUSB/2
Serial Number:	AA12345678
MAC Address:	00101A:12B45C
IP Address:	192.168.1.2
Subnet Mask:	255.255.255.0
Gateway:	192.168.1.1
DHCP:	Disabled
Boot Code:	v1.0.0123
Firmware:	v.1.23.4567
Hardware:	Rev A
Product Type:	2 Port
Device ID:	Digi
Hardware ID:	0x1234
Uptime:	20 days : 7 hrs : 5 mins : 3 secs

Group	Host List
1	Available
2	———
3	———
4	———
5	———

Total Discovered: 3 Connected To Me: 0 Available For Connection: 3 In Use By Others: 0 Unconfigured: 0

For details about the AnywhereUSB Remote Hub Configuration Utility, see AnywhereUSB Remote Hub Configuration Utility.

AnywhereUSB Remote Hub Configuration Utility

This chapter explains how to use the AnywhereUSB Remote Hub Configuration Utility.

Start the AnywhereUSB Remote Hub Configuration Utility

This section explains how to start the AnywhereUSB Hub Configuration Utility.

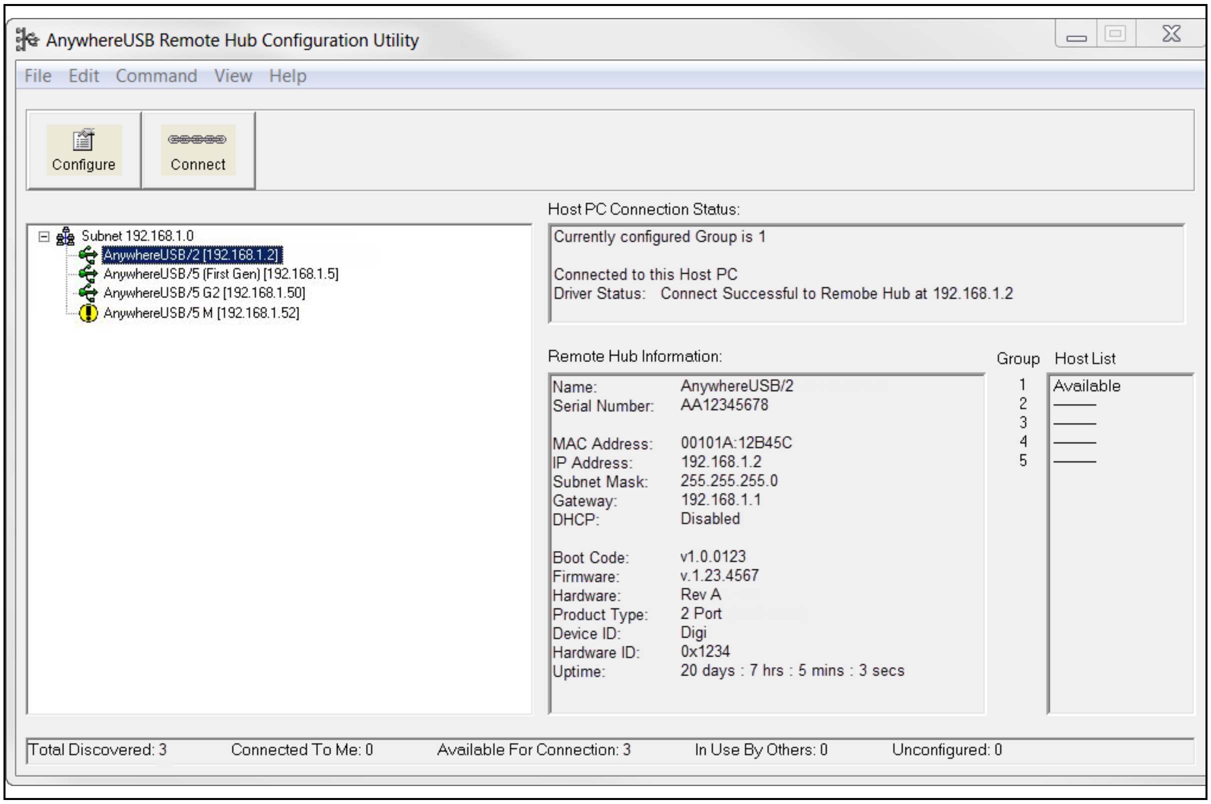
Note A basic user (a user without administrative privileges) is not allowed to start the AnywhereUSB Hub Configuration Utility. If an attempt to start the Utility is made by a basic user, an error occurs and the Utility will not work as expected. If a basic user must use the Utility, a user with administrative privileges must log in to the PC on which the Utility is installed, launch the Utility, and connect to the Hubs to which the basic user is allowed access. Once the basic user is allowed access to a Hub (or Hubs), that user is able to access and communicate with the USB devices that are attached to the Hub.

1. Log in to a Microsoft Windows computer with an account that has administrative privileges.
2. Select **Start > Programs > AnywhereUSB > AnywhereUSB Remote Hub Configuration Utility**.

   After the AnywhereUSB Remote Hub Configuration Utility has been started, it remains in the Windows system tray. You can open the utility from the system tray by double clicking its icon.

Remote Hub Configuration Utility window

The AnywhereUSB Remote Hub Configuration Utility displays AnywhereUSB devices grouped by their subnet addresses. The utility automatically discovers AnywhereUSB devices on the local subnet. To discover devices on other subnets, add those subnet addresses to the Discovery List. For more information, see Discover AnywhereUSB devices on other subnets.



```
Subnet 192.168.1.0
    AnywhereUSB/2 [192.168.1.2]
    AnywhereUSB/5 (First Gen) [192.168.1.5]
    AnywhereUSB/5 G2 [192.168.1.50]
    AnywhereUSB/5 M [192.168.1.52]

Host PC Connection Status:
Currently configured Group is 1

Connected to this Host PC
Driver Status:   Connect Successful to Remobe Hub at 192.168.1.2

Remote Hub Information:                                  Group   Host List
Name:            AnywhereUSB/2                             1     Available
Serial Number:   AA12345678                                2     ———
                                                           3     ———
MAC Address:     00101A:12B45C                             4     ———
IP Address:      192.168.1.2                               5     ———
Subnet Mask:     255.255.255.0
Gateway:         192.168.1.1
DHCP:            Disabled

Boot Code:       v1.0.0123
Firmware:        v.1.23.4567
Hardware:        Rev A
Product Type:    2 Port
Device ID:       Digi
Hardware ID:     0x1234
Uptime:          20 days : 7 hrs : 5 mins : 3 secs

Total Discovered: 3    Connected To Me: 0    Available For Connection: 3    In Use By Others: 0    Unconfigured: 0
```

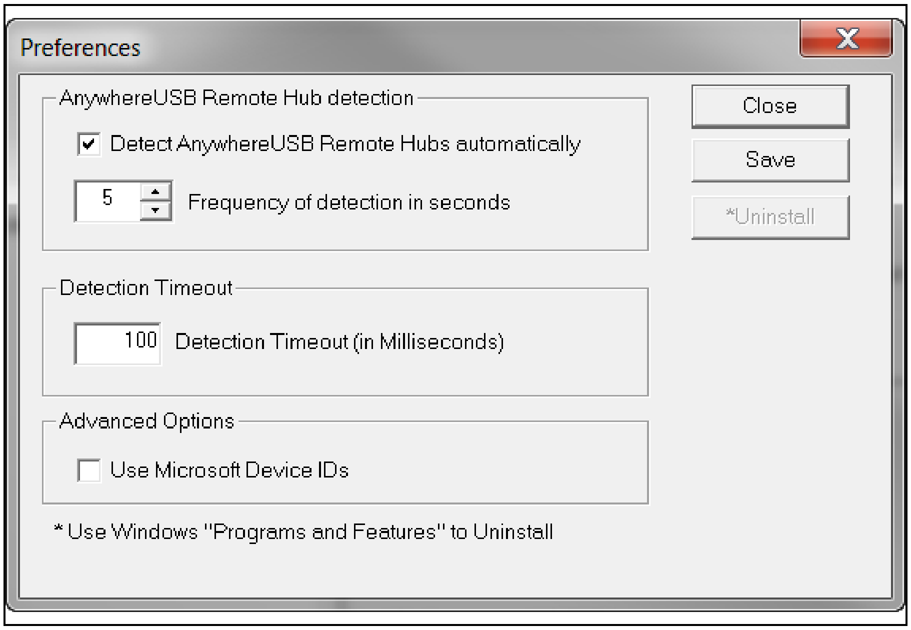
Icon Color Legend:

Icon	Description
🟩	Green: Available for connection.
⬜	Gray with bold text: Connected to this computer.
⬜	Gray: In use by another host computer.
🟥	(AnywhereUSB/5 first generation only) Red: Updating firmware.
❗	Warning: The IP address is not configured, or this is a multi-host connections-enabled device that is configured to connect to a non-existent Group.

Remote Hub Configuration Utility window menu options

This section explains the Remote Hub Configuration Utility window menu options.

File menu: Preferences



☑ Detect AnywhereUSB Remote Hubs automatically

5 Frequency of detection in seconds

100 Detection Timeout (in Milliseconds)

□ Use Microsoft Device IDs

* Use Windows "Programs and Features" to Uninstall

Detect AnywhereUSB Remote Hubs automatically and F**requency of detection in seconds**: Configure how often to query the network for AnywhereUSB devices.

Note AnywhereUSB devices are automatically detected when you open the AnywhereUSB Remote Hub Configuration Utility. Enabling this setting will make the AnywhereUSB Remote Hub Configuration Utility re-scan the network for newer AnywhereUSB devices at the configured frequency.

Detection Timeout: Configures how long the Remote Hub Configuration Utility will wait to hear from all the AnywhereUSB devices before the Remote Hub Configuration Utility updates the list of devices in the Main Window.

Use Microsoft Device IDs: Changes how the AnywhereUSB software creates the device ID for attached USB devices. A device ID consists of three parts: the name of the bus driver, the Product Identifier, and a unique serial number. For example, a Digi Edgeport USB to Serial converter that is plugged directly into the USB port of a computer would have a Device ID similar to (where **USB** indicates the Microsoft USB bus driver):

USB\VID_1608&PID_0215\A20299384

When attaching devices to an AnywhereUSB device, the bus driver name is **AWUSB**. Therefore the same device plugged into an AnywhereUSB device would have a Device ID of:

AWUSB\VID_1608&PID_0215\A20299384

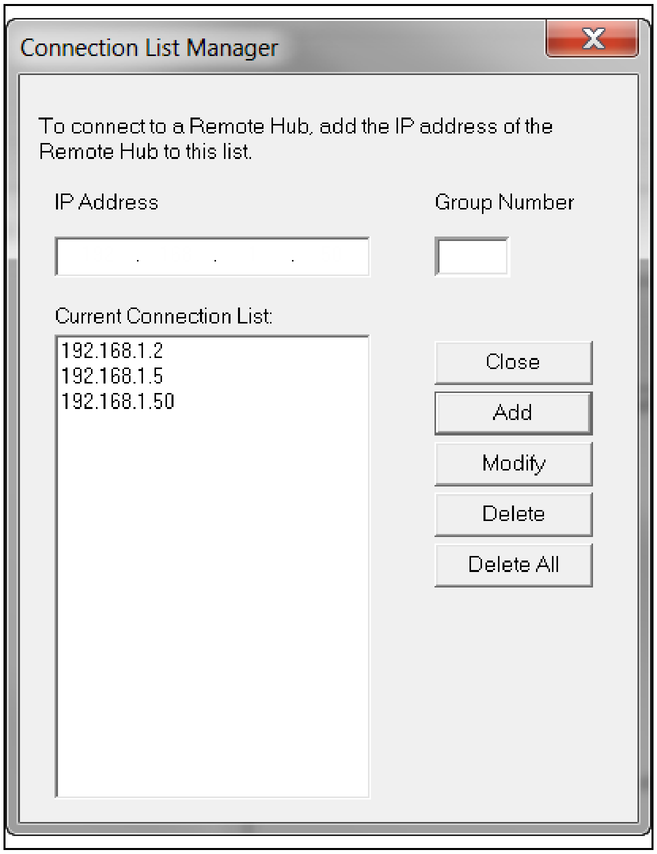
Some USB class drivers expect to see the bus driver name as “USB”, and as a result will not operate unless the **Use Microsoft Device IDs** checkbox is checked.

Edit menu: Connection List

The Connection List displays the IP addresses of the AnywhereUSB device to which the host computer will try to connect. When an IP address is added to this list, the host computer immediately tries to connect to the AnywhereUSB device. If an IP Address is deleted from the **Connection List**, the AnywhereUSB device will disconnect from the host computer and return to an “Available for Host Connection” state.

Select an AnywhereUSB and click **Connect** to add the selected AnywhereUSB IP address to the Connection List. We advise to connect using this method but you can also manually add the AnywhereUSB IP address to the Connection List. Use the manual method when the AnywhereUSB device has a known IP address but is not discoverable or when the AnywhereUSB is behind a router or firewall.

If an AnywhereUSB is behind a router or firewall, and you are using port forwarding, add the router's public-facing IP address to the Connection List. Port 3422 TCP (or port 3423 for encrypted connections) should be used for port forwarding.



Connection List Manager

To connect to a Remote Hub, add the IP address of the Remote Hub to this list.

IP Address

Group Number

Current Connection List:

192.168.1.2
192.168.1.5
192.168.1.50

Note Use Group 0 when you are manually adding an AnywhereUSB device that does not support multi-host connections.

Edit menu: Discovery List

The **Discovery List Manager** displays a list of subnet addresses of remote networks or IP addresses of individual devices where the Remote Hub Configuration Utility will search for AnywhereUSB devices.

For details, see Discover AnywhereUSB devices on other subnets.

Command menu: Configure

The options in the **Configure** dialog depend on the model of the selected AnywhereUSB device.

AnywhereUSB/5 (first generation)

The **Remote Hub** field at the top-left is the friendly name for the first generation AnywhereUSB/5 that appears on the left side of the AnywhereUSB Remote Hub Configuration Utility.

For the first generation AnywhereUSB/5, you can configure IP address settings in this window only.

AnywhereUSB/2 and AnywhereUSB/5 (G2) and AnywhereUSB TS 44

Use the Configure button to enable encryption for these AnywhereUSB models.

- For details about configuring AnywhereUSB IP settings, see Initial AnywhereUSB configuration.
- For details about AnywhereUSB encryption, see Configure AnywhereUSB encryption.
- For details about configuring the AnywhereUSB device name, see System settings.

AnywhereUSB/5 M and AnywhereUSB/14

For the multi-host capable AnywhereUSB models, use the Configure button to configure the Group Number that the host computer should connect to.

- For details about multi-host connections, see Multi-host connections.
- For details about configuring AnywhereUSB IP settings, see Initial AnywhereUSB configuration.
- For details about AnywhereUSB encryption, see Configure AnywhereUSB encryption.
- For details about configuring the AnywhereUSB device name, see System settings.

Command menu: Connect

Use the Connect command to add the IP address of the selected AnywhereUSB device to the Connection List.

Command menu: Web UI

The web UI command opens the web interface for the selected device.

Note The first generation AnywhereUSB/5 does not have a web UI.

When you open the web UI, you are required to log in.

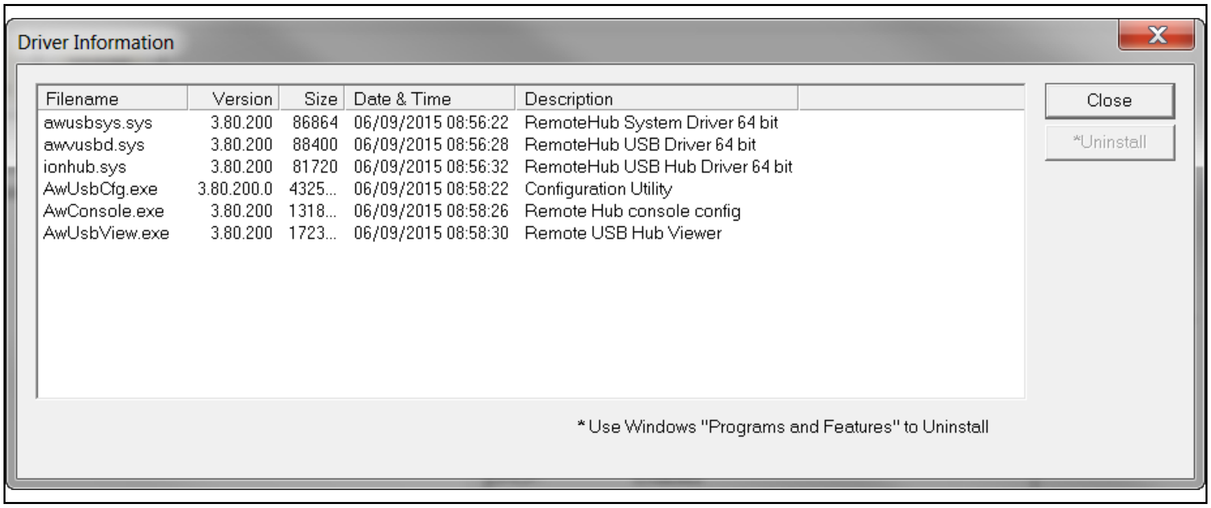
- **User name**: **root**
- **Password**: The unique, default password printed on the device label. If the default user name and password does not work, they may have been changed. Contact your system administrator for help.

Note If a password is not printed on the label, or the log in screen does not display, password authentication has not been enabled. See Security settings or contact your system administrator for help.

View menu: Driver Information

Use the Driver Information window to see AnywhereUSB driver version numbers and to uninstall older AnywhereUSB drivers. To uninstall current AnywhereUSB drivers, use Microsoft Windows Programs and Features.

- You must perform the uninstall as Windows Administrator.
- When the uninstall process is complete, reboot Windows once.



Filename	Version	Size	Date & Time	Description
awusbsys.sys	3.80.200	86864	06/09/2015 08:56:22	RemoteHub System Driver 64 bit
awvusbd.sys	3.80.200	88400	06/09/2015 08:56:28	RemoteHub USB Driver 64 bit
ionhub.sys	3.80.200	81720	06/09/2015 08:56:32	RemoteHub USB Hub Driver 64 bit
AwUsbCfg.exe	3.80.200.0	4325...	06/09/2015 08:58:22	Configuration Utility
AwConsole.exe	3.80.200	1318...	06/09/2015 08:58:26	Remote Hub console config
AwUsbView.exe	3.80.200	1723...	06/09/2015 08:58:30	Remote USB Hub Viewer

* Use Windows "Programs and Features" to Uninstall

View menu: Refresh (F5)

The **Refresh** command updates information for discovered AnywhereUSB devices listed in the utility’s main window.

Configure AnywhereUSB encryption

You can encrypt AnywhereUSB traffic by installing a digital certificate on the device. This is an optional setting that allows a host computer to confirm the AnywhereUSB device authenticity and to encrypt USB-over-IP traffic. This digital certificate must be signed by a Trusted Certificate Authority (CA). Since an AnywhereUSB is not publicly accessible, an enterprise CA can self-sign the digital certificate.

The installation process you use depends on whether you have one or two certificates.

One certificate: Follow this process to configure and enable encryption:

1. Create and validate the CA certificate
2. Install the CA certificate on the AnywhereUSB device
3. Enable the Encrypted AnywhereUSB network service
4. Install the CA certificate on the host computer

Two certificates: Follow this process to configure and enable encryption:

- Install two CA certificates

Create and validate the CA certificate

Use OpenSSL tools to generate a CA certificate and then use it to sign device certificates.

1. Download the OpenSSL command line app from openssl.org.
2. Create a CA certificate (cacert.crt) and its private 2048-bit RSA key (cakey.pem) and store cakey.pem in a safe place.

   ```
   openssl req -nodes -new -newkey rsa:2048 -x509 -extensions v3_ca -keyout cakey.pem -out
   cacert.crt -days 3650 -subj "[your email information]"
   ```

   Use the following email information string as an example:

   ```
   /C=US/ST=MN/L=Townname/O=Companyname/OU=Department/emailAddress=email@compan
   y.com/
   ```

   You will install cacert.crt on your host computer in a following step.
3. Generate a private 2048-bit RSA key for the server and store server.key in a safe place.

   ```
   openssl genrsa -out server.key 2048
   ```

4. Generate a Certificate Signing Request file server.csr. For example:

   ```
   openssl req -new -key server.key -out server.csr -subj "[your email information]"
   ```

   Example email information string:

```
/C=US/ST=MN/L=Townname/O=Companyname/OU=Department2/emailAddress=email@compa
ny.com/
```

Note The Organizational Unit (OU) in this step must be different than the OU used in step 2.

5. With server.csr, generate the actual certificate (server.crt).

```
openssl x509 -req -days 3650 -CA cacert.crt -CAkey cakey.pem -set_serial 001 -in server.csr -out
server.crt
```

6. Validate the certificates to each other. If this command is successful, the **server.crt: OK** message appears. If this command fails, an error message appears.

   The private CA key is not used in this step.

```
openssl verify -CAfile cacert.crt server.crt
```

7. After successfully completing certificate validation in the previous step, concatenate server.crt and server.key to create server.pem.

```
copy server.crt server.pem
```

```
type server.key >> server.pem
```

Install the CA certificate on the AnywhereUSB device

Upload the CA certificate to the AnywhereUSB device using the AnywhereUSB web UI:

1. Access and log in to the web user interface.
2. Select **Administration > X.509 Certificate/Key Management**.
3. Click **Secure Sockets Layer (SSL)/Transport Layer Security (TLS) Certificates**.
4. Click **Identity Certificates and Keys**.
5. Click **Choose File** and browse to the server.pem file.
6. Click **Upload**.

Enable the Encrypted AnywhereUSB network service

You must enable the encrypted AnywhereUSB network service:

1. Access and log in to the web user interface.
2. Select **Configuration > Network**.
3. Click **Network Services Settings**.
4. Select the **Enable Encrypted AnywhereUSB** check box.

Note Ensure the Encrypted AnywhereUSB service is running on port 3423. If a different port number is shown, contact Digi Technical Support for assistance.

5. Clear the **Enable AnywhereUSB** check box, if it is selected.

   Note **Enable AnywhereUSB** is selected (enabled) by default. Make sure to select (enable) only the **Enable Encrypted AnywhereUSB** option. If both of the AnywhereUSB network services are enabled, you risk having unencrypted connections on the device.

6. Click **Apply**.

Install the CA certificate on the host computer

Use the AnywhereUSB Remote Hub Configuration Utility to install the CA certificate on the host computer.

1. Open the AnywhereUSB Remote Hub Configuration Utility.
2. Select your AnywhereUSB device.
3. Click **Configure**.
4. Select the **Encrypt Connection** check box.

   Note Tunnel connections is automatically selected when you select Encrypt connection.

5. Browse to or type the path of the CA certificate (cacert.crt) in the Digital Certificate field.
6. Click **Update**.

Install two CA certificates

You can upload two CA certificates (Root CA and an Intermediate CA) to the host computer and the device.

The following requirements must be met:

- Both CAs are in DER format with a .cer file extension.
- OpenSSL must be installed.

To upload two CA certificates:

1. Convert both CAs from DER format to PEM format:

```
openssl x509 -inform der -in intermediate-ca.cer -out intermediate-ca.pem
```

```
openssl x509 -inform der -in root-ca.cer -out root-ca.pem
```

2. Combine the CAs into a single file that is in PEM format, with .crt file extension:

```
copy intermediate-ca.pem + root-ca.pem certchain.crt
```

3. On the host computer, launch the **AnywhereUSB Configuration Utility** interface.
   a. Select **AnywhereUSB**.
   b. Click **Configure**.
   c. In the **Digital Certificate** section, browse for: **certchain.crt**
   d. Click **Update**.

4. On the device, open the AnywhereUSB web interface.
    a. Select **Administration > X.509 Certificate/Key Management**.
    b. Click **Secure Sockets Layer (SSL)/Transport Layer Security (TLS) Certificates**.
    c. Click **Identity Certificates and Keys**.
5. Upload the end user certificate, which is the .pem file, signed by the Intermediate CA.
    a. If necessary, convert the CA from DER format to PEM format.
    b. Click **Choose File** and browse to the .pem file.
    c. **Click Upload**.
6. Upload the private key associated with the end user certificate.
    a. Click **Choose File** and browse to the private key file.
    b. Click **Upload**.

Specify a certificate folder for Encrypted AnywhereUSB connections

You can specify a certificate folder instead of a certificate file when setting up Encrypted AnywhereUSB connections. You can specify the folder from the AnywhereUSB Configuration Utility (AwUsbCfg.exe) or the console application (AwConsole.exe), following the same process you would use to specify a file.

Note To use this feature, you must have the v3.90.223 AnywhereUSB driver or higher installed.

To use a folder, each certificate must be renamed after the subject hash. For example, you have a folder named c:\my-certs that contains two certificates: CertA.crt and CertB.crt. You need to rename each certificate.

To rename a certificate:

1. Download an OpenSSL installer for Windows.

    Note You must download version 1.0 or newer, as pre-1.0 versions use an older hash which does not work with AnywhereUSB.

2. Open a command prompt from your certificate folder:

    ```
    c:\my-certs
    ```

3. Create a subject hash:

    ```
    c:\my-certs> openssl x509 -hash -in CertA.crt -noout
    ```

    The output is an 8-digit hash, such as bc35a2e5.

4. Rename (or copy) your certificate file with the hash as its base and the zero character as its extension:

    ```
    c:\my-certs> copy CertA.crt bc35a2e5.0
    ```

5. Repeat this process for any additional certifications.

Windows Certificate Store support

Users can import CA certificates to the Windows Certificate Store to authenticate server certificates. The CA certificate must be installed on the "Local Computer" in the Trusted Root Certification Authorities store. This requires the AnywhereUSB driver v3.95 or newer.

Troubleshoot AnywhereUSB encryption

See the following troubleshooting tips for issues with configuring AnywhereUSB encryption:

- Ensure the Encrypted AnywhereUSB service is enabled, and port 3423 is in use.
- If an Encrypted connection attempt fails, attempt to connect to the AnywhereUSB with **Tunneling** enabled and with **Encryption** disabled, within the Configuration area of the AnywhereUSB Configuration Utility.
  - If a Tunneled/Unencrypted connection works, the problem is likely to be related to the certificates.
  - If a Tunneled/Unencrypted connection fails, the problem is not likely to be related to the certificates, but instead related to the network; for example, port 3423 being blocked.
- Ensure that the Digi AnywhereUSB Network Service is running on the host computer. You can verify that the service has been started and is running in the Windows Services console (services.msc) or Windows System Configuration (msconfig) within the **Services** tab.
- The certificate for the CA that is used within the AnywhereUSB Configuration Utility must have a ".crt" file extension that must be in the PEM format. If the certificate for the CA instead has a ".cer" file extension (which is in the DER format), it must be converted from .cer to .crt using OpenSSL.

Discover AnywhereUSB devices on other subnets

This section explains how to enable the AnywhereUSB Remote Hub Configuration Utility to discover AnywhereUSB devices on additional IP subnets.

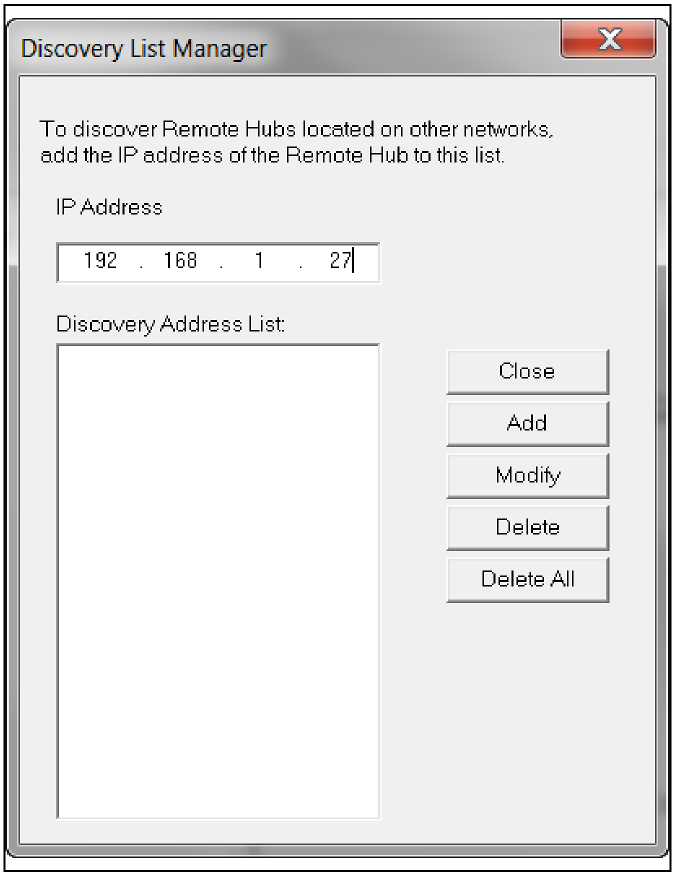
Add IP addresses to the Discovery List

By default, the AnywhereUSB Remote Hub Configuration Utility scans the local subnet for AnywhereUSB devices. To discover AnywhereUSB devices on other subnets, add their IP address or subnet to the Discovery List in the Discovery List Manager Dialog box.

1. Select **Edit > Discovery List.**
2. Type the subnet address or the IP address of the individual device in the IP Address field.

   For example, to add the Class C network 192.168.2.x, enter 192.168.2.255. For a Class B network 145.75.x.x, enter 145.75.255.255 (configure the router to forward subnet broadcasts).
3. Click **Add**.
4. Click **Close** to get back to the AnywhereUSB Remote Hub Configuration Utility main window.
5. Select **View > Refresh**. The device appears in the AnywhereUSB Remote Hub Configuration Utility device list.

Note If discovery fails, make sure that the Microsoft Windows firewall is off. For additional help, see No remote hubs found.



Discovery List Manager

To discover Remote Hubs located on other networks, add the IP address of the Remote Hub to this list.

IP Address

192 . 168 . 1 . 27

Discovery Address List:

Hardware specifications

This section provides the physical dimensions, environmental, and power requirements of the AnywhereUSB.

AnywhereUSB/2

Dimensions

Length: 2.38 in (6.04 cm)

Width: 3.9 in (10 cm)

Height: 1.0 in (2.54 cm)

Weight: 5 oz. (142 g)

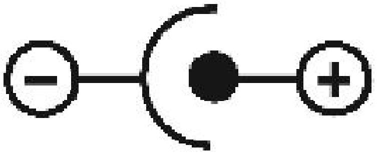
Environmental

Operating temperature: 32° F to 131° F (0° C to 55° C)

Relative humidity: 0% to 95% (non-condensing)

Power requirements

The AnywhereUSB uses a 120/230 VAC 50/60 Hz power adapter that supplies 5 V DC to the device. It is recommended that only the enclosed power supply be used with the AnywhereUSB. However, power is supplied to the AnywhereUSB by a UL-Listed Direct Plug-In Power device or Information Technology Equipment Rated Power device rated 5 V DC, at least 3.0 A, if used in the U.S. and Canada or a power supply with similar rating and approved by your local safety code if it is used elsewhere. For polarity, see the following diagram:



Hardware interface features

The device provides 2 USB ports (standard A-type receptacles). The downstream ports support Low, Full, and High Speed downstream devices.

Memory: 64 MB RAM

Network interface features

Standards: IEEE 802.3, 802.3i (10Base-T), 802.3u (100Base-TX), 802.3x (full duplex and flow control), HP Auto-MDIX (auto-detection of straight-through or crossover cabling)

Physical layer: 10/100 Mbps in half- or full-duplex mode, with auto-negotiation of speed and duplex

Ethernet connector: RJ-45

AnywhereUSB/5 (G2), AnywhereUSB/5 M

Dimensions

Length: 4.35 in (11.05 cm)

Width: 7.20 in (18.29 cm)

Height: 1.03 in (2.61 cm)

Weight: 10.00 oz. (283.5 g)

Environmental

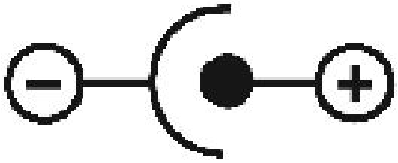
Operating temperature: 32° F to 131° F (0° C to 55° C)

Relative humidity: 0% to 95% (non-condensing)

Power requirements

The AnywhereUSB uses a 120/230 VAC 50/60 Hz power adapter that supplies 5 V DC to the device. It is recommended that only the enclosed power supply be used with the AnywhereUSB. However, power is supplied to the AnywhereUSB by a UL-Listed Direct Plug-In Power device or Information Technology Equipment Rated Power device rated 5 V DC, at least 3.0 A, if used in the U.S. and Canada or a power supply with similar rating and approved by your local safety code if it is used elsewhere.

For polarity, see the following diagram:



Note The power supplies between the AWUSB/5 first and second generation (G2) models are not interchangeable. Use the power supply provided with the device.

Hardware interface features

The device provides 5 USB ports (standard A-type receptacles). The downstream ports support Low, Full, and High Speed downstream devices.

Memory: 128MB RAM

Network interface features

Standards: IEEE 802.3, 802.3i (10Base-T), 802.3u (100Base-TX), 802.3x (full duplex and flow control), HP Auto-MDIX (auto-detection of straight-through or crossover cabling)

Physical layer: 10/100 Mbps in half- or full-duplex mode, with auto-negotiation of speed and duplex

Ethernet connector: RJ-45

AnywhereUSB/5 (first generation)

Dimensions

Length: 4.35 in (11.05 cm)

Width: 7.20 in (18.29 cm)

Height: 1.03 in (2.61 cm)

Weight: 10.00 oz. (283.5 g)

Environmental

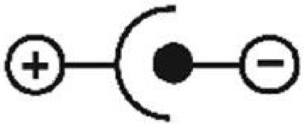
Operating temperature: 32° F to 131° F (0° C to 55° C)

Relative humidity: 0% to 95% (non-condensing)

Power requirements

Power to this product many be supplied by a UL Listed Direct Plug-In Power device marked “Class 2" or a UL listed power supply rated with a minimum rating of 5 V DC 2.5 A if used in the U.S. and Canada or a power supply with similar rating and approved by your local safety code if it is used elsewhere.

For polarity, see the following diagram:



Note The power supplies between the AWUSB/5 first and second generation (G2) models are not interchangeable. Use the power supply provided with the device.

AnywhereUSB TS44

Dimensions

Length: 4.35 in (11.05 cm)

Width: 7.20 in (18.29 cm)

Height: 1.03 in (2.61 cm)

Weight: 10.00 oz. (283.5 g)

Environmental

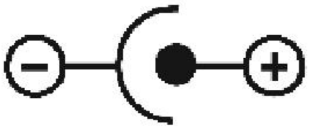
Operating temperature: 32° F to 131° F (0° C to 55° C)

Relative humidity: 0% to 95% (non-condensing)

Power requirements

The AnywhereUSB uses a 120/230 VAC 50/60 Hz power adapter that supplies 5 V DC to the device. It is recommended that only the enclosed power supply be used with the AnywhereUSB. However, power is supplied to the AnywhereUSB by a UL-Listed Direct Plug-In Power device or Information Technology Equipment Rated Power device rated 5 V DC, at least 3.0 A, if used in the U.S. and Canada or a power supply with similar rating and approved by your local safety code if it is used elsewhere.

For polarity, see the following diagram:



Hardware interface features

The device provides 4 USB ports (standard A-type receptacles) and 4 serial ports. The downstream ports support Low, Full, and High Speed downstream devices.

Memory: 128MB RAM

Serial interface features

- 10-pin serial ports
- EIA-232 interface
- Throughput up to 230,400 bps
- 5, 6, 7, 8 data bits
- 1, 1.5, 2 stop bits
- Mark/space/even/odd parity
- Hardware and Software Flow Control

Serial port pinouts

Pin Number	Signal
Pin 1	RI
Pin 2	DSR
Pin 3	RTS
Pin 4	Ground
Pin 5	TxD
Pin 6	RxD

Pin Number	Signal
Pin 7	Signal Ground
Pin 8	CTS
Pin 9	DTR
Pin 10	DCD

Network interface features

- Standards: IEEE 802.3, 802.3i (10Base-T), 802.3u (100Base-TX), 802.3x (full duplex and flow control)
- Physical layer: 10/100 Mbps in half- or full-duplex mode, with auto-negotiation of speed and duplex
- Ethernet connector: RJ-45AnywhereUSB TS44

AnywhereUSB/14

Dimensions

Length: 4.97 in (12.62 cm)

Width: 17.00 in (43.18 cm)

Height: 1.74 in (4.42 cm)

Weight: 40.00 oz. (1134 g)

Environmental

Operating temperature: 32° F to 131° F (0° C to 55° C)

Relative humidity: 0% to 95% (non-condensing)

Power requirements

The AnywhereUSB/14 uses single or dual 120/230 VAC 50/60 Hz power input(s) through the rear IEC 60320 inlet(s). Redundant (dual) supply enables it to support mission critical applications where uninterrupted powering is a must. In case of redundant (dual) powering, both supplies provide power to the device. When one of the supplies fails the other will provide the complete power to the device. In case of single powering, use the left side inlet (rear view). The maximum power requirement of the AnywhereUSB/14 is 45 W.

Hardware interface features

The device provides 14 USB ports (standard A-type receptacles). The downstream ports support Low Speed, Full Speed, and High Speed downstream devices.

The device supports two Ethernet connectors (dual RJ-45) LAN1 & LAN2 for mission critical applications (redundant Ethernet). The device can switch from LAN1 to LAN2 and vice-versa if any of them fails. The primary input is LAN1.

The device also provides an RS232 UART Management port via a DB9 connector at the rear next to the network connectors.

Network interface features

Standards: IEEE 802.3, 802.3i (10Base-T), 802.3u (100Base-TX), 802.3x (full duplex and flow control), HP Auto-MDIX (auto-detection of straight-through or crossover cabling)

Physical layer: 10/100 Mbps in half- or full-duplex mode, with auto-negotiation of speed and duplex

Multi-host connections

This section describes the multi-host connections feature exclusively available on the AnywhereUSB/14 and AnywhereUSB/5 M models. The multi-host connections feature allows multiple host computers to establish concurrent connections with the AnywhereUSB device. Each host computer requests a different group of USB ports, where the group assignments have been previously configured on the AnywhereUSB device.

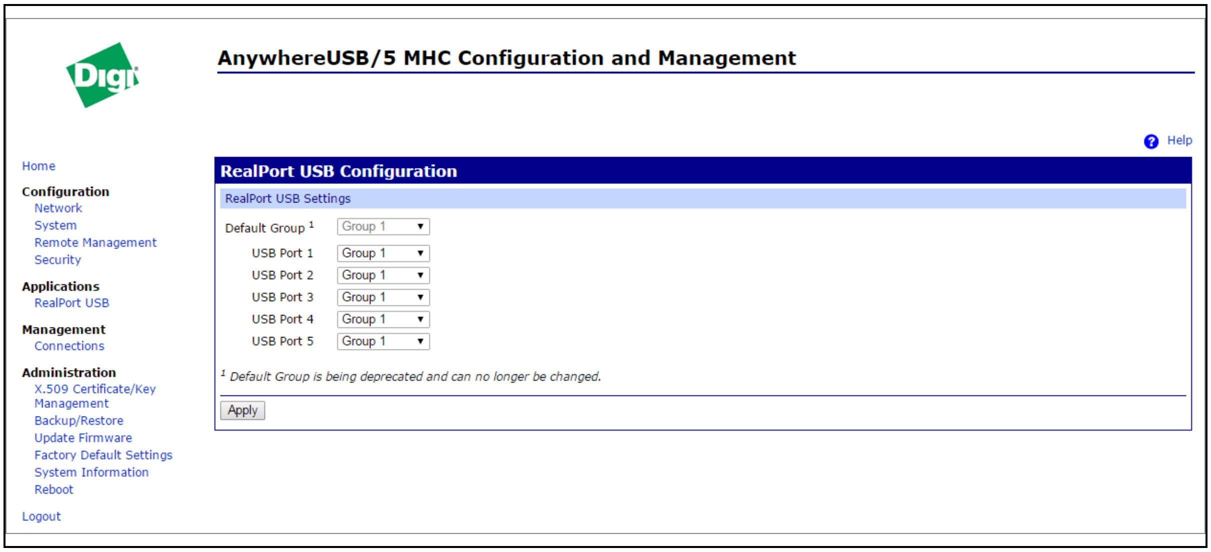
Requirement: Older AnywhereUSB driver and firmware versions may not support multi-host connections.

Configure groups

This procedure explains how to assign the AnywhereUSB device's physical USB port to groups.

After a group has been assigned, you can change group assignments without restarting the device. For details, see Dynamic group assignment.

1. Access and log in to the web user interface.
2. Select **RealPort USB**.



AnywhereUSB/5 MHC Configuration and Management

RealPort USB Configuration

RealPort USB Settings

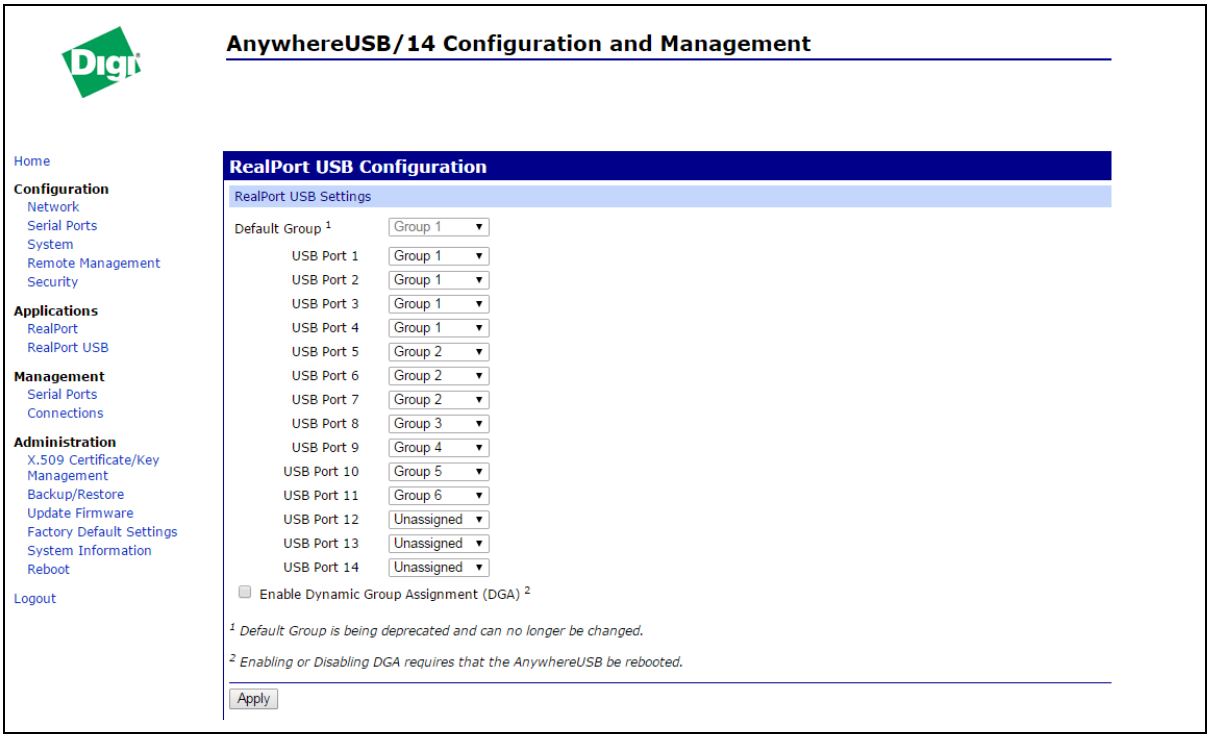
Default Group [1]	Group 1
USB Port 1	Group 1
USB Port 2	Group 1
USB Port 3	Group 1
USB Port 4	Group 1
USB Port 5	Group 1

[1] *Default Group is being deprecated and can no longer be changed.*

2. Click **Apply** and reboot the AnywhereUSB for group configuration changes to take effect.

   The options on this page allows the user to select which physical USB ports on the AnywhereUSB device are assigned to which group. By default, all the USB Ports are assigned to Group 1. Therefore, a host computer requesting Group 1 takes ownership of all of the physical USB ports on the AnywhereUSB device.

   In the AnywhereUSB/14 configuration example below, a host computer requesting Group 1 is granted access only to physical USB ports 1 through 4. A host computer requesting Group 2 is granted access to physical USB ports 5 through 7. A host computer requesting Group 6 is given access to physical USB port 11, and so on. The USB ports 12 through 14 are unassigned, and as a result do not support any attached USB devices.



RealPort USB Configuration

RealPort USB Settings

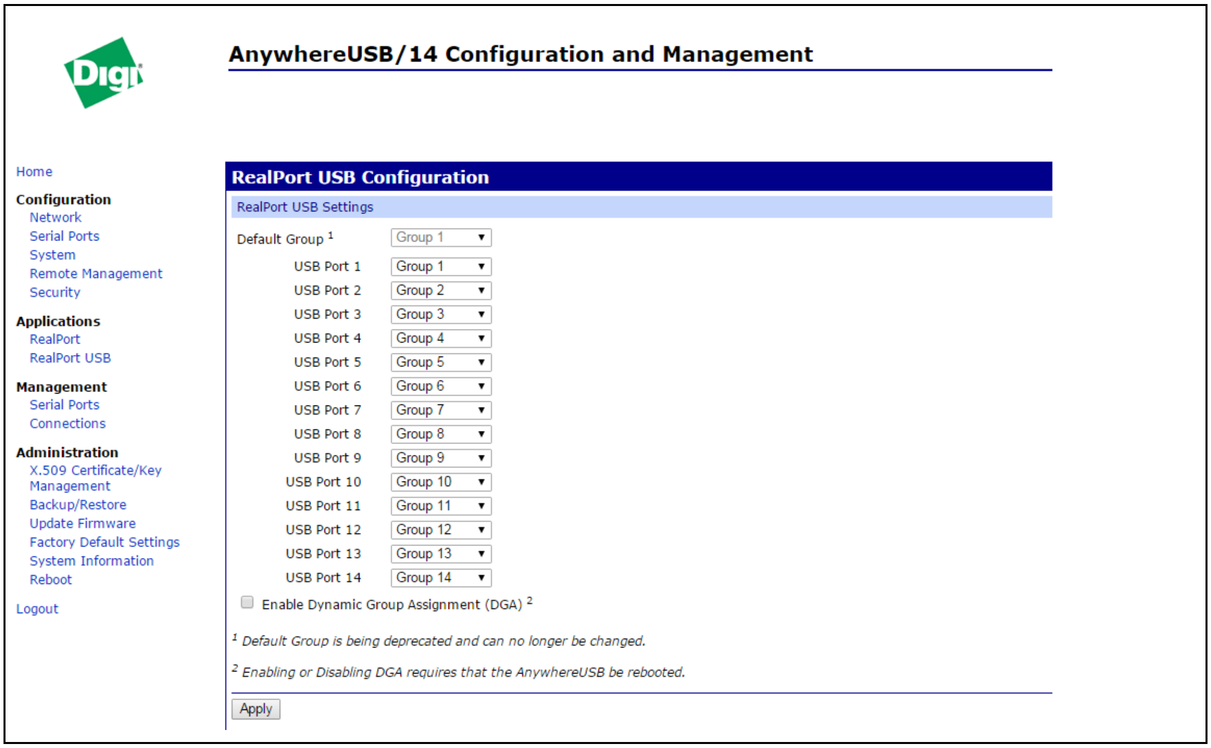
Default Group [1]	Group 1
USB Port 1	Group 1
USB Port 2	Group 1
USB Port 3	Group 1
USB Port 4	Group 1
USB Port 5	Group 2
USB Port 6	Group 2
USB Port 7	Group 2
USB Port 8	Group 3
USB Port 9	Group 4
USB Port 10	Group 5
USB Port 11	Group 6
USB Port 12	Unassigned
USB Port 13	Unassigned
USB Port 14	Unassigned

□ Enable Dynamic Group Assignment (DGA) [2]

[1] *Default Group is being deprecated and can no longer be changed.*

[2] *Enabling or Disabling DGA requires that the AnywhereUSB be rebooted.*

In the example below, the AnywhereUSB/14 device has been configured to have 14 groups, each providing access to a single physical USB port.



RealPort USB Configuration

RealPort USB Settings

Default Group [1]	Group 1
USB Port 1	Group 1
USB Port 2	Group 2
USB Port 3	Group 3
USB Port 4	Group 4
USB Port 5	Group 5
USB Port 6	Group 6
USB Port 7	Group 7
USB Port 8	Group 8
USB Port 9	Group 9
USB Port 10	Group 10
USB Port 11	Group 11
USB Port 12	Group 12
USB Port 13	Group 13
USB Port 14	Group 14

□ Enable Dynamic Group Assignment (DGA) [2]

[1] *Default Group is being deprecated and can no longer be changed.*

[2] *Enabling or Disabling DGA requires that the AnywhereUSB be rebooted.*

After a group has been assigned, you can change group assignments without restarting the device. For details, see Dynamic group assignment.

Dynamic group assignment

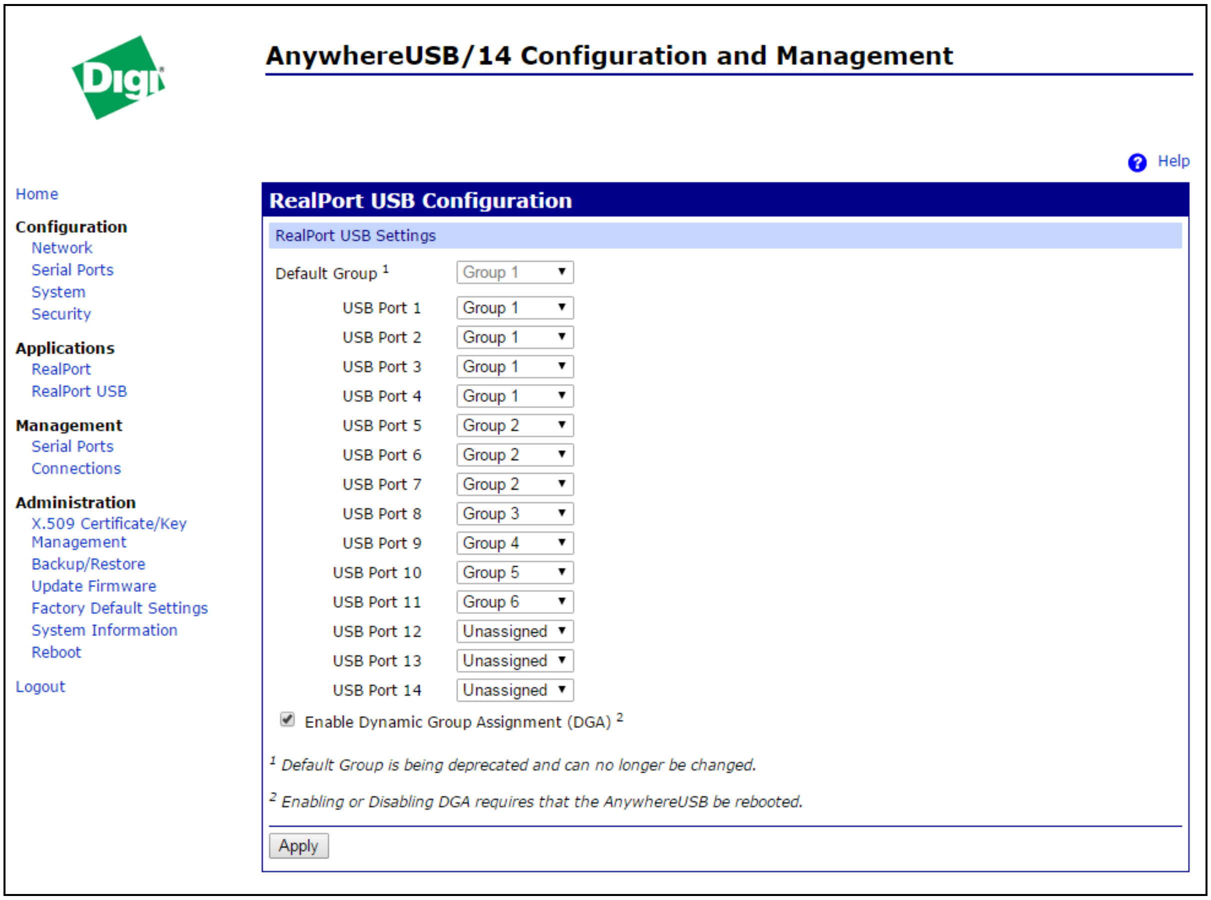
The AnywhereUSB/14 device allows you to change group assignments without restarting the device using Dynamic Group Assignment (DGA). Making group changes using DGA does not disrupt unaffected USB ports. For example, if you enable DGA and make changes to USB ports 1, 2 and 3, then USB ports 4-14 remain connected without any interruption.

To enable DGA and make group changes:

1. Select the **Enable Dynamic Group Assignment (DGA)** check box.
2. Click **Apply** and restart the device.

   Note Enabling or disabling DGA requires you to restart the device.

3. Access and log in to the web user interface.
4. Xlick **RealPort USB**.
5. Change groups for USB ports as needed.
6. Click **Apply**. Group changes take effect immediately.



RealPort USB Configuration

RealPort USB Settings

Default Group [1]	Group 1
USB Port 1	Group 1
USB Port 2	Group 1
USB Port 3	Group 1
USB Port 4	Group 1
USB Port 5	Group 2
USB Port 6	Group 2
USB Port 7	Group 2
USB Port 8	Group 3
USB Port 9	Group 4
USB Port 10	Group 5
USB Port 11	Group 6
USB Port 12	Unassigned
USB Port 13	Unassigned
USB Port 14	Unassigned

☑ Enable Dynamic Group Assignment (DGA) [2]

[1] *Default Group is being deprecated and can no longer be changed.*

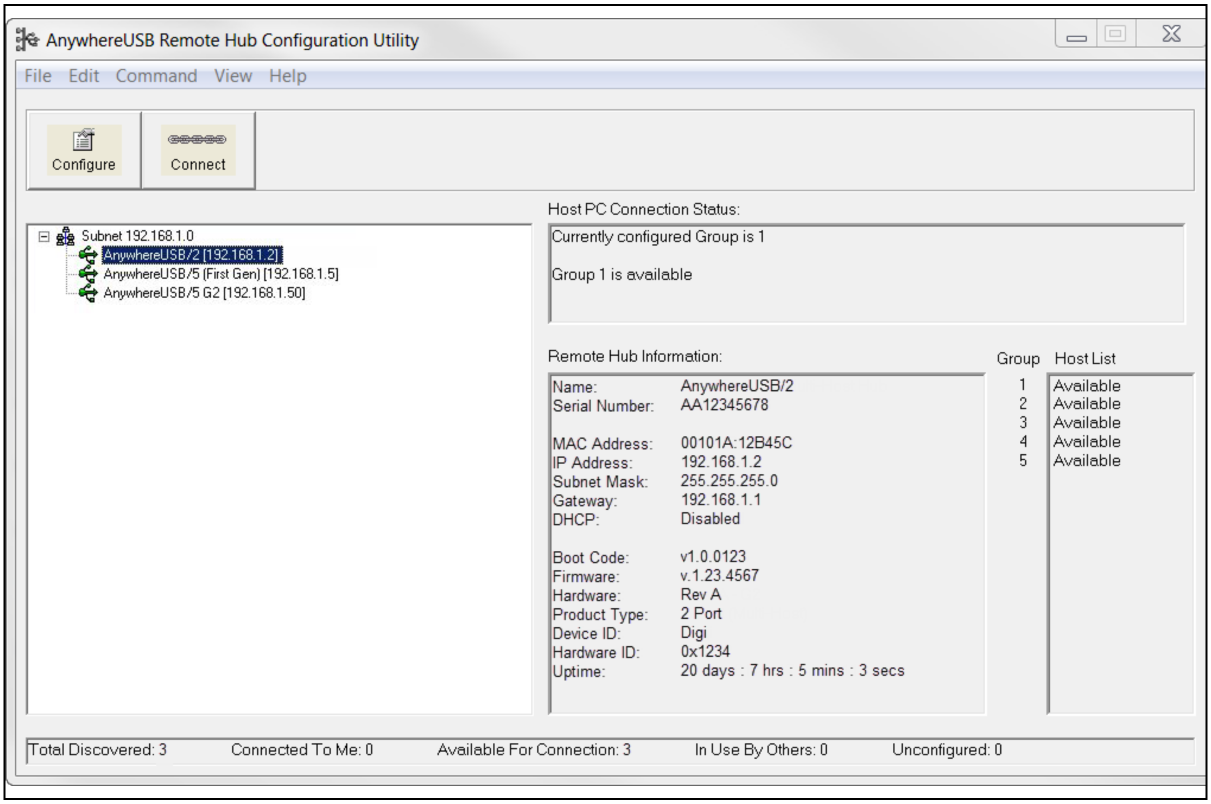
[2] *Enabling or Disabling DGA requires that the AnywhereUSB be rebooted.*

Host computer configuration

In the AnywhereUSB Remote Hub Configuration Utility, you must specify the group number that each host computer should connect to. Each host computer may only connect to one group. When the host computer connects to the AnywhereUSB, it takes ownership of the associated USB ports.

The following example shows an AnywhereUSB/5 M device that has five groups configured, each group provides access to a single physical USB port on the AnywhereUSB device.

In the Host List column is on the right, “available” indicates that the Group is associated with one or more USB ports and there are no host computers currently connected to that Group.


AnywhereUSB Remote Hub Configuration Utility
File Edit Command View Help
Configure
Connect

Subnet 192.168.1.0
AnywhereUSB/2 [192.168.1.2]
AnywhereUSB/5 (First Gen) [192.168.1.5]
AnywhereUSB/5 G2 [192.168.1.50]

Host PC Connection Status:

Currently configured Group is 1

Group 1 is available

Remote Hub Information:

Name:	AnywhereUSB/2
Serial Number:	AA12345678
MAC Address:	00101A:12B45C
IP Address:	192.168.1.2
Subnet Mask:	255.255.255.0
Gateway:	192.168.1.1
DHCP:	Disabled
Boot Code:	v1.0.0123
Firmware:	v.1.23.4567
Hardware:	Rev A
Product Type:	2 Port
Device ID:	Digi
Hardware ID:	0x1234
Uptime:	20 days : 7 hrs : 5 mins : 3 secs

Group	Host List
1	Available
2	Available
3	Available
4	Available
5	Available

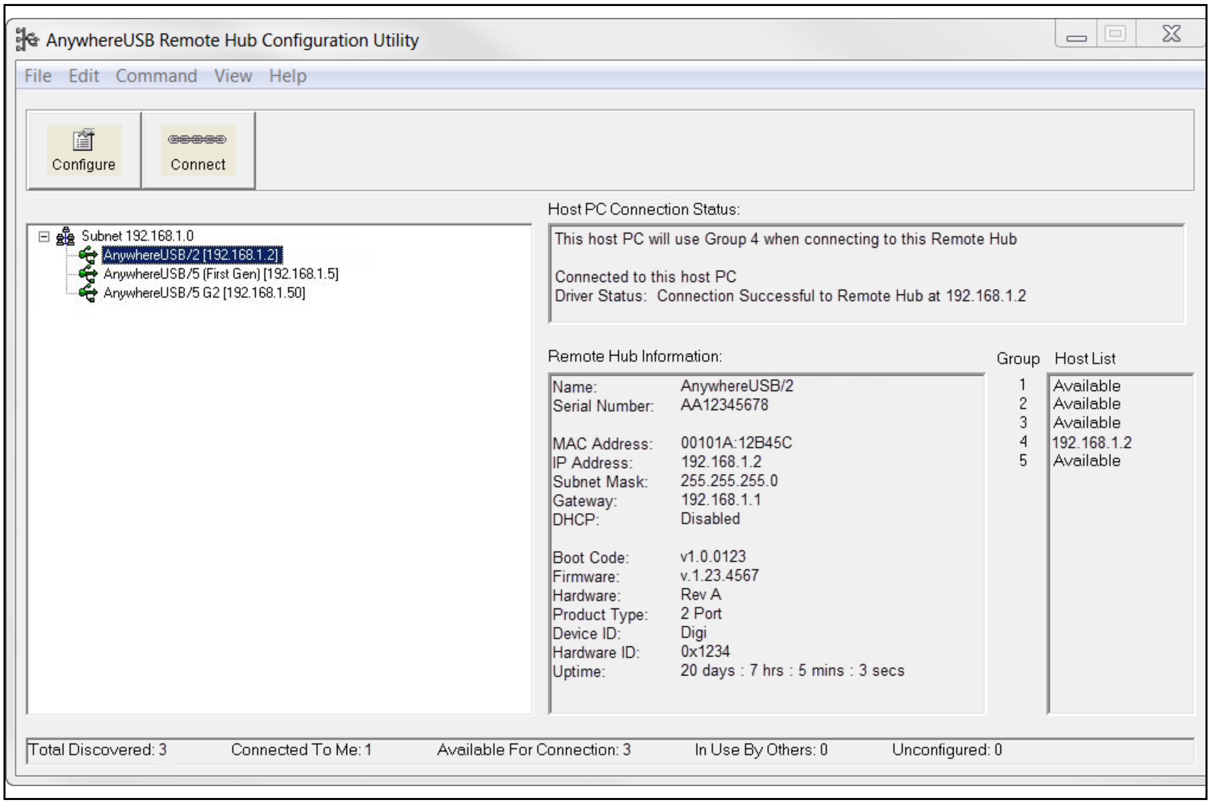
Total Discovered: 3 Connected To Me: 0 Available For Connection: 3 In Use By Others: 0 Unconfigured: 0

To connect an AnywhereUSB device to the host computer:

1. Log in to a Microsoft Windows computer with an account that has administrative privileges.
2. Select **Start > Programs > AnywhereUSB > AnywhereUSB Remote Hub Configuration Utility**.
3. Select your device from the list and click Connect or right-click and click **Connect**.

   For example, the following image shows a host computer that connects to Group 4 on the AnywhereUSB device. Clicking **Connect** initiates the connection process between the host computer and the selected AnywhereUSB/5 M device.

   After the connection process completes, the AnywhereUSB Remote Hub Configuration Utility updates its Connection Status information.


AnywhereUSB Remote Hub Configuration Utility
File Edit Command View Help
Configure
Connect
Subnet 192.168.1.0
AnywhereUSB/2 [192.168.1.2]
AnywhereUSB/5 (First Gen) [192.168.1.5]
AnywhereUSB/5 G2 [192.168.1.50]

Host PC Connection Status:

This host PC will use Group 4 when connecting to this Remote Hub

Connected to this host PC
Driver Status: Connection Successful to Remote Hub at 192.168.1.2

Remote Hub Information:

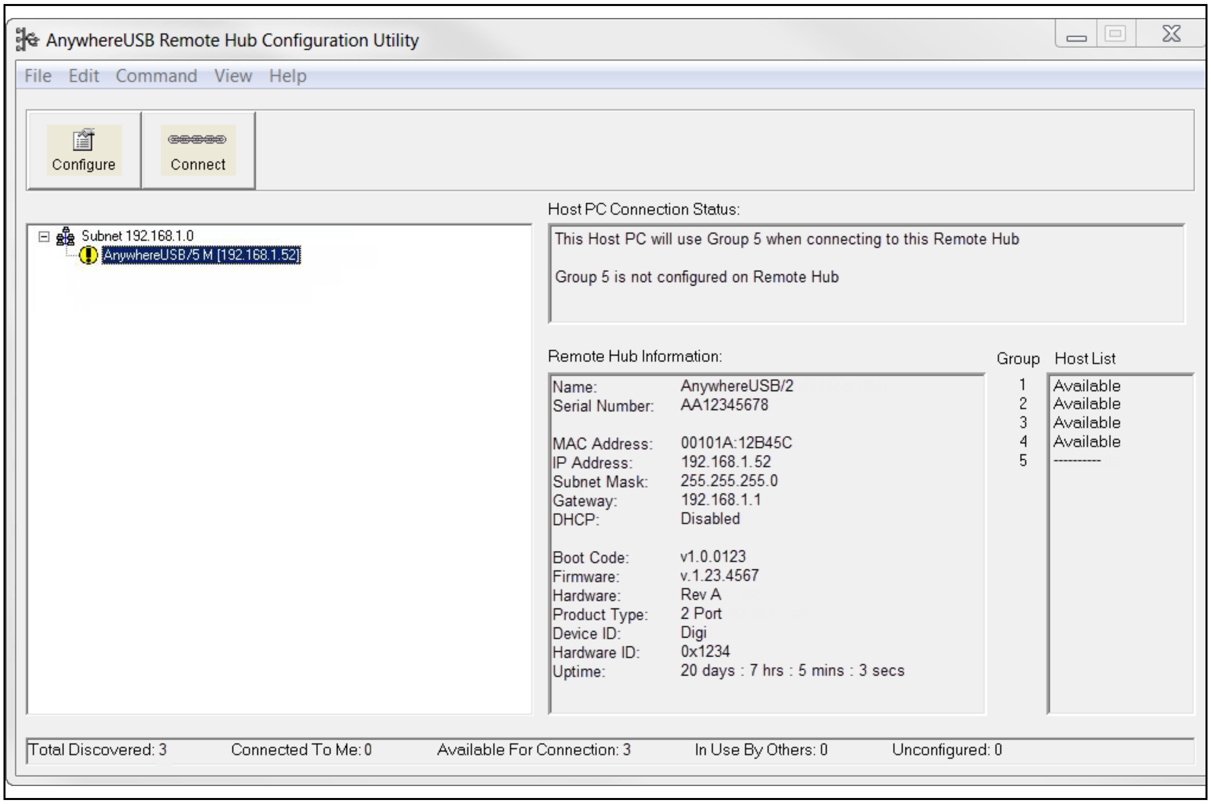
Name:	AnywhereUSB/2
Serial Number:	AA12345678
MAC Address:	00101A:12B45C
IP Address:	192.168.1.2
Subnet Mask:	255.255.255.0
Gateway:	192.168.1.1
DHCP:	Disabled
Boot Code:	v1.0.0123
Firmware:	v.1.23.4567
Hardware:	Rev A
Product Type:	2 Port
Device ID:	Digi
Hardware ID:	0x1234
Uptime:	20 days : 7 hrs : 5 mins : 3 secs

Group	Host List
1	Available
2	Available
3	Available
4	192.168.1.2
5	Available

Total Discovered: 3 Connected To Me: 1 Available For Connection: 3 In Use By Others: 0 Unconfigured: 0

Note The Host PC Connection Status now says “Connected to this Host PC,” and the host computer's IP address is listed in the Host List column for Group 4.

In the event the host computer requests a group that is not configured on the AnywhereUSB device, the Host PC Connection Status displays something similar to the following image indicating that the selected Group is not configured on the given AnywhereUSB device.


AnywhereUSB Remote Hub Configuration Utility
File
Edit
Command
View
Help
Configure
Connect
Subnet 192.168.1.0
AnywhereUSB/5 M [192.168.1.52]

Host PC Connection Status:

This Host PC will use Group 5 when connecting to this Remote Hub

Group 5 is not configured on Remote Hub

Remote Hub Information:

Name: AnywhereUSB/2
Serial Number: AA12345678

MAC Address: 00101A:12B45C
IP Address: 192.168.1.52
Subnet Mask: 255.255.255.0
Gateway: 192.168.1.1
DHCP: Disabled

Boot Code: v1.0.0123
Firmware: v.1.23.4567
Hardware: Rev A
Product Type: 2 Port
Device ID: Digi
Hardware ID: 0x1234
Uptime: 20 days : 7 hrs : 5 mins : 3 secs

Group	Host List
1	Available
2	Available
3	Available
4	Available
5	----------

Total Discovered: 3 Connected To Me: 0 Available For Connection: 3 In Use By Others: 0 Unconfigured: 0

In the above example, the Host List column on the far right indicates that groups 1 through 4 are associated with one or more USB ports, and there are no host computers currently connected with one or more of these groups. Group 5 is not associated with any USB port, therefore it is not possible for a host computer to connect to it. When a host computer is configured to connect to a group that is not associated with any USB ports on an AnywhereUSB device, a yellow warning symbol appears next to the AnywhereUSB device in the Remote Hub Configuration Utility and a message appears in the Host PC Connection Status area.

Configure from the web interface

This section describes the configuration options in the web UI Configuration, Management, and Administration sections and their sub-menus. With the exception of the title of the specific Configuration and Management screens, menus and sub-menus for both models remain the same.

Note This feature is not available on the first generation AWUSB/5 model.

Configuration and Management home page

The home page appears when the web UI is opened.

The left side of the home page has a list of choices that display pages for configuration, applications, management, and administration tasks, and to log out of the web UI.

Access and log in to the web user interface

You can access the web user interface from the AnywhereUSB Remote Hub Configuration Utility.

1. Log in to a Microsoft Windows computer with an account that has administrative privileges.
2. Select **Start** > **Programs** > **AnywhereUSB** > **AnywhereUSB Remote Hub Configuration Utility**.
3. Select **Command** > **Configure**. A log in screen displays.
   - **User name**: **root**
   - **Password**: The unique, default password printed on the device label. If the default user name and password does not work, they may have been changed. Contact your system administrator for help.

Note If a password is not printed on the label, or the log in screen does not display, password authentication has not been enabled. See Security settings or contact your system administrator for help.

Apply and save changes

The web UI runs locally on the device, which means that the interface always maintains and displays the latest settings for the connected AnywhereUSB device.

Cancel changes

To cancel changes to configuration settings, click **Refresh** or **Reload** in the web UI. This causes the browser to reload the page. Any changes made since the last time the **Apply** button was clicked are reset to their original values.

Log out

Click **Logout** to disconnect the configuration and management session with an AnywhereUSB. It does not close the browser window, but displays a logout window.

To finish logging out of the web UI and prevent access by other users, close the browser window. Or, log back on to the device by clicking the link on the screen. After 5 minutes of inactivity, the idle timeout also automatically performs a user logout.

Restore the AnywhereUSB to factory defaults

You can reset the device configuration to factory defaults as needed during the configuration process.

For details, refer to Factory default settings.

Online help

Online help is available for all screens of the web UI, and for common configuration and administration tasks. There is also a tutorial available on the **Home** page.

The Get Started section has a link to a tutorial on configuring and managing the AnywhereUSB.

The System Summary section notes all available device-description information.

Web UI Configuration

The configuration section of the web UI consists of sub-menus that are specific to the particular model of the AnywhereUSB device being configured. These configuration options may include: Network, Serial Ports (AnywhereUSB/14 and AnywhereUSB TS44 only), System, Remote Management, and Security.

Network settings

The **Ethernet IP Settings** page shows IP address settings for the: DHCP or static IP address, subnet mask, default gateway. You can view or change the IP settings on this page.

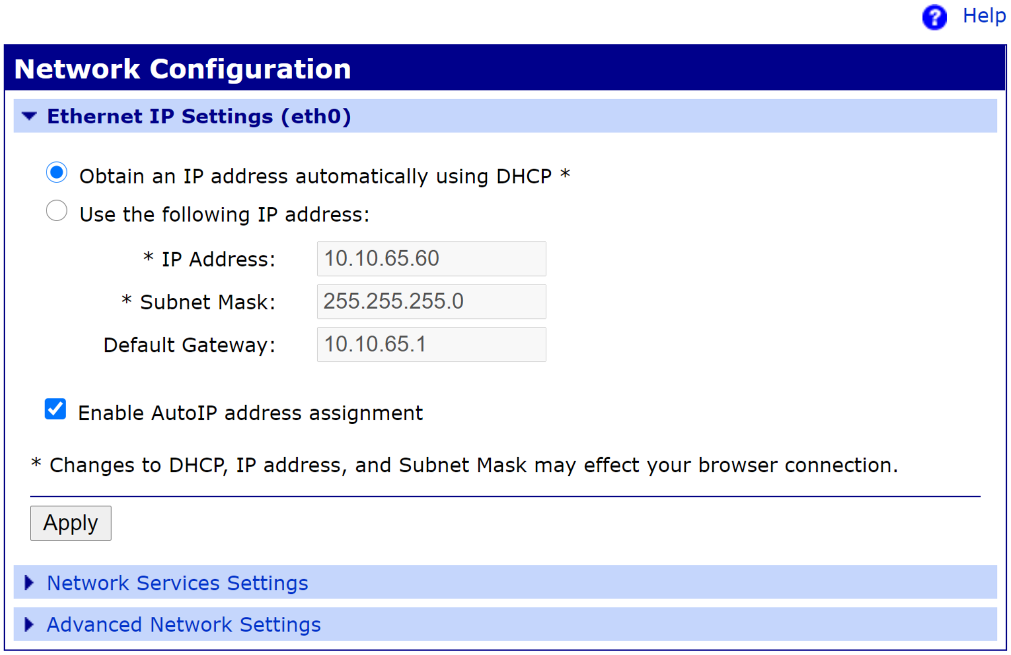
Contact your network administrator for more information about these settings.

To access this page:

1. Access and log in to the web user interface.
2. Select **Configuration** > **Network**.
3. Make your desired changes.
   - Ethernet IP Settings page
   - Network Services page
   - Advanced Network Settings page
4. Click **Apply** to save the changes.

Ethernet IP Settings page

The **Ethernet IP Settings** page enables you to obtain an IP address using DCHP, specify a static IP address, or enable the auto IP address assignment feature.



Network Configuration

▼ Ethernet IP Settings (eth0)

● Obtain an IP address automatically using DHCP *

○ Use the following IP address:

* IP Address:	10.10.65.60
* Subnet Mask:	255.255.255.0
Default Gateway:	10.10.65.1

☑ Enable AutoIP address assignment

* Changes to DHCP, IP address, and Subnet Mask may effect your browser connection.

Obtain an IP address automatically using DHCP

Choose this option to automatically get an IP address for the device. When the Digi device server is rebooted, it will obtain new network settings.

Contact your network administrator to find out if a DHCP server is available.

Use the following IP address

Choose this option to define a static IP address.

- **IP Address:** Enter the IP address for the device. An entry is required.
- **Subnet Mask**: The Subnet Mask is combined with the IP address to determine which network this Digi device server is part of. An entry is required.
- **Default Gateway:** The IP address of the computer that enables this Digi device server to access other networks, such as the Internet.

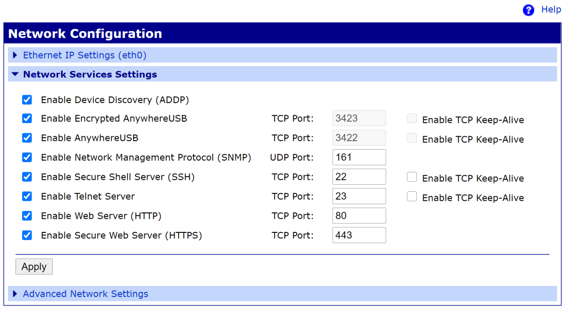
Enable AutoIP address assignment

With AutoIP enabled, the Digi device server automatically self-configures an IP address when an address isn't available from other methods, for example, when the Digi device server is configured for DHCP and a DHCP server isn't currently available.

Network Services page

In the **Network Services** page, you can enable or disable the network services and configure the TCP port for the service.

Several services have a setting for whether TCP keep-alives are sent for the network services. To configure TCP keep-alives, see the Advanced Network Settings page.



Network Configuration

▸ Ethernet IP Settings (eth0)

▾ Network Services Settings

☑	Enable Device Discovery (ADDP)			
☑	Enable Encrypted AnywhereUSB	TCP Port:	3423	□ Enable TCP Keep-Alive
☑	Enable AnywhereUSB	TCP Port:	3422	□ Enable TCP Keep-Alive
☑	Enable Network Management Protocol (SNMP)	UDP Port:	161	
☑	Enable Secure Shell Server (SSH)	TCP Port:	22	□ Enable TCP Keep-Alive
☑	Enable Telnet Server	TCP Port:	23	□ Enable TCP Keep-Alive
☑	Enable Web Server (HTTP)	TCP Port:	80	
☑	Enable Secure Web Server (HTTPS)	TCP Port:	443	

▸ Advanced Network Settings

Enable or disable the following network services

For each network service, the **TCP Port** or **UDP Port** field shows the port on which the service is running.

- **Device Discovery (ADDP)**: This service controls use of Advanced Device Discovery Protocol. If it is disabled, you can no longer use Digi Device Discovery utility to locate the device.
- **AnywhereUSB and Encrypted AnywhereUSB**: These services enable or disable the ability for a host computer to connect with your AnywhereUSB device. You must enable only one of these options. Disabling both of these options disconnects your AnywhereUSB device from the host computer. Use these options as follows:
  - **AnywhereUSB**: Enable this to allow host computer connections to your AnywhereUSB device without encrypting network traffic.
  - **Encrypted AnywhereUSB**: Enable this option to allow host computer connections to your AnywhereUSB device and to encrypt network traffic.

Note The TCP Port numbers for AnywhereUSB and Encrypted AnywhereUSB are static and cannot be changed.

- **Network Management Protocol (SNMP)**: Enables or disables the use of SNMP. If disabled, SNMP services such as traps and device information are not used.
- **Secure Shell Server (SSH)**: Enables or disables the SSH server service. If disabled, users cannot make a Secure Shell connection to the device.
- **Telnet Server**: Enables or disables the telnet service. If disabled, users cannot telnet to the device.
- **RealPort or Encrypted RealPort**: (AnywhereUSB/14 and AnywhereUSB TS44 only.) These services control use of COM port redirection. If disabled, COM port redirection cannot be used for the device. .
- **Web Server (HTTP)** or **Secure Web Server (HTTPS)**: These services control the use of the web UI. If you disable them, device users cannot use the web UI or Java applet to configure, monitor, and administer the device.

IP network failover settings (AnywhereUSB/14 only)

The IP Network Failover feature allows the AnywhereUSB/14 to recover from an Ethernet failure. The failover conditions are configurable, and once the AnywhereUSB/14 determines that the primary Ethernet link has failed, it automatically routes the Ethernet traffic to the secondary Ethernet link.

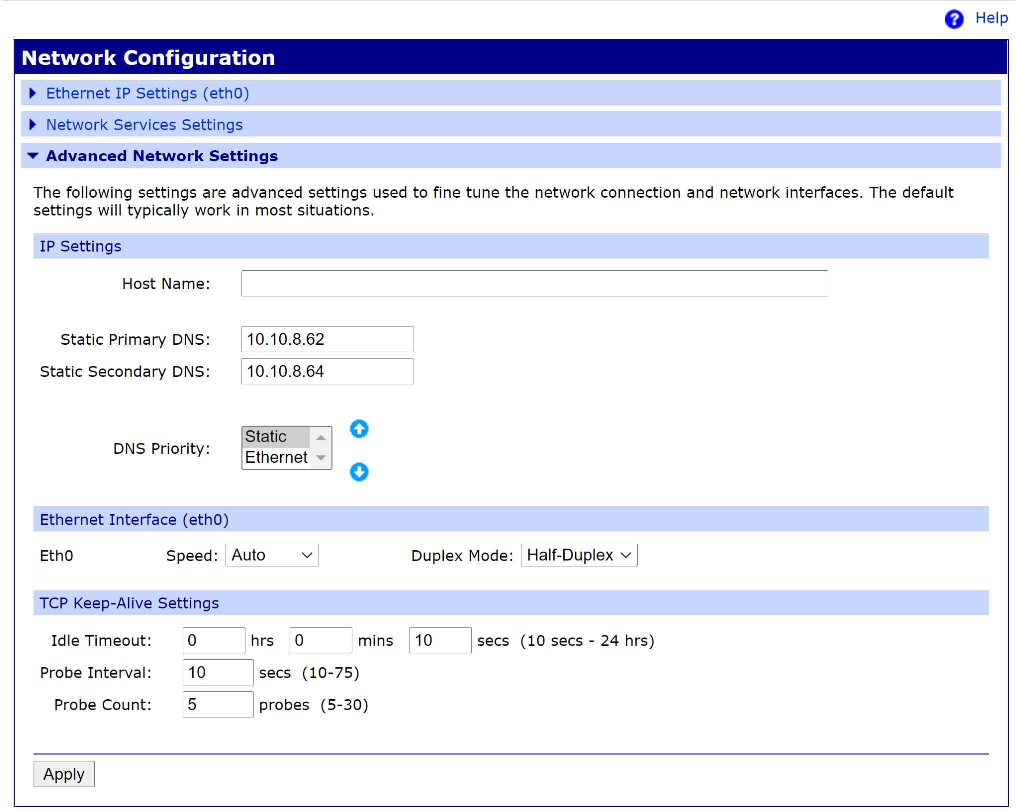
Ethernet port use:

- **LAN1** is the primary Ethernet port. Use this port when connecting only one Ethernet cable or as the main Ethernet connection when connecting both Ethernet ports.
- **LAN2** is the secondary Ethernet port and is used only for redundancy. Only connect an Ethernet cable to this port when you are already using LAN1.

For more information about this feature on the AnywhereUSB/14 device, visit the Digi Knowledge Base at knowledge.digi.com.

Advanced Network Settings page

Use the **Advanced Network Settings** page to further define the network interface.



Help
Network Configuration
Ethernet IP Settings (eth0)
Network Services Settings
Advanced Network Settings
Apply

The following settings are advanced settings used to fine tune the network connection and network interfaces. The default settings will typically work in most situations.

IP Settings

Host Name:

Static Primary DNS: 10.10.8.62

Static Secondary DNS: 10.10.8.64

DNS Priority: Static, Ethernet

Ethernet Interface (eth0)

Eth0 Speed: Auto Duplex Mode: Half-Duplex

TCP Keep-Alive Settings

Idle Timeout: 0 hrs 0 mins 10 secs (10 secs - 24 hrs)

Probe Interval: 10 secs (10-75)

Probe Count: 5 probes (5-30)

IP Settings

- **Host Name**: The name of the host. This is an optional setting which is only used when DHCP is enabled. The entry appears in the DHCP Option 12 field.
- **Static Primary DNS**: The primary IP address that should be used to resolve computer host names to IP addresses. Static DNS servers are specified independently of any network interface and its connection state. An IP address of 0.0.0.0 indicates no server is specified.
- **Static Secondary DNS**: The IP address that should be used to resolve computer host names to IP addresses if the primary IP address is not available. Static DNS servers are specified independently of any network interface and its connection state. An IP address of 0.0.0.0 indicates no server is specified.

- **DNS Priority**: A list of DNS servers in the order they are used to resolve computer host names. Each type of server is tried, starting with the first in the list. For each server type, the primary server is tried first. If no response is received, then the secondary server is tried. If it cannot contact either server, it tries the next server type in the list. A network interface may obtain a DNS server from DHCP or other means when it is connected. If an interface does not obtain a DNS server, it will be skipped and the next server in the priority list will be tried. To change the priority order, select an item from the list and press the up or down arrow.

Ethernet Interface

The options in this section permit the configuration of Ethernet speed and duplex settings.

- **Speed**: Select the Ethernet speed from the options in the list box.
- **Duplex Mode**: Select the desired mode from the options in the list box.

TCP Keep Alive Settings

- **Idle Timeout**: Specify the period of time that a TCP connection is idle before a keep-alive is sent. The range is from 10 seconds to 24 hours.
- **Probe Interval**: Specify the time period between each keep-alive probe. The range is from 10 - 75 seconds.
- **Probe Count**: The number of times TCP probes the connection to determine if it is alive after the keep-alive options has been activated. The connection is assumed lost after sending this number of keep-alive probes. The range is from 5 - 30.

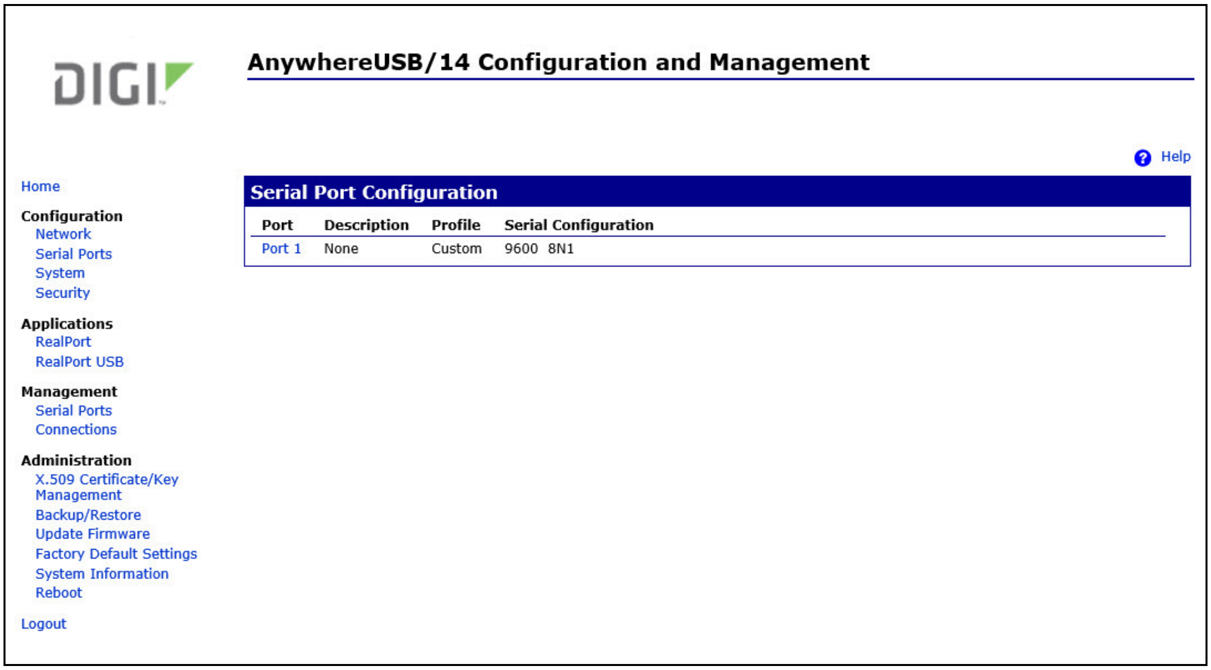
Serial port settings (AnywhereUSB/14 and AnywhereUSB TS44 only)

Configure serial port

The Serial Ports page configures the serial port settings for the management port on the rear of the AnywhereUSB/14 and the four serial ports on the rear of the AnywhereUSB TS44.

Serial Port Configuration page

Use the Serial Port Configuration page to establish a port profile for the serial port of the AnywhereUSB TS44. The Serial Port Configuration page includes the currently selected port profile for the serial port, detailed configuration settings for the serial port, dependent on the port profile selected, and links to Basic Serial Settings and Advanced Serial Settings.



AnywhereUSB/14 Configuration and Management

Serial Port Configuration

Port	Description	Profile	Serial Configuration
Port 1	None	Custom	9600 8N1

Configure a port profile

Port profiles simplify serial port configuration by displaying only those items that are relevant to the currently selected profile. There are several port profile choices, but not all port profiles are supported in all products. Support of port profiles varies by product. If a profile listed in this description is not available on the page, it is not supported.

If a port profile has already been selected, it is shown at the top of the screen. You can change the profile, or retain it and adjust individual settings.

Everything displayed on the Serial Port Configuration screen between Port Profile Settings and the links to the Basic Serial Settings and Advanced Serial Settings depends on the port profile selected.

When using serial ports for the terminal emulator's host or keyboard connections, you must configure those ports for the Custom port profile.

Select and configure a port profile:

1. Access and log in to the web user interface.
2. Select **Serial Ports**.
3. Click the port to configure.
4. Click **Change Profile**.
5. Select the appropriate profile and click **Apply**.
6. Enter the appropriate parameters for each profile; descriptions of each profile follow.
7. Click **Apply** to save the settings.

A list of the ports available on the Digi device server along with a summary of each port's current configuration is displayed when you select Serial Ports under the Configuration heading.

Edit port settings

Click the port's link under the Port heading.

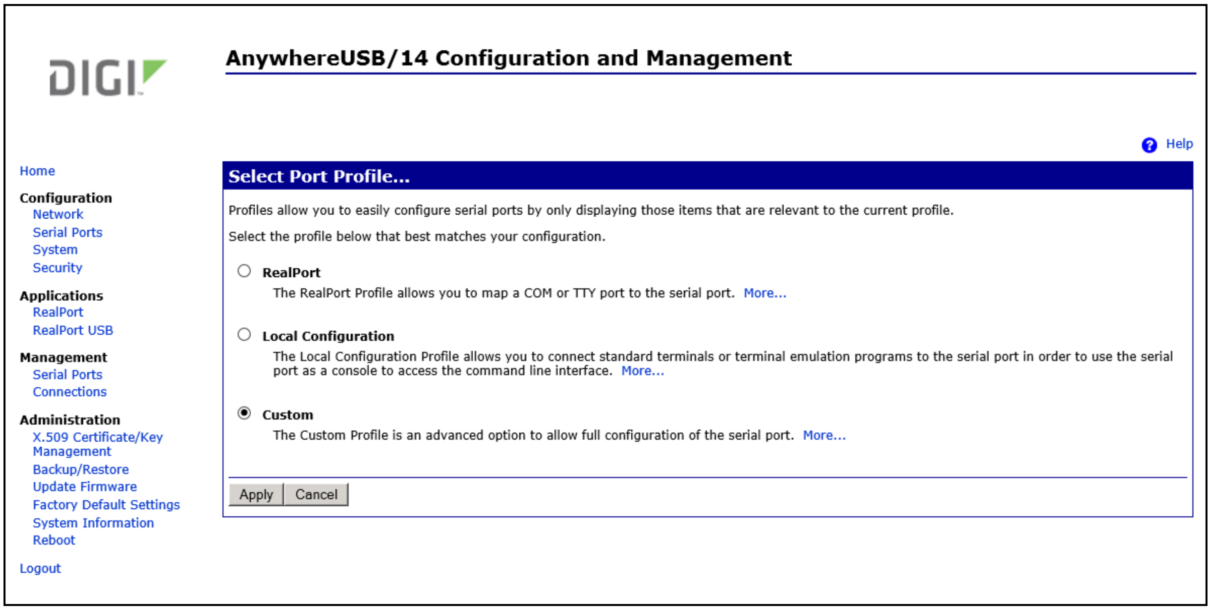
Port profile

A port profile allows you to easily configure a serial port based on how you will be using that port. By selecting one of the predefined profiles, the configuration options are focused only on the settings required for that particular profile.

For situations that do not fit into one of the predefined port profiles, select the **Custom** profile option. All of the port options are available in the custom profile.

Port profile options:

- **RealPort**: Use this option to map a COM port to the serial port. You must have the RealPort driver installed on the host computer. See the *RealPort Installation User Guide* for more information.
- **Local Configuration**: Use this option to connect standard terminals or terminal emulation programs to the serial port. This allows the serial port to act as a console to access the CLI.
- **Custom**: Use this for advanced configuration options.



Select Port Profile...

Profiles allow you to easily configure serial ports by only displaying those items that are relevant to the current profile.

Select the profile below that best matches your configuration.

○ **RealPort**
The RealPort Profile allows you to map a COM or TTY port to the serial port. More...

○ **Local Configuration**
The Local Configuration Profile allows you to connect standard terminals or terminal emulation programs to the serial port in order to use the serial port as a console to access the command line interface. More...

● **Custom**
The Custom Profile is an advanced option to allow full configuration of the serial port. More...

Basic serial setting

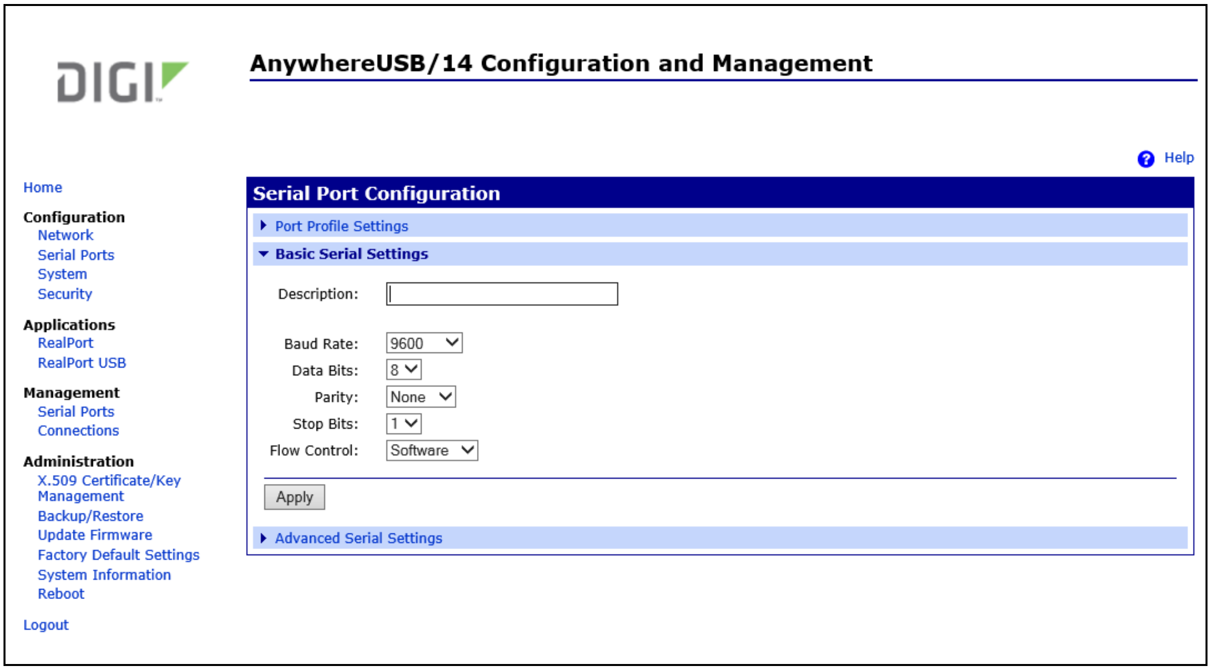
The basic serial port settings must match the serial settings of the connected device. If you do not know these settings consult the documentation that came with your serial device. These serial settings may be documented as 9600 8N1, which means that the device is using a baud rate of 9600 bits per second, 8 data bits, no parity, and 1 stop bit.

When using RealPort (COM port redirection) or RFC 2217, these settings are supplied by applications running on the computer or server and you do not need to change the default values on your Digi device server.

The Description specifies an optional character string that to use for identifying the device connected to the port.

- Baud Rate
- Data Bits
- Parity

- Stop Bits
- Flow Control



AnywhereUSB/14 Configuration and Management

Serial Port Configuration

Basic Serial Settings

Description:

Baud Rate: 9600

Data Bits: 8

Parity: None

Stop Bits: 1

Flow Control: Software

Advanced serial settings

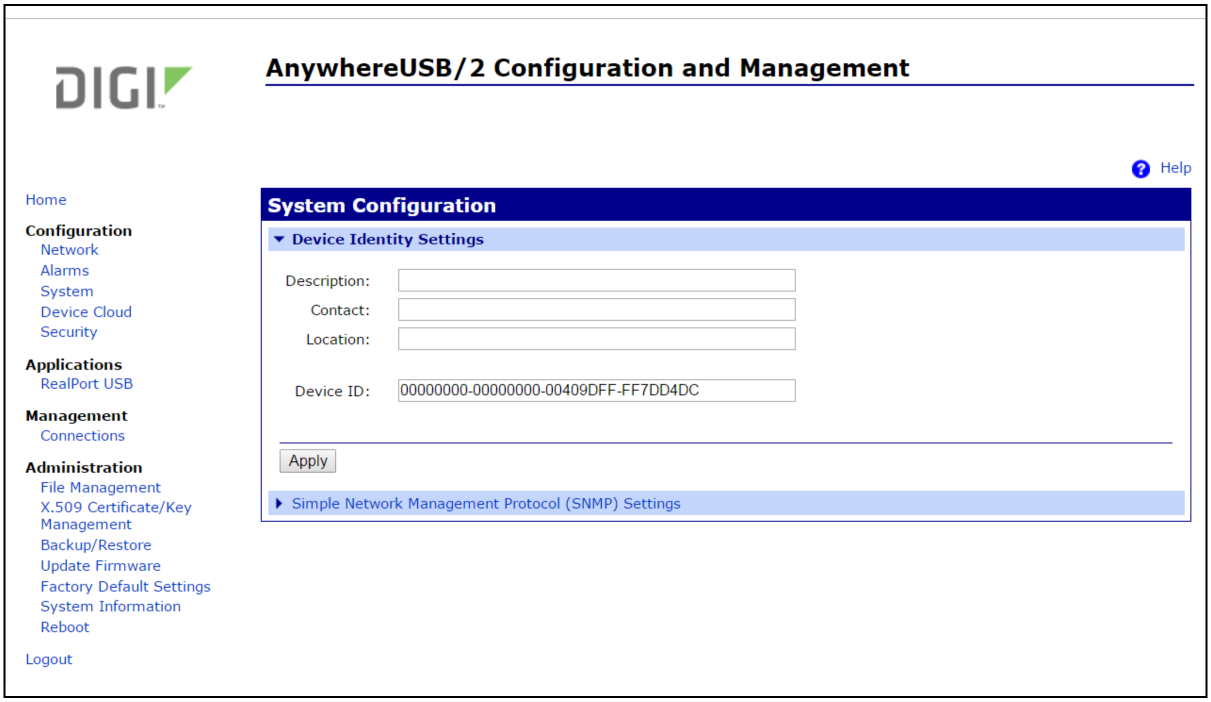
The advanced serial settings rarely change.

System settings

You can use the options in the System Configuration page to configure the following:

Configure device description information: Configure device description information, such as the device name, contact, and location.

Configure SNMP: Configure SNMP to determine whether SNMP is enabled or disabled and whether the SNMP traps are enabled.



Description:

Contact:

Location:

Device ID: 00000000-00000000-00409DFF-FF7DD4DC

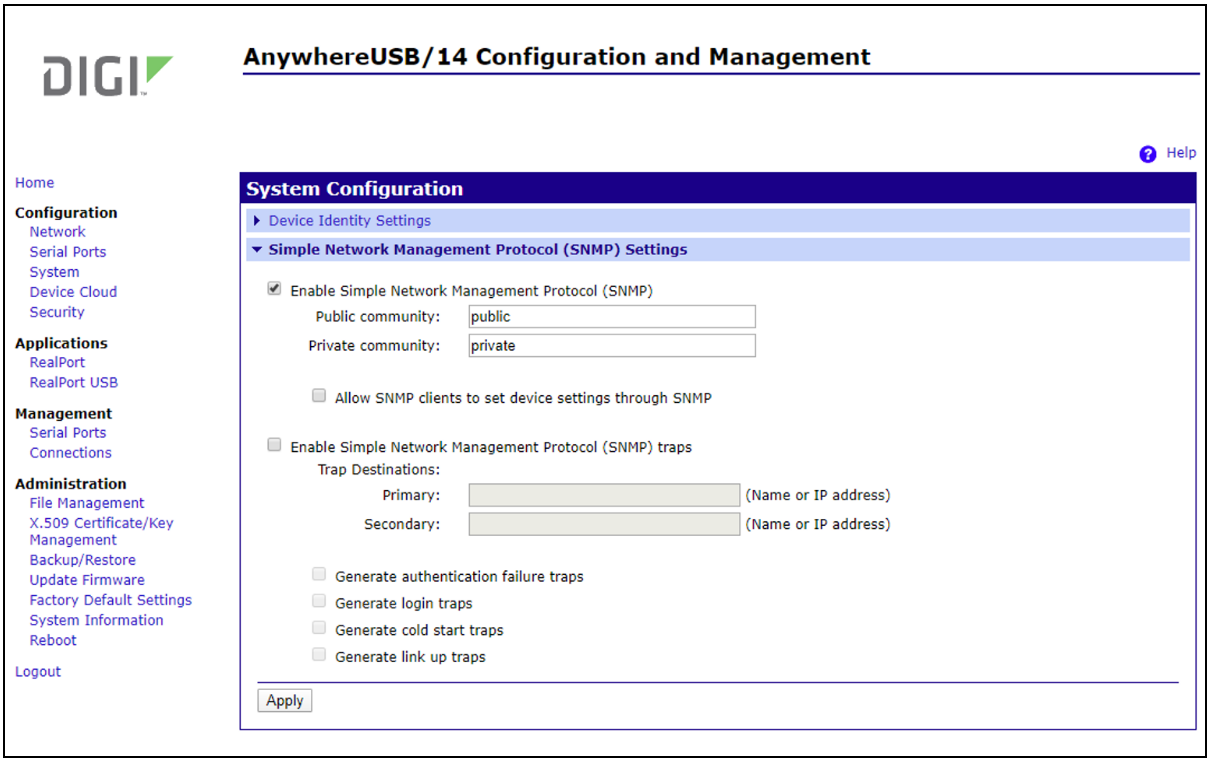
Configure device description information

A device description is a system description of the AnywhereUSB name, contact, and location. Use the device description for identifying a specific AnywhereUSB when working with a large number of devices in multiple locations.

Note The information in the description field represents the “friendly” name of the AnywhereUSB device that appears on the left side of the AnywhereUSB Remote Hub Configuration Utility.

Configure SNMP

Use the Simple Network Management Protocol (SNMP) protocol to manage and monitor network devices. Configure Digi devices to use SNMP features, or disable SNMP for security reasons. To configure SNMP settings, click the SNMP Settings link at the bottom of the System Configuration page.



☑ Enable Simple Network Management Protocol (SNMP)

Public community: public

Private community: private

□ Allow SNMP clients to set device settings through SNMP

□ Enable Simple Network Management Protocol (SNMP) traps

Trap Destinations:

Primary: (Name or IP address)

Secondary: (Name or IP address)

□ Generate authentication failure traps

□ Generate login traps

□ Generate cold start traps

□ Generate link up traps

SNMP settings include:

- **Enable Simple Network Management Protocol (SNMP)**: This checkbox enables or disables the use of SNMP.
- The Public community and Private community fields specify passwords required to get or set SNMP-managed objects. Changing public and private community names from their defaults is recommended to prevent unauthorized access to the device.
  - **Public community**: The password required to get SNMP managed objects. The default is public.
  - **Private community**: The password required to set SNMP managed objects. The default is private.
- **Allow SNMP clients to set device settings through SNMP**: This checkbox enables or disables the capability for users to issue SNMP “set” commands use of SNMP read-only for the AnywhereUSB.
- **Enable Simple Network Management Protocol (SNMP) traps**: Enables or disables the generation of SNMP traps. Additional options are available at the bottom of the page for the SNMP traps: authentication failure, login, cold start, and link up traps.

Remote Manager configuration

The Remote Manager configuration page sets up the connection to the Device Management remote management server so the Digi device can connect to the server. Device Management allows you to configure and manage Remote Manager-registered devices from remote locations.

In this discussion:

- Remote Manager refers to the Digi machine-to-machine cloud-based network operating platform.
- Device Management refers to a web based device management application that allows a user to manage their inventory of devices.
- Remote Manager-registered device is a Digi device that connects to the Remote Manager platform which implements the EDP protocol in order to establish and maintain this connection.

For more information about Remote Manager, these terms, and how to remotely configure and manage

this device, see the *Digi Remote Manager User Guide*.

After you have configured Remote Manager, you must configure the following settings:

- Connection settings
- Short messages
- Advanced settings

Connection settings

Use the connection settings to connect to Remote Manager. You can choose how your AnywhereUSB device connects and communicates with Remote Manager through the following connection types:

- Device-initiated connection
- Server-initiated connection
- Timed connection (device-initiated)

Device-initiated connect

In a device-initiated connection, the AnywhereUSB device attempts to reach Remote Manager to establish the connection. An advantage of the device-initiated connection is that you can use it on any network, whether the device has a public or private IP address, provided the Remote Manager Server is accessible on that network. Configure the following settings for a device-initiated connection:

- **Enable Device-Initiated Connection**. When enabled, the AnywhereUSB device initiates the connection to Remote Manager. This is the typical connection method.
- **Remote Manager Server Address**. The IP address or hostname of Remote Manager (for example, **my.devicecloud.com**).
- **Automatically reconnect to Remote Manager after being disconnected**. If enabled, the AnywhereUSB device waits the specified amount of time after a connection to Remote Manager ends, and then it reconnects to Remote Manager.

Server-initiated connection

A server-initiated connection works the opposite from device-initiated connections. Remote Manager opens a TCP connection, and the Digi device server listens for the connection. An advantage of a server-initiated connection is that the connection is only established when it is needed; this minimizes the overhead of maintaining a connection. A disadvantage is that the device appears disconnected in the Remote Manager's device list most of the time. In addition, server-initiated connections cannot be used if the device has a private IP address or is behind a NAT. Configure the following settings for a server-initiated connection:

- **Enable Server-Initiated Connection**. When enabled, this device listens for a connection initiated by Remote Manager.
- **Enable Device IP Address updates to the following server**. If enabled, the Digi device server connects to Remote Manager to informing the server of the current IP address of the Digi device server. This permits Remote Manager to connect back to the device, or to dynamically update a DNS with the IP address of the device.
- **Remote Manager Server Addres**s. The IP address or hostname of Remote Manager (for example, **my.devicecloud.com**).
- **Retry if the IP Address update fails**. If enabled, when a Device IP Address update fails, the Digi device server waits the specified amount of time before retrying the Device IP Address update.

Timed connection

A timed connection is another form of a device-initiated connection. For a timed connection, the AnywhereUSB device attempts to connect to Remote Manager at a configured, regular interval (period). If a connection to Remote Manager is already established, the device server does not attempt to connect a timed connection. The next attempt for a timed connection occurs at the next scheduled interval. Configure the following settings for a timed connection:

- **Enable Timed Connection**. When enabled, this device initiates the connection to Remote Manager at the configured interval (period). A timed connection defers to (that is, does not disrupt) a Remote Manager connection that is already established. If a timed connection defers to an existing Remote Manager connection, or if the timed connection cannot be successfully established, the AnywhereUSB device tries again at the next interval.
- **Remote Manager Server Address**. The IP address or hostname of Remote Manager (for example, **my.devicecloud.com**).
- **Connect every: H hrs M mins**. The interval (period) in hours and minutes at which the AnywhereUSB device attempts a timed connection to the specified Remote Manager Server.
- **After boot, wait before first timed connection**. When the AnywhereUSB device boots (start-up), you may see a delay before the device attempts the first timed connection. There are three choices for this delay:
    - Immediate - The device attempts the first timed connection immediately.
    - One Interval -The device attempts the first timed connection after one configured interval (period) has elapsed.
    - Random Delay - The device attempts the first timed connection at a random interval of time between zero (immediate) and the configured interval (period). A random delay may be helpful when a number of devices are deployed in a single location, and you want to distribute first Remote Manager timed connection attempts over time when power is restored following an outage.

Short messages

Use these settings when you are sending Short Messages to Remote Manager. For more information, see the *Digi Remote Manager User Guide*.

Advanced settings

You can use these settings in advanced situations and the defaults are typically suitable for most environments.

Note These settings control the keep alive settings of the various interfaces and should only be changed when the defaults do not properly work.

Advanced settings - connection settings

These are advanced settings you can use to fine tune the connection between Remote Manager and the AnywhereUSB device.

- **Disconnect when the Remote Manager Connection is idle**.
  - **Idle Timeout** - Enables or disables the idle timeout for the Remote Manager connection. If enabled, an idle connection will be ended after the specified amount of time. Note that keep-alive messages are considered to be normal packets and they will reset the idle timer.
- **Authenticate to Remote Manager with a password**. These fields are only applicable if your Remote Manager account has been configured to expect a password from the Remote Manager-registered device. Typically, this option is set through Remote Manager. Both the Remote Manager-registered device and Remote Manager need to be configured identically.

Advanced settings - Ethernet settings

These settings apply to device-initiated Remote Manager connections over Ethernet networks. Each network has the following settings:

- **Remote Manager Connection Keep-Alive Settings**. These settings control how often keep-alive packets are sent over the device-initiated connection to Remote Manager, and whether the Remote Manager-registered device waits before dropping the connection.
  - **Device Send Interval**. Specifies how frequently the device sends a keep-alive packet to the Remote Manager Server if the Remote Manager connection is idle. Remote Manager expects to receive either Remote Manager protocol messages or keep-alive packets from the device at this interval.
  - **Server Send Interval**. Specifies how frequently Remote Manager sends a keep-alive packet to the AnywhereUSB device if the Remote Manager connection is idle. The device expects to receive either Remote Manager protocol messages or keep-alive packets from Remote Manager at this interval.
  - **Assume connection is lost after *n* timeouts**. Signals when the connection has been lost and works with the interval settings.

  Keep-alives for the Remote Manager connection serve three basic purposes:

1. Keep the Remote Manager connection alive through network infrastructure such as routers, NATs, and firewalls.
2. Inform the other (remote) side of the Remote Manager connection that its peer is still active.
3. Test the Remote Manager connection to detect whether it has stopped responding and should be abandoned. Recovery actions are taken as configured in other settings.

The device and server each perform their own independent monitoring of the Remote Manager connection state (active, idle and missed keep-alives). If Remote Manager protocol messages or data other than keep-alives are exchanged over the Remote Manager connection, the idle timers that trigger keep-alives are reset, and the consecutive missed keep-alive counts are cleared to zero.

- **Connection Method**. Specifies the method by which the associated interface connects to Remote Manager. Select one of the following values:
  - **TCP (default)**. This is typically satisfactory for most connections, and it is the most efficient method of connecting to the remote server in terms of speed and transmitted data bytes. **None** has the same effect as selecting TCP.
  - **SSL**. Connect using Secure Socket Layer.

Note For Remote Manager service, select TCP or SSL, as the other connection methods are not supported by Remote Manager.

  - **Automatic**. This value is less efficient, but it is useful in situations where a firewall or proxy may prevent direct connection via TCP. This value tries each combination until it makes a connection.
  - **HTTP**. Connect using HTTP.
  - **HTTP over Proxy Options**. Specifies the proxy settings required to communicate over a proxy network using HTTP. These settings only apply when Automatic or HTTP over Proxy are selected.
    - **Enable persistent proxy connections**: Specifies whether the Remote Manager-registered device should attempt to use HTTP persistent connections. Not all HTTP proxies correctly handle HTTP persistent connections. The use of persistent connections can improve performance of the exchange of messages between the Remote Manager-registered device and Remote Manager, when that connection is HTTP/proxy. You can reuse the same HTTP connection for multiple consecutive HTTP requests and replies, eliminating the overhead of establishing a new TCP connection for each individual HTTP request/reply, then closing that connection when the request is complete.

USB information in Remote Manager

This section provides information about some state classes available in Digi Remote Manager.

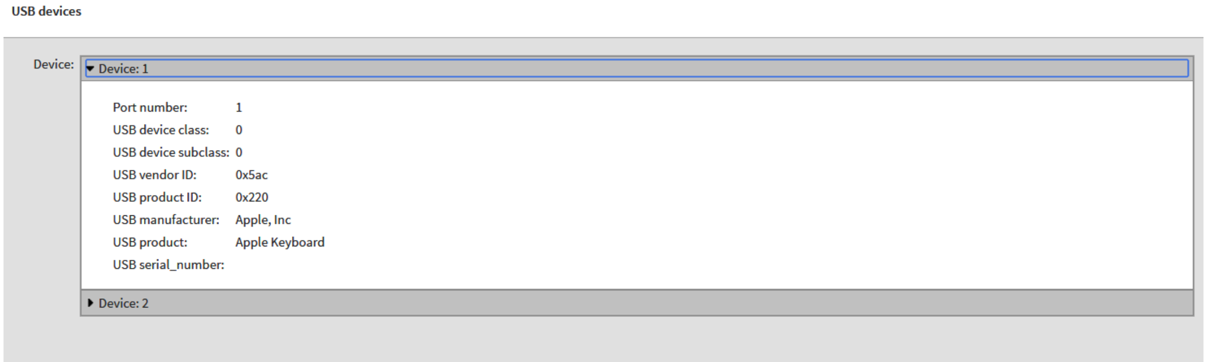
For more detailed information about Remote Manager, see the *Digi Remote Manager User Guide*.

To access the Remote Manager application:

1. Go to devicecloud.digi.com/login.do, and log in with your Username and Password.
2. In Remote Manager, select **Device Management**, and navigate to the AnywhereUSB unit you want to access.
3. Select the AnywhereUSB you want to access, and click **Properties**.

Viewing USB information

- To view USB devices, expand **System Information** and select **USB devices**.



USB devices

Device: ▾ Device: 1

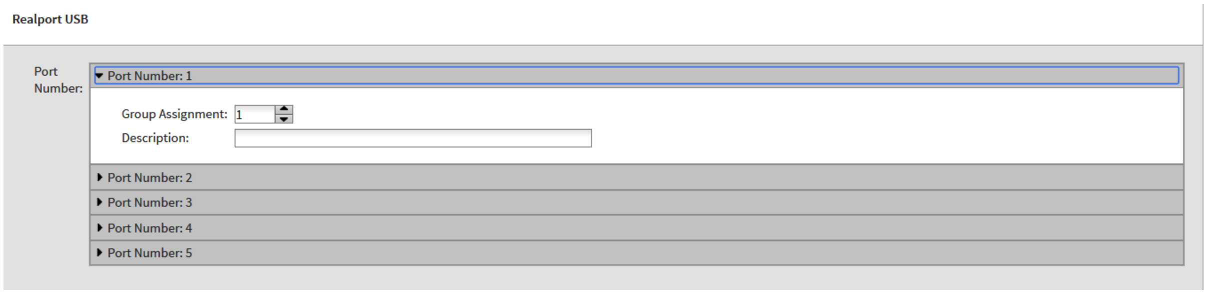
Port number: 1
USB device class: 0
USB device subclass: 0
USB vendor ID: 0x5ac
USB product ID: 0x220
USB manufacturer: Apple, Inc
USB product: Apple Keyboard
USB serial_number:

▸ Device: 2

The USB Devices window displays information about each of the USB devices that are physically attached to the AnywhereUSB. The AnywhereUSB must be successfully connected to a host computer to display in the USB Devices window. It always reports the port number of the upstream AnywhereUSB port number and never the port number of the external USB hub, if applicable.

Note If any of the attached USB devices are connected to the AnywhereUSB through USB hubs, the USB devices still display under the USB port of the specific AnywhereUSB.

- To view Realport USB, expand **Advanced Configuration** and select **Realport USB**.



Realport USB

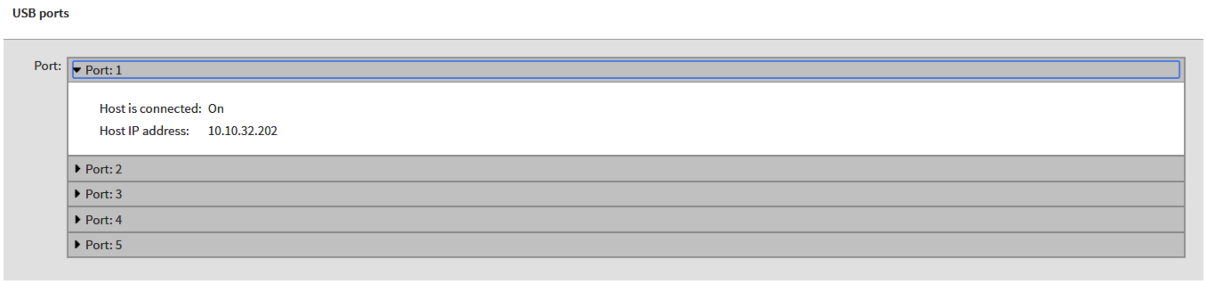
Port Number: ▾ Port Number: 1

Group Assignment: 1
Description:

▸ Port Number: 2
▸ Port Number: 3
▸ Port Number: 4
▸ Port Number: 5

For more information, see Configure groups.

- To view USB ports, expand **System Information** and select **USB ports**.


USB ports

Port:

Port: 1

Host is connected: On

Host IP address: 10.10.32.202

Port: 2

Port: 3

Port: 4

Port: 5

The USB Ports section shows the hosts and which ports they own.

Security settings

On the Security page, you can specify the authentication information required for logging into the AnywhereUSB web UI or CLI.

Password authentication enabled

For devices with the most recent firmware installed, the **Enable password authentication** option is selected by default and the feature is enabled. This ensures that a user is required to log in to the web UI. The log in defaults are:

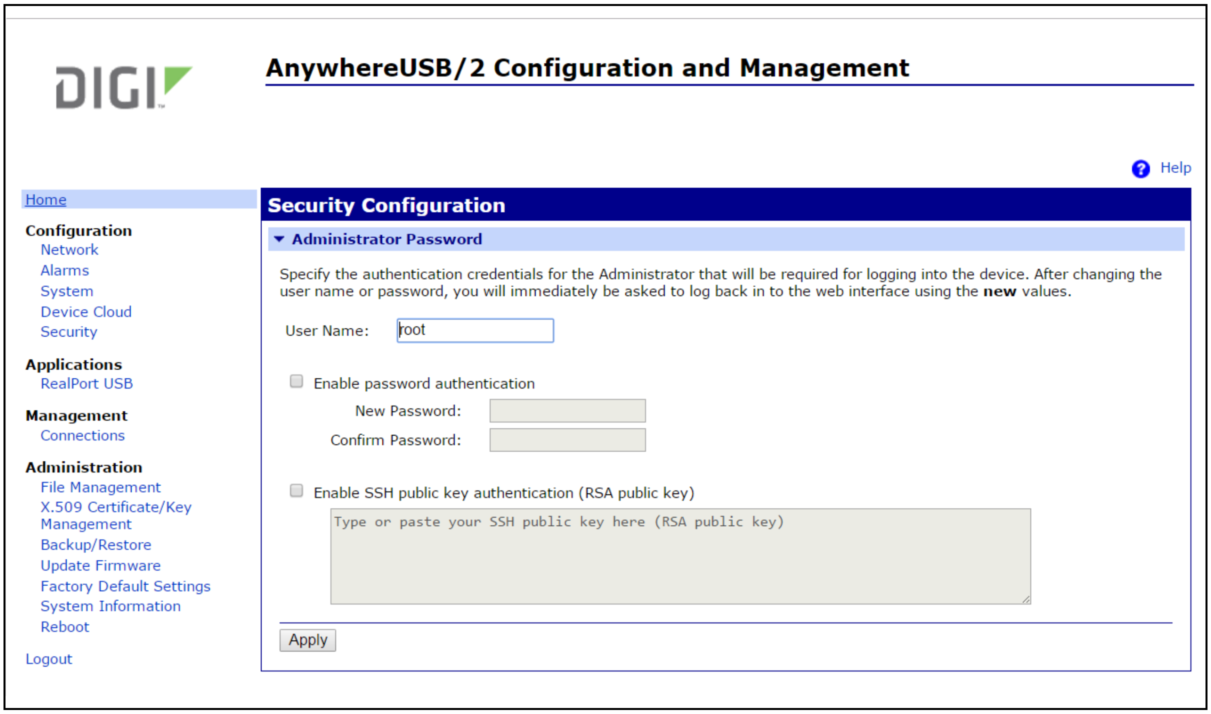
- **User name**: **root**
- **Password**: The unique, default password is printed on the device label.

Note If the default user name and password does not work, it may have been changed. Contact your system administrator for help.

Password authentication not enabled

If your device does not have a password printed on the label, the password authentication feature has not been enabled. You will need to enable the feature set a password.

1. Log in to a Microsoft Windows computer with an account that has administrative privileges.
2. Select **Start** > **Programs** > **AnywhereUSB** > **AnywhereUSB Remote Hub Configuration Utility**.
3. Select **Configuration** > **Security**. The **Security Configuration** page appears.
4. In the **User Name** field, you can change the user name from the default, if desired.
5. Select **Enable password authentication**.
    a. In the **New Password** field, enter the password.
    b. In the **Confirm Password** field, re-enter the same password. The entries in both fields must match.
6. Click **Apply**. You must log in to the web UI using the new values.



AnywhereUSB/2 Configuration and Management

Security Configuration

Administrator Password

Specify the authentication credentials for the Administrator that will be required for logging into the device. After changing the user name or password, you will immediately be asked to log back in to the web interface using the **new** values.

User Name: root

□ Enable password authentication

New Password:

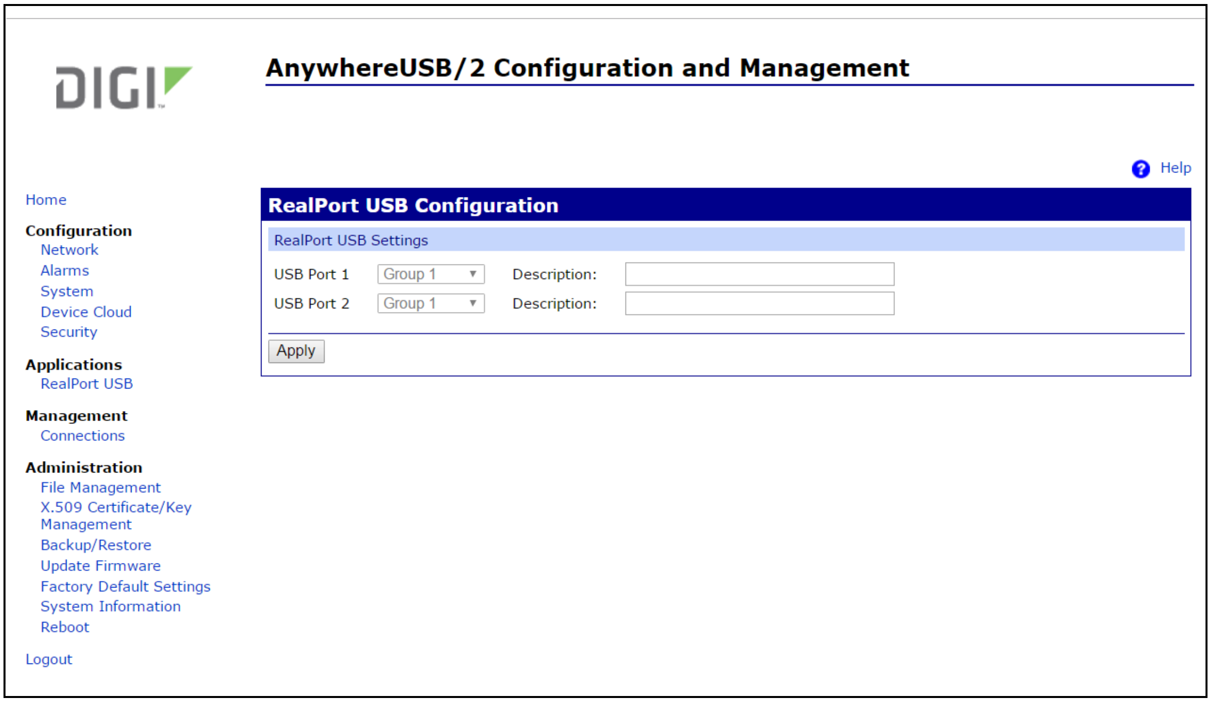
Confirm Password:

□ Enable SSH public key authentication (RSA public key)

Type or paste your SSH public key here (RSA public key)

Applications (AnywhereUSB/5M and AnywhereUSB/14)

The RealPort USB Configuration page under Applications allows you to configure the Groups feature for the multi-host devices (AnywhereUSB/5M and AnywhereUSB/14). You can assign each USB port of (AnywhereUSB/5M and AnywhereUSB/14) to a single group. You can connect only one host computer to a group. Unassigning a port makes it unavailable to any host computer. Use the RealPort USB Configuration page to configure groups.



AnywhereUSB/2 Configuration and Management

RealPort USB Configuration

RealPort USB Settings

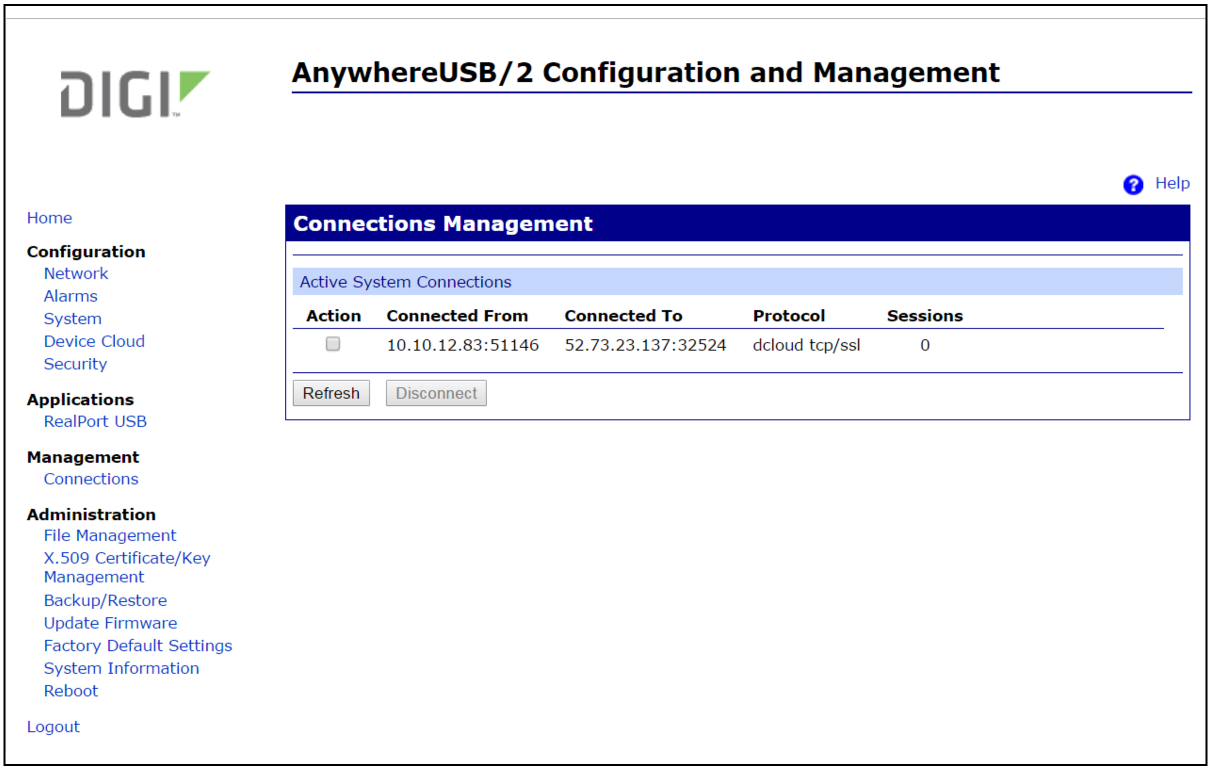
USB Port 1 Group 1 Description:

USB Port 2 Group 1 Description:

Management

The Connection Management page displays additional information about the current connections to the AnywhereUSB.

The example below shows a USB connection to a host computer.



Active System Connections

Action	Connected From	Connected To	Protocol	Sessions
□	10.10.12.83:51146	52.73.23.137:32524	dcloud tcp/ssl	0

Note Clicking **Disconnect** will only temporarily disconnect the session. Since the connection request is driven by the host computer, the session will automatically get re-established.

Click **Disconnect** only for troubleshooting purposes, such as when instructed by Digi Technical Support.

If you need to disconnect the device from a host computer, use **Disconnect** in the **AnywhereUSB Remote Hub Configuration Utility**.

Administration

Administration tasks for the AnywhereUSB include certificate and key management, backing up and restoring device configurations, updating firmware, restoring the device configuration to factory defaults, viewing system information, and restarting the device. As with device configuration and monitoring, it covers performing administrative tasks through a variety of device interfaces.

The Administration section of the web UI main menu provides the following menus:

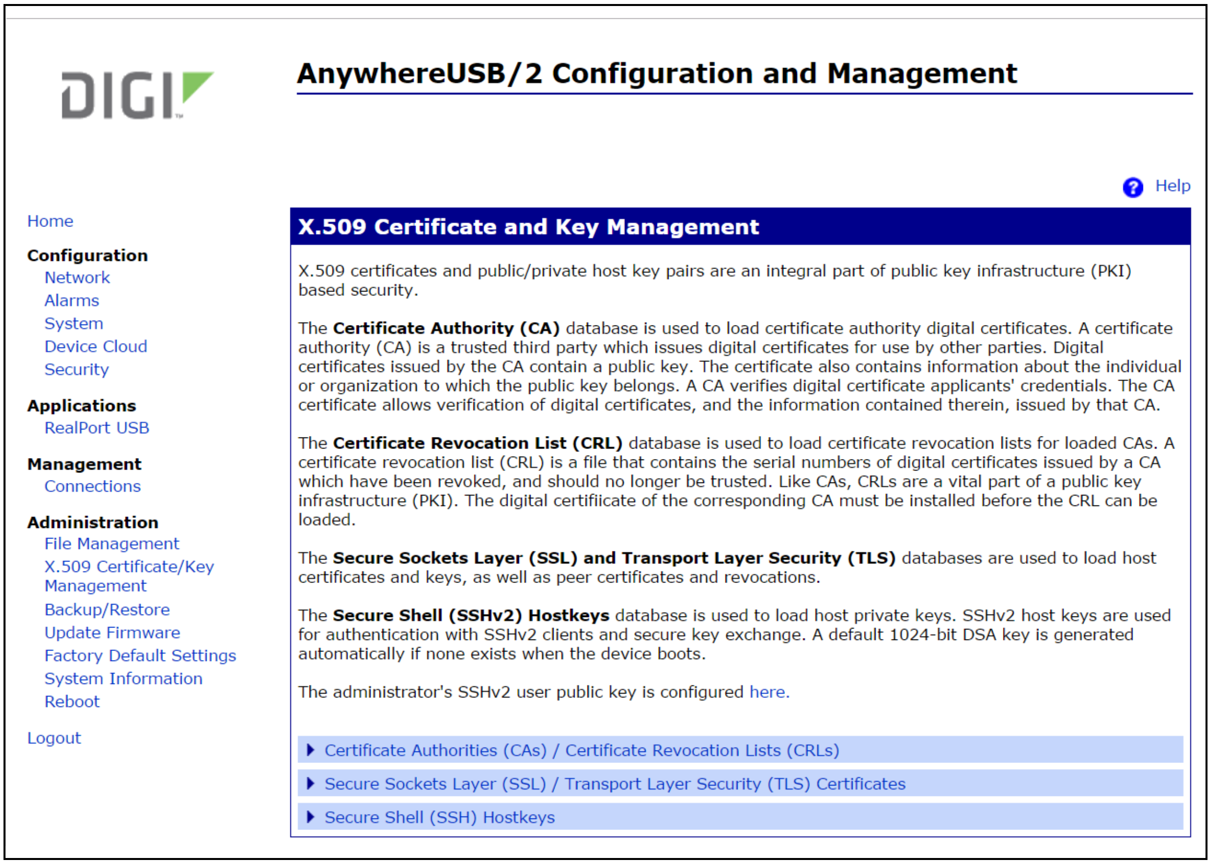
- X.509 Certificate and Key Management: For configuring security.
- Backup/restore settings: For backing up or restoring a device's configuration settings.
- Update firmware: For updating firmware, including Boot code.
- Factory default settings: For restoring a device to factory default setting.

- System information: For displaying general system information for the device and device statistics.
- Reboot the AnywhereUSB: For restarting the device.

X.509 Certificate and Key Management

The AnywhereUSB devices use X.509 certificates and public/private host key pairs as part of their public key infrastructure (PKI) based security. Configure and install a digital certificate on the device to encrypt traffic to and from the device.

This is an optional setting that allows a host computer to confirm AnywhereUSB device authenticity and to encrypt USB-over-IP traffic. This digital certificate must be signed by a Trusted Certificate Authority (CA). Since an AnywhereUSB is not publicly accessible, an enterprise CA can self-sign the digital certificate.



X.509 Certificate and Key Management

X.509 certificates and public/private host key pairs are an integral part of public key infrastructure (PKI) based security.

The **Certificate Authority (CA)** database is used to load certificate authority digital certificates. A certificate authority (CA) is a trusted third party which issues digital certificates for use by other parties. Digital certificates issued by the CA contain a public key. The certificate also contains information about the individual or organization to which the public key belongs. A CA verifies digital certificate applicants' credentials. The CA certificate allows verification of digital certificates, and the information contained therein, issued by that CA.

The **Certificate Revocation List (CRL)** database is used to load certificate revocation lists for loaded CAs. A certificate revocation list (CRL) is a file that contains the serial numbers of digital certificates issued by a CA which have been revoked, and should no longer be trusted. Like CAs, CRLs are a vital part of a public key infrastructure (PKI). The digital certifiicate of the corresponding CA must be installed before the CRL can be loaded.

The **Secure Sockets Layer (SSL) and Transport Layer Security (TLS)** databases are used to load host certificates and keys, as well as peer certificates and revocations.

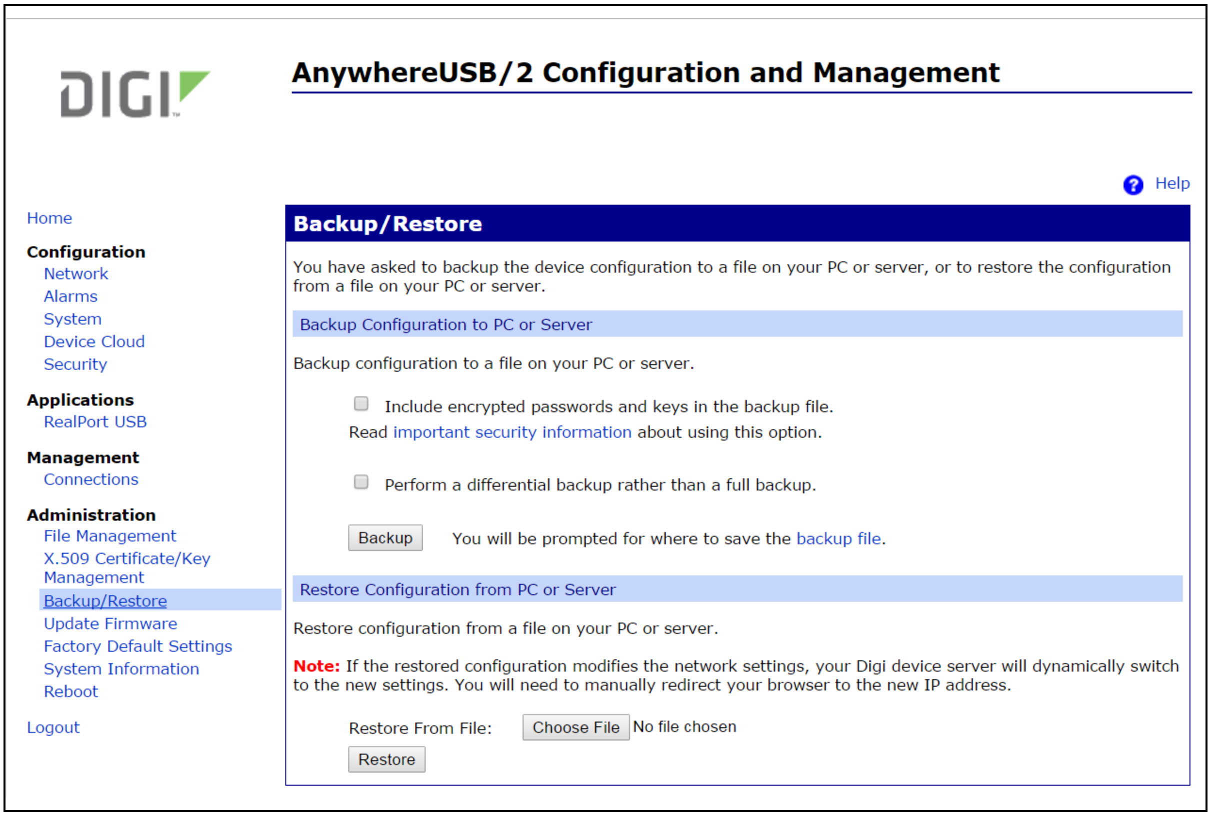
The **Secure Shell (SSHv2) Hostkeys** database is used to load host private keys. SSHv2 host keys are used for authentication with SSHv2 clients and secure key exchange. A default 1024-bit DSA key is generated automatically if none exists when the device boots.

The administrator's SSHv2 user public key is configured here.

▸ Certificate Authorities (CAs) / Certificate Revocation Lists (CRLs)
▸ Secure Sockets Layer (SSL) / Transport Layer Security (TLS) Certificates
▸ Secure Shell (SSH) Hostkeys

Backup/restore settings

Once the AnywhereUSB is configured, backing up the configuration settings using the Backup/Restore page is recommended in case problems occur later, firmware is upgraded, or hardware is added. When configuring multiple devices, use the backup/restore feature as a convenience, where the first device's configuration settings are backed up to a file, and then the file is loaded onto the other devices.



AnywhereUSB/2 Configuration and Management

Backup/Restore

You have asked to backup the device configuration to a file on your PC or server, or to restore the configuration from a file on your PC or server.

Backup Configuration to PC or Server

Backup configuration to a file on your PC or server.

□ Include encrypted passwords and keys in the backup file.
Read important security information about using this option.

□ Perform a differential backup rather than a full backup.

Backup You will be prompted for where to save the backup file.

Restore Configuration from PC or Server

Restore configuration from a file on your PC or server.

Note: If the restored configuration modifies the network settings, your Digi device server will dynamically switch to the new settings. You will need to manually redirect your browser to the new IP address.

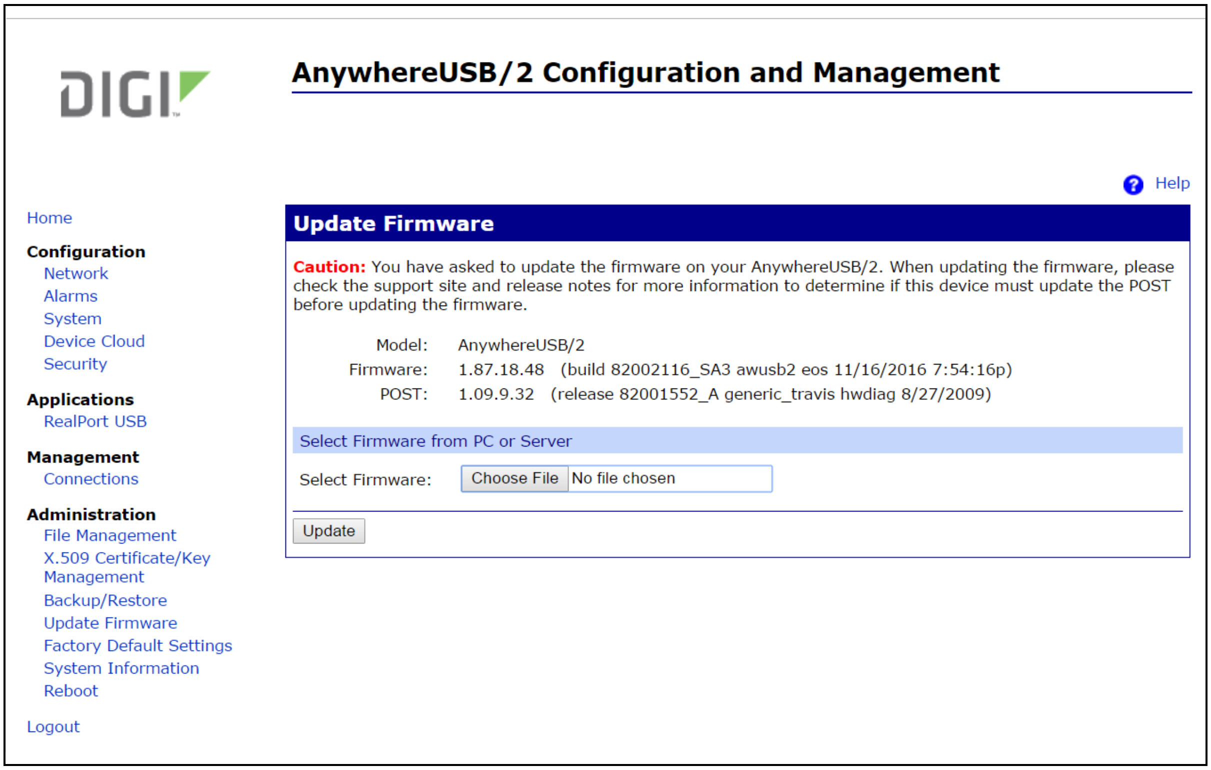
Restore From File: Choose File No file chosen

Restore

Update firmware

From the Update Firmware page, update the firmware for the AnywhereUSB from a file on a computer.

1. From the main menu, select **Administration > Update Firmware**. The Update Firmware page is displayed.
2. Enter the name of the firmware file in the **Select Firmware** field, or click **Browse** to locate and select the firmware file.
3. Click **Update**. DO NOT close the browser until the update is complete and a restart prompt appears.



Caution: You have asked to update the firmware on your AnywhereUSB/2. When updating the firmware, please check the support site and release notes for more information to determine if this device must update the POST before updating the firmware.

Model: AnywhereUSB/2
Firmware: 1.87.18.48 (build 82002116_SA3 awusb2 eos 11/16/2016 7:54:16p)
POST: 1.09.9.32 (release 82001552_A generic_travis hwdiag 8/27/2009)

Select Firmware: No file chosen

Factory default settings

If needed, you can reset the device configuration of an AnywhereUSB device to the factory default settings.

Restoring the AnywhereUSB to its factory default settings clears all current configuration settings. In addition, any files loaded into the device through the **File Management** page are also removed. If the **Keep network settings** checkbox is checked, the network settings will not be reset.

The password will be reset to the factory default during the reboot. Some models have the default password printed on the device label. If this password is on the label, the password is reset to this default. If a password is not printed on the label, you will need to manually reset the password. See Security settings.

There are several ways to reset the device configuration of an AnywhereUSB device to the factory default settings:

- Using the web UI

  Resetting factory defaults from the web UI clears all current settings, resets the password for the administrative/root user, and restores the settings to the factory defaults. Using the restore operation from the web UI is the best way to reset the configuration. Before performing the restore operation, back up the settings using the Backup/Restore operation to save the current configuration in case you want to restore it at a later time.

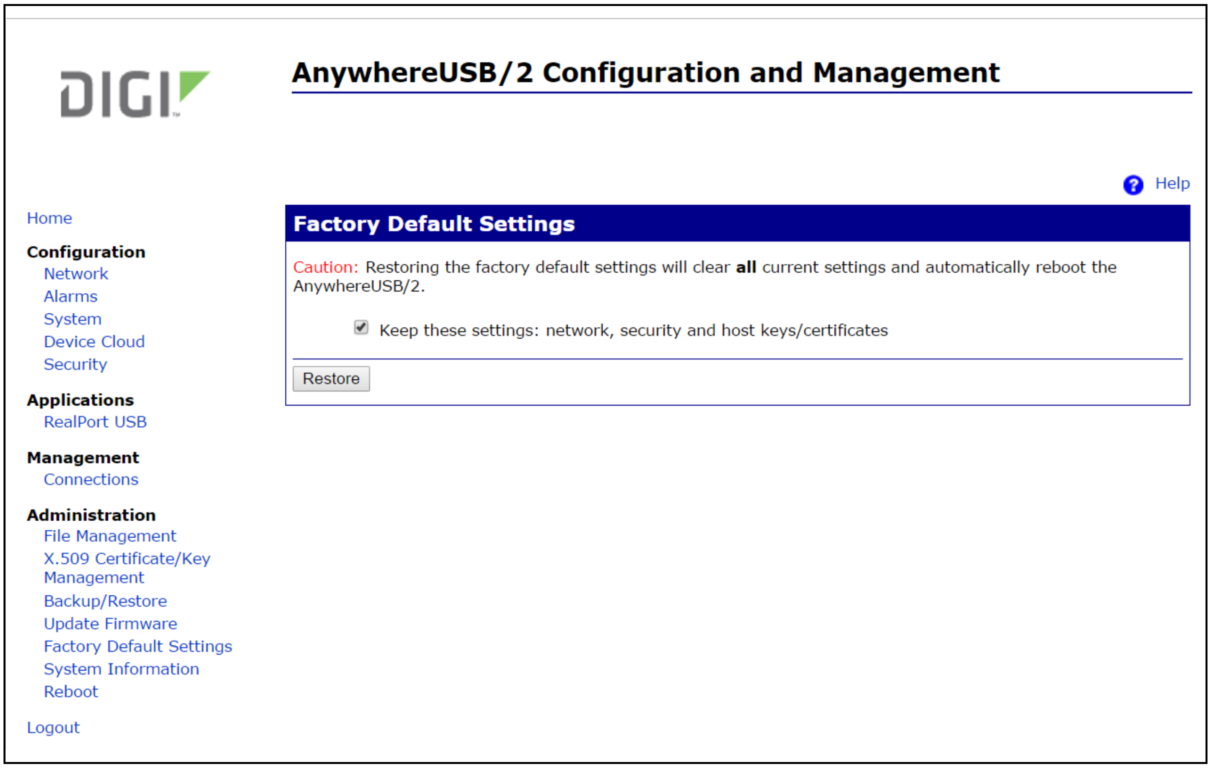
  A reboot from the web UI is a soft reset.

- Using the boot command

  A reboot using the boot command is a soft reset.

- Using the front panel Reset button

  A reboot using the Reset button/signal method is a hard reset.



AnywhereUSB/2 Configuration and Management

Factory Default Settings

Caution: Restoring the factory default settings will clear **all** current settings and automatically reboot the AnywhereUSB/2.

☑ Keep these settings: network, security and host keys/certificates

Using the web UI

The Factory Default Settings operation from the web UI clears all current settings, resets the password for the administrative/root user, and restores the settings to the factory defaults.

The password will be reset to the factory default during the reboot. Some models have the default password printed on the device label. If this password is on the label, the password is reset to this default. If a password is not printed on the label, you will need to manually reset the password. See Security settings.

1. Make a backup copy of the configuration using the **Backup/Restore** operation.
2. From the **Main** menu, click **Administration > Factory Default Settings**. The Factory Default settings page is displayed.
3. (Optional) Check the **Keep network settings** checkbox to keep the current network settings such as the IP address and host key settings. In addition, any files that were loaded into the device through the File Management page such as custom-interface files and applet files are retained.
4. Click **Restore**.

Using the boot command

For details, see Configure from the command line.

From the command line, the `boot action=factory` command clears all current configuration settings, except the IP address settings, host key settings, and password for the administrative/root user; restores the settings to the factory defaults; then restarts the device.

The password will be reset to the factory default during the reboot. Some models have the default password printed on the device label. If this password is on the label, the password is reset to this default. If a password is not printed on the label, you will need to manually reset the password. See Security settings.

#> boot action=factory

There are several other options for using the boot command to load configuration settings. Type help boot to see all command options.

Using the front panel Reset button

If the AnywhereUSB is not accessible from the web UI, restore the configuration to factory defaults using the Reset button.

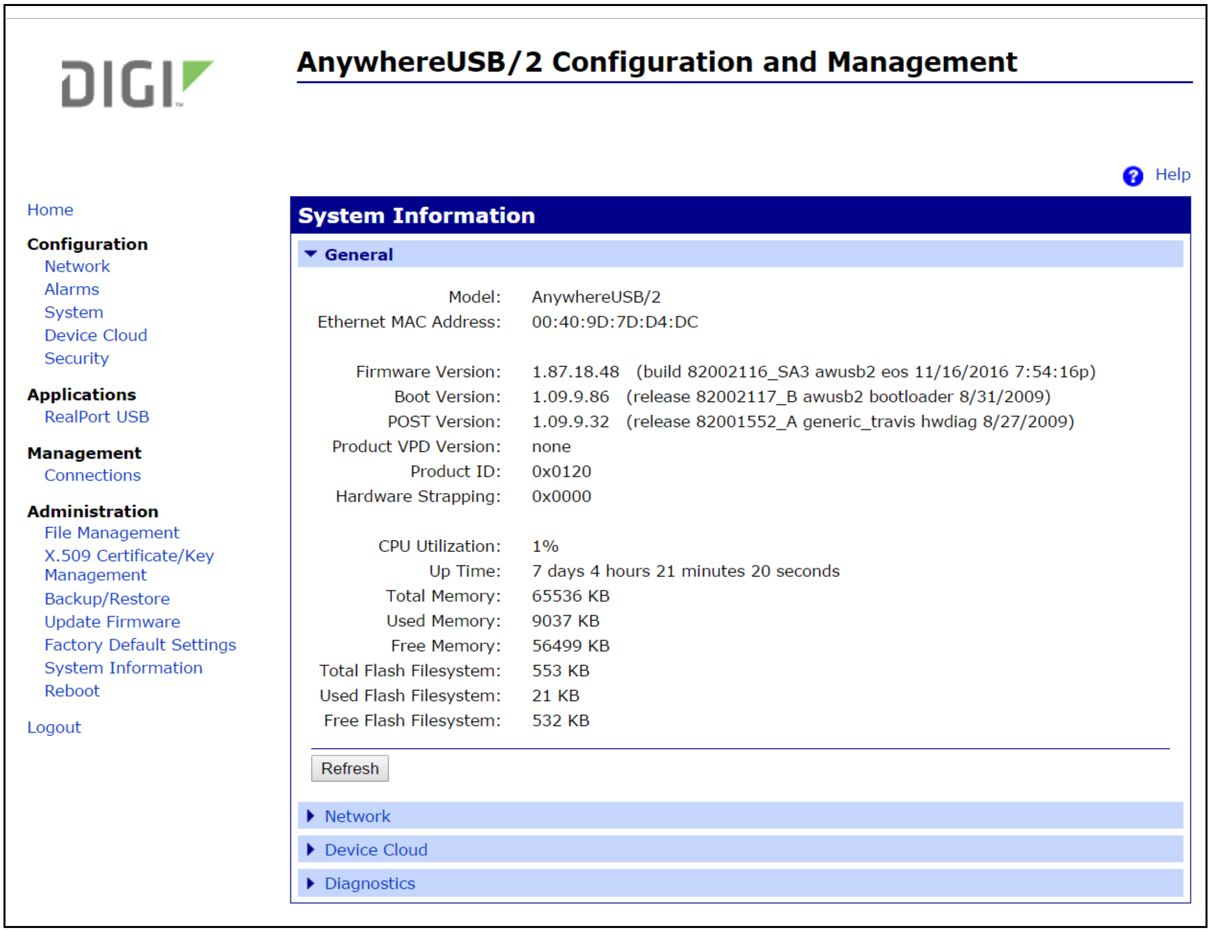
1. Disconnect power from the AnywhereUSB.
2. Hold down the front panel **Reset** button.
3. While holding the **Reset** button down, connect power to the AnywhereUSB.
4. Wait about 10 seconds, until the System Status LED blinks a Red 1-5-1 code.
5. Release the **Reset** button.

System information

System information displays the model, MAC address, firmware version, and boot version of the AnywhereUSB device. It also displays memory statistics, CPU utilization, and how long the device has been running since the last power-on or restart.

To access system information:

1. Access and log in to the web user interface.
2. Select **Administration > System Information**.
3. Select **General**, **Network**, or **Diagnostics** for the appropriate information.



Model: AnywhereUSB/2
Ethernet MAC Address: 00:40:9D:7D:D4:DC

Firmware Version: 1.87.18.48 (build 82002116_SA3 awusb2 eos 11/16/2016 7:54:16p)
Boot Version: 1.09.9.86 (release 82002117_B awusb2 bootloader 8/31/2009)
POST Version: 1.09.9.32 (release 82001552_A generic_travis hwdiag 8/27/2009)
Product VPD Version: none
Product ID: 0x0120
Hardware Strapping: 0x0000

CPU Utilization: 1%
Up Time: 7 days 4 hours 21 minutes 20 seconds
Total Memory: 65536 KB
Used Memory: 9037 KB
Free Memory: 56499 KB
Total Flash Filesystem: 553 KB
Used Flash Filesystem: 21 KB
Free Flash Filesystem: 532 KB

Reboot the AnywhereUSB

Changes to some device settings require saving the changes and rebooting the AnywhereUSB.

To reboot the device from the web UI:

1. Access and log in to the web user interface.
2. Select **Administration > Reboot**.
3. Click **Reboot**. Wait approximately 1 minute for the reboot to complete.

To reboot the device using the front panel Reset button:

1. Hold down the front panel **Reset** button for about 2 seconds, until the front panel LEDs start blinking an amber color.
2. Quickly release the **Reset** button then hold it down again.
3. Wait about 4 seconds, until the front panel LEDs flicker then turn off.
4. Release the **Reset** button.

Note This reboot procedure is only applicable when the AnywhereUSB is in a normal operational state, such as when the System Status LED is blinking green. If the System Status LED is repeatedly blinking red (instead of slow green), please contact Digi Technical Support at www.digi.com/support.

Configure from the command line

This chapter explains how to configure the AnywhereUSB from the command line interface (CLI). Configuring an AnywhereUSB through the CLI consists of entering a series of commands to set values in the device.

Note This feature is not available on the first generation AnywhereUSB/5.

Access the command line interface

To configure devices using commands:

1. Do one of the following to connect the AnywhereUSB to a computer.
   - AWUSB/14 or AWUSB/TS-44 only: Connect a console cable between the DB9 of the AWUSB and a PC or Laptop COMM port, allowing CLI access directly through a Terminal emulation program. Use the following serial settings:
     - **Baud rate or Bits per second**: 9600
     - **Data**: 8 bit
     - **Parity**: None
     - **Stop**: 1 bit
     - **Flow control**: Software
   - All other AWUSB models:
     - Follow the instructions in the *AnywhereUSB Quick Start Guide* to assign an IP address to the AnywhereUSB.
     - Open a terminal emulation program that supports telnet or SSH, and connect to the IP address assigned to the AnywhereUSB. Alternatively, if your operating system has telnet installed, you can telnet from the operating system command line with the supported telnet command.

       Example: telnet <IP address>, where ip-address is the IP address of the AnywhereUSB.
2. If the AnywhereUSB device requires a username and password, a login prompt is displayed. If the user name and password for the device are unknown, contact the system administrator who originally configured the device.
3. After you have successfully accessed the command line, the **#>** prompt is displayed.

Supported commands

To verify whether an AnywhereUSB supports a particular command, online help is available. For example:

- Typing help or ? displays all supported commands for a device.
- Typing set ? displays the syntax and options for the set command. Use this command to determine whether the device includes a particular "set" command variant to configure various features.
- Typing help set displays syntax and options for the set command.

The following table provides some common configuration commands for modifying settings on the AnywhereUSB.

To configure:	Use this command:
System-identifying information	set system
Host name	set host
Network options	set network
Network services	set service
Ethernet	set Ethernet
Users and passwords	set user and newpass

For more information about CLI commands, see the *Digi Connect Family Command Reference* on www.digi.com.

X.509 Certificate/Key Management

Use the X.509 Certificate/Key Management page to upload and manage entries in the database of certificate and private key data. This feature supports displaying, loading, saving, removing, certificate database entries, and importing a private key for the AnywhereUSB device into the database. Certificates and public/private host key pairs are an integral part of public key infrastructure (PKI) based security.

Supported security implementations

The X.509 Certificate/Key Management manages several kinds of certificate databases and security implementations, including:

- **X.509 Certificate Authority/Certificate Revocation**—A trusted third party issues digital certificates for use by other parties.
- **Secure Socket Layer (SSL)/Transport Layer Security (TLS)**—Use SSL and TLS security to secure access to web pages for configuration purposes, secure serial port connections, and SSL autoconnect, an automatic connection (autoconnection) between a serial port on the device and a remote network destination.
- **Secure Shell (SSHv2)**—Use SSHv2 to secure access to a device's console and serial ports for configuration purposes.

Benefits of certificates

You gain the following benefits when you use certificates to manage security:

- Certificates are more secure than Digi self-signed certificates.
- Certificate management allows you to push your own certificates out to the AnywhereUSB.
- The key sizes are more flexible.
- When you manage certificates through the web interface, it creates a repository of certificates that other applications and processes can use.

Additional information on certificate management

Implementing certificate management requires selecting a security type and understanding its technical details and key operations. If you are tasked with certificate management for your organization and need more background information, a good place to start is Wikipedia articles for the security types (X.509 CA/CRL, SCEP, VPN, SSL/TLS), and SSH). These articles reference resources such as standards, Request For Comments pages (RFCs), and articles that provide more technical detail.

Tables managed by the X.509 Certificate/Key Management feature

Certificate and key management information is stored in the following database tables:

Security type	Table	Used to load
X.509 Certificate Authority/Certificate Revocation	CA (Certificate Authority)	Certificate authority digital certificates. A certificate authority (CA) is a trusted third party that issues digital certificates for use by other parties. Digital certificates issued by the CA contain a public key. The certificate contains information about the individual or organization to which the public key belongs. A CA verifies digital certificate applicants' credentials. The CA certificate allows verification of digital certificates, and the information contained therein, issued by that CA.
	CRL (Certificate Revocation List)	Certificate revocation lists for loaded CAs. A certificate revocation list (CRL) is a file that contains the serial numbers of digital certificates issued by a CA which have been revoked, and should no longer be trusted. Like CAs, CRLs are a vital part of a public key infrastructure (PKI). You must install the digital certificate of the corresponding CA before you load the CRL.
Secure Sockets Layer (SSL) and Transport Layer Security (TLS)	SSL Identity	SSL/TLS identity certificates. A default key is generated automatically but can be overridden by a user. Note that this default key is not secure.
	SSL Identity Keys	SSL/TLS identity private keys.
	SSL Peer	SSL/TLS peer certificates.
	SSL Revoked	Verbatim revoked SSL/TLS certificates.
Secure Shell (SSHv2)	SSH Host Keys Table	SSHv2 identity private keys. Used for authentication with SSHv2 clients and secure key exchange. A default 1024-bit DSA key is generated automatically if none exists when the device boots. There is no certificate for SSHv2, just private key data.

Behavior of SSH/SSL private keys on the AnywhereUSB

AnywhereUSB devices generate their SSH/SSL self-signed private keys automatically. While this automatic generation is convenient for device users, as they are not required perform any actions regarding the private keys, it presents some security loopholes.

- With self-signed private keys, you must establish trust in a secure environment. That is, if you cannot guarantee that the environment is secure, you must pull the private keys off the AnywhereUSB.
- You must know about the certificate before you connect, as opposed to third-party signed certificates, where you only need the third-party certificate.

- The length of an AnywhereUSB device's self-signed private keys is 1024 bits. While this length is adequate for 99.9% of all applications, some people or applications prefer a shorter or longer key.

Using TFTP to load and store certificate information

Use TFTP to load and store PEM-formatted certificates into the certificate and private key management tables.

Using HTTP/HTTPS to transfer certificate and key data

You can use HTTP or HTTPS to transfer certificate and private key data on a web browser.

Data retained after factory reset

When you reset an AnywhereUSB to factory defaults, it retains certificates and private key data loaded onto it.

Certificate management settings

There are separate pages of settings for the certificate databases and key management for certificates and key data for the different types of security implementations.

Certificate Authorities (CAs) / Certificate Revocation Lists (CRLs)

Upload CAs and CRLs

Use this section to upload and manage certificate authority (CA) certificates, or certificate revocation list (CRL) files. You can install up to 8 CA certificates and up to 8 CA revocations. You can also obtain CA certificates from a SCEP server. You can install up to 8 SCEP CA certificates.

You an use files in ASN.1 DER or PEM Base64 encoded formats. Click Choose File and type or browse to the name of the file to upload. Click **Upload** to upload the file.

Installed Certificate Authority Certificates

The table lists any certificate authority certificates that are loaded in the Certificate Authority database.

- **Action**: Select to perform allowable actions on the entry. The only allowable action is to delete the entry.
- **Subject**: The entity that received the certificate. This is expressed as the value entered in a browser's URL field; typically a Fully Qualified Domain Name (FDQN) if using DNS or an IP address.
- **Issuer**: The entity that issued the certificate.
- **Expiration**: The expiration date of the certificate.

- **Delete** button: Click to delete the CA certificates selected in the Action column from the database.

Installed Certificate Authority Certificate Revocation Lists

The table lists any certificate authority certificate revocation lists that are loaded in the Certificate Revocation List database.

- **Action**: Select to perform allowable actions on the entry. The only allowable action is to delete the entry.
- **Issuer**: The entity that issued the certificate.
- **Last Update**: The last date and time the certificate revocation list was issued.
- **Next Update**: The effective or expiration date and time of the certificate revocation list. At this date, a new one must be obtained.
- **Delete** button: Click to delete the CA certificate revocation lists selected in the **Action** column from the database.

Secure Socket Layer (SSL) / Transport Layer Security (TLS) Certificates

Use the **Secure Sockets Layer (SSL) and Transport Layer Security (TLS) Certificates** page to load host certificates and keys, as well as peer certificates and revocations.

Identity certificates and keys

You can install up to two SSL/TLS identity certificates. You can also install up to 2 SSL/TLS identity keys.

Upload SSL/TLS Identity Keys and Certificates

Use this section to upload SSL/TLS RSA or DSA identity keys and certificates.

You can use identity certificate and key files in ASN.1 DER or PEM Base64 encoded formats.

Enter or browse to the name of the file to upload in the **Upload File** field. A password is required in the **Password** field only if the host key file is encrypted. Click **Upload** to upload the file.

Installed SSL and TLS Identity Certificates

This table lists the identity certificates that are installed in the SSL and TLS databases.

- **Action**: Select to perform allowable actions on the entry. The only allowable action is to delete the entry.
- **Subject**: The entity that received the certificate.
- **Issuer**: The entity that issued the certificate.
- **Expiration**: The expiration date of the certificate.

- **Matching Key**: The private key associated with the certificate, if any exists.
- **Delete** button: Deletes all certificates selected in the **Action** column from the database.

Installed SSL/TLS identity keys

This table lists the identity keys that are installed in the SSL and TLS databases.

- **Action**: Select to perform allowable actions on the entry. The only allowable action is to delete the entry.
- **Type**: The type of encryption of the identity key: RSA (public key cryptography algorithm) or DSA (digital signature algorithm).
- **Matching Certificate**: The certificate associated with the private key, if any exists.
- **Delete** button: Deletes all keys selected in the **Action** column from the database.

Trusted peer certificate

Use this section to upload and manage SSL and TLS trusted peer certificates.

Upload SSL/TLS trusted peer certificates

Use this section to upload SSL/TLS trusted peer certificates. Certificate files can be in ASN.1 DER or PEM Base64 encoded formats. Enter or browse to the name of the file to upload in the **Upload File** field. Click **Upload** to upload the file.

Installed SSL/TLS trusted peer certificates

This table lists the installed SSL and TLS trusted peer certificates. You can install up to 8 SSL/TLS trusted peer certificates.

- **Action**: Select to perform allowable actions on the entry. The only allowable action is to delete the entry.
- **Subject**: The entity that received the certificate.
- **Issuer**: The entity that issued the certificate.
- **Expiration**: The expiration date of the certificate.
- **Delete** button: Deletes all certificates selected in the **Action** column from the database.

Untrusted revoked certificate

Use this section to upload and manage SSL/TLS untrusted revoked certificates. You can install up to 8 SSL/TLS untrusted revoked certificates.

Upload SSL/TLS untrusted revoked certificates

Use this section to upload SSL/TLS untrusted revoked certificates. Certificate files can be in ASN.1 DER or PEM Base64 encoded formats. Enter or browse to the name of the file to upload in the **Upload File** field. Click the **Upload** button to upload the file.

Installed SSL/TLS untrusted revoked certificates

The table lists the installed SSL and TLS untrusted revoked certificates.

- **Action**: Select to perform allowable actions on the entry. The only allowable action is to delete the entry.
- **Subject**: The entity that received the certificate.
- **Issuer**: The entity that issued the certificate.
- **Expiration**: The expiration date of the certificate.
- **Delete** button: Deletes all certificates selected in the **Action** column from the database.

Secure Shell (SSH) Host Keys

Use the Secure Shell (SSH) Host Keys page to upload and manage SSH host keys.

Upload SSH Host Keys

Use this section to upload SSH RSA or DSA hostkeys. Key files can be in ASN.1 DER or PEM Base64 encoded formats. Enter or browse to the name of the file to upload in the **Upload File** field. A password is required in the **Password** field only if the host key file is encrypted. Click the **Upload** button to upload the file.

Installed SSH host keys

The table lists the installed SSH host keys. You can install up to 2 SSH host keys.

- **Action**: Select to perform allowable actions on the entry. The only allowable action is to delete the entry.
- **Type**: The type of encryption of the identity key: RSA (public key cryptography algorithm) or DSA (digital signature algorithm).
- **Fingerprint**: The fingerprint of the SSH host key. This fingerprint is in the form of a hash code consisting of several hexadecimal bytes to identify the SSH host key.
- **Delete** button: Deletes the selected SSH host keys in the **Action** column from the database.

Secure Shell (SSH) hostkeys

Use the **Secure Shell (SSHv2) Hostkeys database** to load host private keys. You can use SSHv2 host keys for authentication with SSHv2 clients and secure key exchange. The AnywhereUSB automatically generates a default 1024-bit DSA key if none exists when the device boots.

- **Upload SSH Host Keys**: Use this section to upload SSH RSA or DSA hostkeys. Key files may be in ASN.1 DER or PEM Base64 encoded formats. If the host key file is encrypted, a password is required.
- **Installed SSH Host Keys**: Lists the host keys loaded into the SSH Hostkeys database.

Troubleshooting

The following information provides troubleshooting steps for the most common issues. To find information on other issues, visit our Knowledge Base at knowledge.digi.com.

Basic troubleshooting steps

Follow these basic troubleshooting steps first:

- Make sure you have the most current driver and firmware installed for your AnywhereUSB model and USB devices.
- Make sure each USB device has the most current drivers installed.
- Make sure the USB device works as expected using a native USB port by connecting the USB device directly to the computer instead of through an AnywhereUSB.
- Try the "Use Microsoft IDs" AnywhereUSB option; see the Understanding the “Use Microsoft IDs” AnywhereUSB feature Knowledge Base article.

AnywhereUSB error when connecting on a virtual machine

When the AnywhereUSB status says “Connected to this computer” but shows a warning icon with error code 39 in Device Manager, the virtual machine might be missing the necessary USB drivers.

The virtual machine must have a USBD.SY_ or usbd.sys file located in the ...\system32\drivers folder. If this file is missing, do the following:

1. Make sure Windows is configured to show file extensions.

   Windows XP

   a. Open **My Computer**, select **Tools > Folder Options**, and click the **View** tab.

   b. Scroll down and clear the **Hide extensions for known file types** check box and click **OK**.

   For Windows 7 and Server 2008

   a. Open **Computer** and select **Organize > Folder and Search Options**.

   b. Click the **View** tab.

   c. Scroll down and clear the **Hide extensions for known file types** check box and click **OK**.

2. On the Windows virtual machine drive, search for the usbd.sys file.

   The exact location of this file depends on the Windows operating system version:

   - XP 32-bit: i386 folder
   - XP 64-bit: IA64 folder
   - Server 2003: i386 folder
   - Server 2003 R2: i386\DRIVER.CAB
   - Server 2008: sources\install.wim\5\Windows\System32\drivers\
   - Vista: sources\install.wim\5\Windows\System32\drivers\
   - Windows 7: sources\install.wim\4\Windows\System32\drivers\

   Note For newer operating systems with the install.wim file, we recommend using software such as 7-Zip to browse the contents of the install.wim file to locate the USBD.SY_ or usbd.sys file.

3. Copy the USBD.SY_ or usbd.sys file and paste it in the ...\system32\drivers folder on the virtual machine. If you are copying the USBD.SY_ file, rename it to usbd.sys. Make sure to paste it in the drivers subfolder, not system32.
4. Restart the virtual machine.
5. After Windows loads, the AnywhereUSB Host Controller(s) and AnywhereUSB/RealPortUSB Root Hub(s) component(s) should automatically install and appear in Device Manager.

AnywhereUSB USB device compatibility list

The AnywhereUSB is a network-attached USB 2.0 hub. While any USB device should work, there are some limitations. Use the following information to make sure your USB device is compatible with AnywhereUSB.

Note USB 2.0 support was introduced in AnywhereUSB firmware v1.51 for the AnywhereUSB/5 (G2), AnywhereUSB/5 M, AnywhereUSB/5 (G2) TS-44, and AnywhereUSB/14 models. The AnywhereUSB/2 model introduced USB 2.0 support in firmware v1.60. All previous firmware versions are USB 1.1. The first generation AnywhereUSB/5 supports only USB 1.1.

Compatible USB devices

The following list provides some of the USB devices that are compatible with the AnywhereUSB that we recommend and support, but it is not a complete list:

- USB license dongles, also known as security keys or license keys. All brands work, such as SafeNet, WIBU, Rockey4, Aladdin, HASP, and so on
- USB printers, scanners, or multi-function devices
- USB HID (human interface device), such as mice, keyboards, barcode scanners, and magnetic strip card readers
- USB hubs, such as the Digi Hubport product line
- USB-to-serial converters, such as the Digi Edgeport product line
- Digi Rapidport modem bank
- Digi Watchport USB cameras
- Other bulk or interrupt (per USB spec) type USB devices
- Lab style instruments
- Smartphones

Limited support USB devices

The following USB devices have limited support with the AnywhereUSB. We do not recommend using these devices, because they have limited testing. However, they may work for your application.

- USB mass storage devices, such as flash drives and hard drives

Note These devices should enumerate, possibly slower than expected, and might have a noticeable performance decrease compared to a native USB port. Expect transfer rates at about 4-6 Mbit/sec due to various considerations, such as network overhead.

Incompatible USB devices

The following USB devices are incompatible with the AnywhereUSB. We do not recommend or support using them:

- "Isochronous" (per USB spec) devices. Check the spec sheet of the USB device or contact the vendor to determine if a device uses the "isochronous" USB transfer type
- USB audio devices, such as sound cards
- Video streaming devices, such as webcams, except for the Digi Watchport USB cameras
- USB Modems, except for the Digi Rapidport modem bank

USB modems

If you need to use a USB modem, we suggest using a Digi Edgeport USB-to-serial converter with a RS-232 serial modem, which we have successfully tested. Although any serial modem should work, we specifically recommend MultiTech 5634ZBA, US Robotics 5686 based on positive feedback from customers. Some customers have also reported success with US Robotics USR5637 and Multi-Tech MT9234-CDC-XR USB modems, though they are not supported because Digi has not yet tested these devices.

No remote hubs found

The “No remote hubs found” message appearing on the left side of the AnywhereUSB Remote Hub Configuration Utility indicates that the host computer is unable to discover any AnywhereUSB devices on the network.

This message appears when firewall software blocks the port used for device discovery. Try the following:

- For firewall software, either disable it or add an exception for the port.
- Check for a link light on the AnywhereUSB Ethernet port. If the link light is not lit, connect all of the AnywhereUSB devices to switches using network cables.
- Connect the AnywhereUSB device directly to the host computer.
  - First generation AnywhereUSB/5: You must use a crossover network cable to connect first generation AnywhereUSB/5 devices to the host computer.
  - Second generation AnywhereUSB devices: Use the auto-sensing network interface on the second generation AnywhereUSB models to connect to the host computer,
- If the host computer has multiple network interfaces, disable the network interfaces that are not on the same network as the AnywhereUSB device. Then close and re-launch the AnywhereUSB Remote Hub Configuration Utility.
- By default, the AnywhereUSB Remote Hub Configuration Utility only searches the local subnet for AnywhereUSB devices. If the AnywhereUSB device is on a different subnet, you must configure the AnywhereUSB Remote Hub Configuration Utility to look on the other subnet:

  a. Use the Device Discovery Utility to determine the AnywhereUSB device IP settings (for all models except the first generation AnywhereUSB/5).
  b. In the AnywhereUSB Remote Hub Configuration Utility, click Edit / Discovery List and either add the AnywhereUSB IP address or add the other subnet in question, such as192.168.1.255.

- Some anti-virus software might block the connection. You can either temporarily disable it or add an exception for the AnywhereUSB Remote Hub Configuration Utility executable:
  - For 32-bit operating systems, allow AwUsbCfg.exe.
  - For 64-bit operating systems, allow AwUsbCfg64.exe.
- For first generation AnywhereUSB/5 devices: If the System Status LED is solid orange and all five port LEDs are off, the device is configured with the DHCP client enabled and is unable to obtain an IP address. Perform a factory reset. See the AnywhereUSB factory reset feature Knowledge Base article.

USB license dongle cannot be found

Try these suggestions in the following order:

1. Make sure the license information on the dongle has not expired, contact the appropriate dongle/software vendor.
2. Make sure the USB license dongle is functioning correctly:
   a. Connect it directly to a physical computer (not to an AnywhereUSB device).
   b. Install the proper dongle driver and confirm that the dongle is installed properly by checking Windows Device Manager.
   c. If you have software to test the dongle, run the software to make sure the dongle is working properly. If the dongle does not work, it will likely not work with an AnywhereUSB device.
3. Make sure that another USB device works on the same AnywhereUSB port, such as a USB keyboard or mouse.
4. Make sure that you are running the most current AnywhereUSB driver and firmware versions on the host computer.
5. Make sure the computer has the most current dongle driver version.
6. Start the AnywhereUSB Remote Hub Configuration Utility and do the following:
   a. Select **File > Preferences.**
   b. Select the **Use Microsoft Device IDs** check box, and click **Save**.
   c. Disconnect from the AnywhereUSB device then re-connect to the device.
7. If you are launching the protected software from a computer connected through a Windows Remote Desktop Session, you need to use the console option instead to connect directly to the computer and then run the software.

8. Add the dongle as a permitted device based on its PID/VID, as follows:
    a. Open the **AnywhereUSB Viewer Utility**.
    b. In the AnywhereUSB program group, select the USB device and make note of the VID (Vendor ID) and PID (Product ID) of that device. Each ID should be four characters, in HEX format, such as 0x1234. Ignore the leading 0x when taking note of the values.
    c. Using the Windows Registry Editor, go to HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\ionhub.
    d. With ionhub selected, select **Edit > New > Multi-String Value**.
    e. Rename the new value to PermittedDevices (case sensitive).
    f. Double-click **PermittedDevices** and in the **Value** data field, type Vid_1234&Pid_5678 (where 1234 is the Vendor ID and 5678 is the Product ID of the USB device).
    g. Click **OK** and close Registry Editor.
    h. Restart the host computer.
9. Disable Windows Data Execution Prevention.
10. If the parallel port is not used, disable it in the host computer's BIOS.

Note A virtual machine has a BIOS. When the computer running the virtual machine does not have a physical parallel port, the option might be in the BIOS of the virtual machine.

For details, see Appendix A: AnywhereUSB permitted device list.

Connecting to this computer message

When a device remains in the "Connecting to this computer" state in the AnywhereUSB Remote Hub Configuration Utility. The following are the most common causes.

Firewall software

Firewall software, such as Windows Firewall, may be blocking port 3422 TCP that the AnywhereUSB uses. Either add this port as an exception or disable the firewall software.

Windows New Hardware Wizard

The Windows New Hardware Wizard did not open when you connected the AnywhereUSB device. To resolve this issue:

1. Open **Device Manager** and find AnywhereUSB-related components that have a warning icon.
2. Right-click the components that have the warning icon and click **Update Driver**.
3. Complete the installation procedure.
4. Repeat this process as needed for all AnywhereUSB-related components in Device Manager that have warning icons.

AnywhereUSB is connected to a different computer

The AnywhereUSB may already be connected, or trying to connect, to a different computer. This applies only to AnywhereUSB models that connect all of the USB ports to a single host computer, such as legacy AnywhereUSB/5, AnywhereUSB/2, AnywhereUSB/5 (G2), and AnywhereUSB TS44 devices. To resolve this issue:

1. Open the **AnywhereUSB Remote Hub Configuration Utility**.
2. Select **Edit > Connect List**.
3. Delete the IP address of the affected AnywhereUSB device and close the Connection List.
4. Make note of the deleted device’s status in the Host PC Connection Status window and do the following:
   - Status is "Connected to (IP address)": The AnywhereUSB is already connected to a different host computer. First, disconnect from the other host computer by removing the AnywhereUSB device's IP address from the Connection List. Then reconnect the device to the desired host computer.
   - Status is "Available for Host Connection": There is another issue that is causing the problem. Contact Digi Technical Support for assistance.

Check the network configuration

If the AnywhereUSB is configured with a static IP address (with the DHCP client disabled), check the following:

- Determine if the AnywhereUSB's Static IP address is in use by another device on the network by disconnecting the network cable from the AnywhereUSB device, then try to ping that same IP address from the host computer. If you get a ping reply, then another device on the network is using the same IP address.

  Note Using ping may not provide reliable results because not all devices respond to this command. We recommend configuring the AnywhereUSB device with a different static IP address that is outside of the DHCP range if a DHCP server is on the network.

- Make sure the subnet mask is correct.
- Make sure the host computer’s IP address is correct, especially when configured with a static IP address.
- Make sure the host computer’s network configuration is properly configured so it communicates with the AnywhereUSB device. Also, make sure they are both on the same subnet.
- Ping the AnywhereUSB device. If you do not get a response, then you will not be able to connect to the device.

Reinstall the AnywhereUSB software

If none of the troubleshooting suggestions help, uninstall the AnywhereUSB software, reboot the host computer, re-install the AnywhereUSB software (with admin privileges), and connect to the AnywhereUSB again.

Regulatory and safety information

GOST certification

Safety information

Продукция соответствует требованиям нормативных документов:

ГОСТ Р МЭК 60950-1-2009, ГОСТ Р 51318.22-99, ГОСТ Р 51318.24-99, ГОСТ Р 51317.3.2-2006 (Разд. 6, 7), ГОСТ Р 51317.3.3-2008

Transitional CoC No + issuing/expiration dates

№. РОСС US.MH08.B02068

Срок действия с 14.02.2013 по 13.02.2014

Address and phone of service facility

Digi International Inc. 10000 West 76th Street, Eden Prairie, MN 55344, США

Address and phone of service facility

Digi International Inc. 10000 West 76th Street, Eden Prairie, MN 55344, США

⚠ **WARNING!** For the AnywhereUSB/14 only: HAZARDOUS VOLTAGE INSIDE. Before servicing any device, make sure the power is disconnected.

Appendix A: AnywhereUSB permitted device list

About the permitted device list

An option has been added to the AnywhereUSB product that limits access to a set of select devices. This option allows an administrator to build a list of supported devices by adding specific Vendor ID/Product ID or Class values into the registry. The AnywhereUSB will compare the IDs of each USB device (when the USB device is connected), with the value(s) in the registry and if there is a match, the device will enumerate; otherwise an “unknown device” message will appear in the Notification Area.

The key is located in this location:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\ionhub
```

The new key value is PermittedDevices. This Multi String value contains a list of devices that the AnywhereUSB will enumerate all other devices will show as "unknown device."

Examples

Following are some examples of values in the permitted device list:

- For a hub, use the value GENERICHUB (Class_09 is not supported).
- For a composite device, use the value COMPOSITE.
- For specific device, use Vid_xxxx&Pid_yyyy where xxxx and yyyy are the vendor id and product ID of the device.
- For a device class such as mass storage, use Class_xx where xx is the class of device. Classes are as follows:
  - Communications: 02
  - Human interface: 03
  - Printer: 07
  - Storage: 08
  - Vendor Specific: FF

Configure the permitted device list

To allow a specific USB device with an embedded hub, such as an Edgeport/8:

```
PermittedDevices REG_MULTI_SZ Vid_1608&Pid_0215 GENERICHUB
```

To allow all human interface devices such as mouse or keyboard:

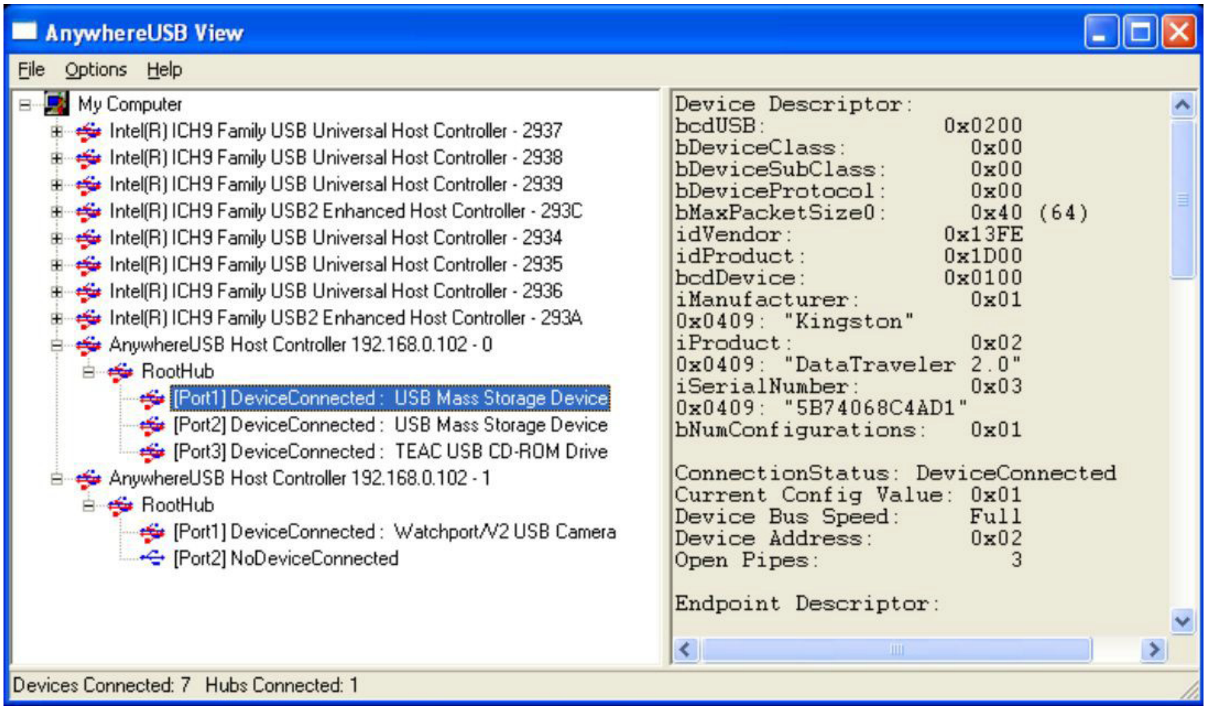
```
PermittedDevices REG_MULTI_SZ Class_03
```

To allow all mice and all printers:

PermittedDevices REG_MULTI_SZ Class_03 Class_07

Use the AnywhereUSB View utility to see the USB device's Vid/Pid values. The fields are called idVendor and idProduct. In the following example, the highlighted USB flash drive has the following properties:

- idVendor: 0x13FE
- idProduct: 0x1D00



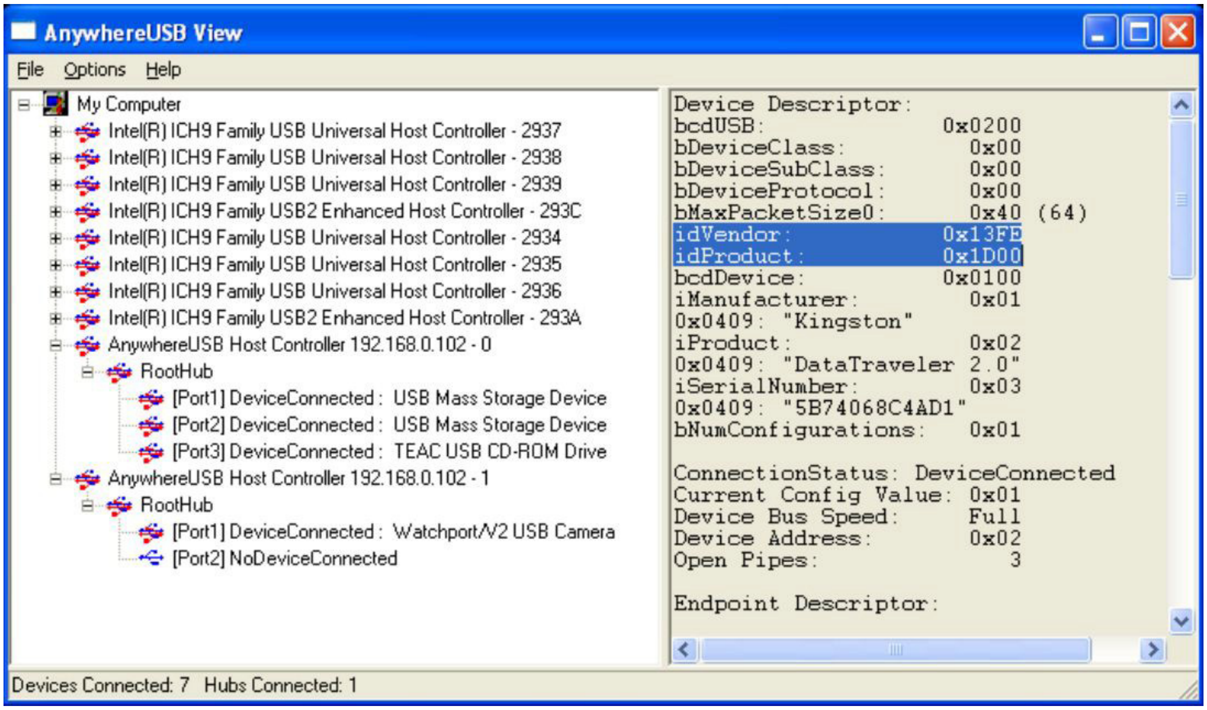
```
My Computer
  Intel(R) ICH9 Family USB Universal Host Controller - 2937
  Intel(R) ICH9 Family USB Universal Host Controller - 2938
  Intel(R) ICH9 Family USB Universal Host Controller - 2939
  Intel(R) ICH9 Family USB2 Enhanced Host Controller - 293C
  Intel(R) ICH9 Family USB Universal Host Controller - 2934
  Intel(R) ICH9 Family USB Universal Host Controller - 2935
  Intel(R) ICH9 Family USB Universal Host Controller - 2936
  Intel(R) ICH9 Family USB2 Enhanced Host Controller - 293A
  AnywhereUSB Host Controller 192.168.0.102 - 0
    RootHub
      [Port1] DeviceConnected :  USB Mass Storage Device
      [Port2] DeviceConnected :  USB Mass Storage Device
      [Port3] DeviceConnected :  TEAC USB CD-ROM Drive
  AnywhereUSB Host Controller 192.168.0.102 - 1
    RootHub
      [Port1] DeviceConnected :  Watchport/V2 USB Camera
      [Port2] NoDeviceConnected
```

```
Device Descriptor:
bcdUSB:             0x0200
bDeviceClass:         0x00
bDeviceSubClass:      0x00
bDeviceProtocol:      0x00
bMaxPacketSize0:      0x40 (64)
idVendor:           0x13FE
idProduct:          0x1D00
bcdDevice:          0x0100
iManufacturer:        0x01
0x0409: "Kingston"
iProduct:             0x02
0x0409: "DataTraveler 2.0"
iSerialNumber:        0x03
0x0409: "5B74068C4AD1"
bNumConfigurations:   0x01

ConnectionStatus: DeviceConnected
Current Config Value: 0x01
Device Bus Speed:     Full
Device Address:       0x02
Open Pipes:              3

Endpoint Descriptor:
```

Devices Connected: 7   Hubs Connected: 1



```
My Computer
  Intel(R) ICH9 Family USB Universal Host Controller - 2937
  Intel(R) ICH9 Family USB Universal Host Controller - 2938
  Intel(R) ICH9 Family USB Universal Host Controller - 2939
  Intel(R) ICH9 Family USB2 Enhanced Host Controller - 293C
  Intel(R) ICH9 Family USB Universal Host Controller - 2934
  Intel(R) ICH9 Family USB Universal Host Controller - 2935
  Intel(R) ICH9 Family USB Universal Host Controller - 2936
  Intel(R) ICH9 Family USB2 Enhanced Host Controller - 293A
  AnywhereUSB Host Controller 192.168.0.102 - 0
    RootHub
      [Port1] DeviceConnected : USB Mass Storage Device
      [Port2] DeviceConnected : USB Mass Storage Device
      [Port3] DeviceConnected : TEAC USB CD-ROM Drive
  AnywhereUSB Host Controller 192.168.0.102 - 1
    RootHub
      [Port1] DeviceConnected : Watchport/V2 USB Camera
      [Port2] NoDeviceConnected
```

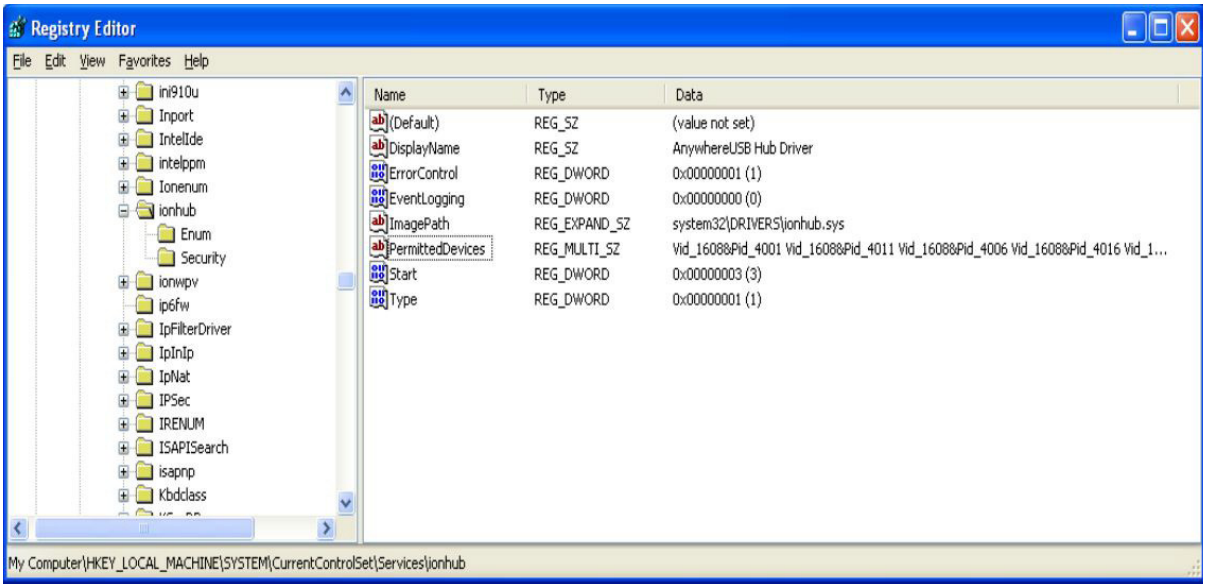
```
Device Descriptor:
bcdUSB:              0x0200
bDeviceClass:          0x00
bDeviceSubClass:       0x00
bDeviceProtocol:       0x00
bMaxPacketSize0:       0x40 (64)
idVendor:            0x13FE
idProduct:           0x1D00
bcdDevice:           0x0100
iManufacturer:         0x01
0x0409: "Kingston"
iProduct:              0x02
0x0409: "DataTraveler 2.0"
iSerialNumber:         0x03
0x0409: "5B74068C4AD1"
bNumConfigurations:    0x01

ConnectionStatus: DeviceConnected
Current Config Value:  0x01
Device Bus Speed:      Full
Device Address:        0x02
Open Pipes:               3

Endpoint Descriptor:
```

Devices Connected: 7 Hubs Connected: 1

The following is a view of the registry with the new Key of "PermittedDevices":

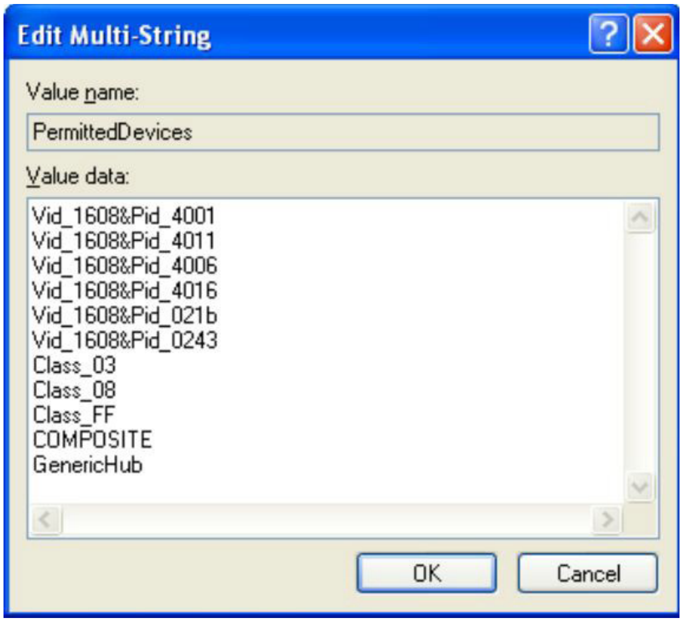


```
ini910u
Inport
IntelIde
intelppm
Ionenum
ionhub
  Enum
  Security
ionwpv
ip6fw
IpFilterDriver
IpInIp
IpNat
IPSec
IRENUM
ISAPISearch
isapnp
Kbdclass
```

Name	Type	Data
(Default)	REG_SZ	(value not set)
DisplayName	REG_SZ	AnywhereUSB Hub Driver
ErrorControl	REG_DWORD	0x00000001 (1)
EventLogging	REG_DWORD	0x00000000 (0)
ImagePath	REG_EXPAND_SZ	system32\DRIVERS\ionhub.sys
PermittedDevices	REG_MULTI_SZ	Vid_1608&Pid_4001 Vid_1608&Pid_4011 Vid_1608&Pid_4006 Vid_1608&Pid_4016 Vid_1...
Start	REG_DWORD	0x00000003 (3)
Type	REG_DWORD	0x00000001 (1)

My Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\ionhub

Double-clicking on the key will bring up the Edit Multi-String dialog.



Value name:

PermittedDevices

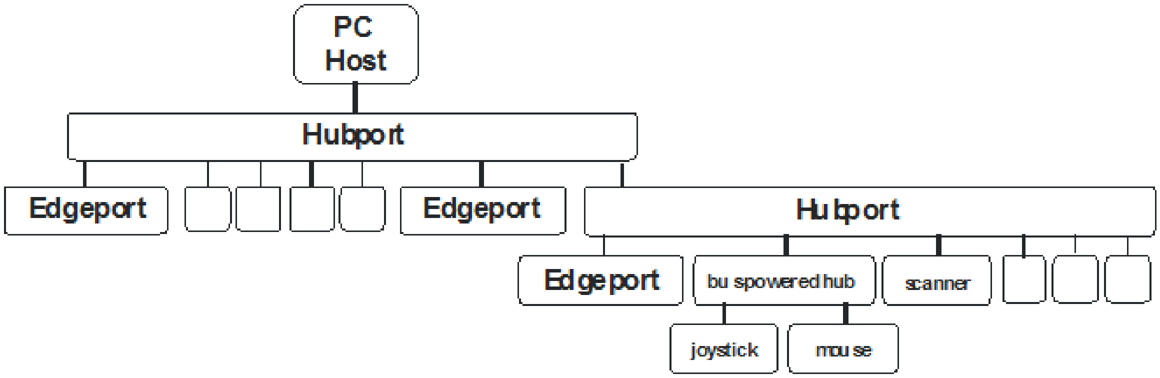
Value data:

```
Vid_1608&Pid_4001
Vid_1608&Pid_4011
Vid_1608&Pid_4006
Vid_1608&Pid_4016
Vid_1608&Pid_021b
Vid_1608&Pid_0243
Class_03
Class_08
Class_FF
COMPOSITE
GenericHub
```

Appendix B: Understanding hubs

About hubs

Hubs are critical components in the plug-and-play architecture. They are wiring concentrators that enable the attachment of multiple devices, thus converting a single attachment point into multiple attachment points. USB architecture allows a cascaded multiple hub configuration with certain power limitations (explained later in this section). The figure below shows an example of a typical hub configuration.



Upstream and downstream ports

Each hub has an upstream port, connecting to the host, and multiple downstream ports, connecting to downstream devices, including other hubs. A hub can detect attachment and detachment of downstream devices and enable and monitor the distribution of the power to downstream devices via their integral hardware and the operating system.

Power requirements

Each USB device reports its power requirements to the operating system, which then enables and disables the device as a function of its power requirements and the amount of available power. High-speed devices typically connect to a self-powered hub, which obtains power from its external power supply and provides up to 500 mA for each downstream port. Connect only simple devices, such as a mouse, to a bus-powered hub, which obtains power from its upstream host and provides up to 100 mA for each downstream port.

Due to the limited available power for bus-powered hubs, cascading two bus-powered hubs is an illegal topology, and devices connected to the second hub will not function. (USB specifications limit the connection of a bus-powered hub to a self-powered hub or host only.)

Series limits

According to the USB Specification, the maximum limit of hubs cascaded in series cannot exceed five. In other words, you may have a maximum of five hubs between any device and the host. This does not mean that the maximum number of hubs in a system is five. Connect up to seven parallel hubs at any given level. You must tally both external and embedded hubs when counting downstream hubs.

Appendix C: Firewall support

Configure for firewall support

To access an AnywhereUSB that is behind a firewall:

- Your firewall must have a well-known static IP address, for example: 10.52.48.37
- The AnywhereUSB must have an IP address on the private subnet, for example, 192.189.1.10
- You must configure your firewall to allow TCP/IP and UDP/IP packets to pass through port 3422
- You must configure the firewall to send these TCP/IP and UDP/IP packets directed to the IP address of the AnywhereUSB; in this example the address would be 192.188.1.10.
- You must manually add the address of the firewall to the Connection List.

Note You can access only one AnywhereUSB through each firewall.

For more information on how to configure your firewall, refer to your firewall manual.

If you would like AnywhereUSB information in the discovery window of the AnywhereUSB Remote Hub Configuration Utility, you can add the address of the firewall into the Discovery List.

Note AnywhereUSB devices behind firewalls, as displayed in the discovery window, who the UP address of their private network.