



Secured Protocols with the Galaxy Pulsar Edge Controller

Introduction

The Galaxy Pulsar Edge controller is the first of GE Critical Power DC Systems' controllers to receive the software enhancements for secured protocol support. Initial Secured protocols include support for the SNMPv3, IPv6, HTTPS/SSL, SSH, and SFTP protocols. These protocols will migrate into the Galaxy Pulsar Plus and Galaxy Millennium II controllers over the next few quarters. Versions of the Galaxy Pulsar Edge are currently shipping with SNMPv3 and IPV6. HTTPS/SSL, SSH, and SFTP will be released Q4 2014. This document briefly describes use of this feature set for the Galaxy Pulsar Edge which will represent similar operation in the other controllers. This document will be a working document and updated over time.

The implementation of these secured protocols required a hardware upgrade to the Pulsar Edge mother board. Thus, the existing standard Pulsar Edge controllers cannot be upgraded with this new software containing support for these secured features due to their existing memory capacity limitations. However, the enhanced hardware for the Galaxy Pulsar Edge upgrade is designed and assembled in the same form factors as its predecessors so that easy field and factory replacement upgrades can be made. The Galaxy Pulsar Plus has the same memory limitation and also requires a hardware upgrade. Thus, the same software incompatibility exists in the Galaxy Pulsar Plus but the enhanced hardware is again packaged in the same form-factors providing the easy upgrade or replacement path. The Galaxy Millennium 2 is an exception. Its hardware contains the necessary memory and can be updated to the latest software that supports the secured protocols in the near future.

The enhanced Galaxy Pulsar Edge controllers are identified by new part numbers (comcodes) and a trailing "S" extension in its naming nomenclature. Similarly, the application and web firmware have been identified with "sec" (for "secure") embedded in the file names for identification, e.g. cp841a-sec-app.bin and cp841a-sec-pages.web.

As a reference, the following table provides the basic naming nomenclature utilized for the different Pulsar Edge controller configurations.

Table 1 Pulsar Edge Family Naming Convention

ZZZ 841 A_nW mR_XXX_S_YYY	
Where:	
ZZZ	Identifies the product family of Pulsar Edge controller. (Valid IDs are CP, GCP, SPS, QS, and NE)
A	This identifies the controller form factor option (A or E = Shelf Mount, D = Panel Mount)
nW mR	Identifies the input/output hardware configuration ¹ for the controller. “nW” identifies the inputs and how they are configured. The first digit, “n”, represents the number of inputs (0 through 9). The second digit, “W”, represents the type of return provided for these inputs (I=Individual Returns, C = Common Return). “mR” identifies the alarm outputs. The first digit, “m”, represents the number of outputs present (0 through 5). The second digit is R (for Relay).
XXX	Identifies the front panel Craft port interface option installed (Blank = standard DB9 female interface, RJ= Standard TIA RJ45, RJC = Cisco RJ45, D = Mini USB with Display, DS = Mini USB with Display)
S	Identifies Secured Protocols ² option installed. (Blank = Standard, S = Secure Protocols)
YYY	Identifies a customer or application specific software configuration version of the controller (Blank = Standard). These codes are specifically assigned to an application where defaults are clearly predefined to minimize field configuration and error. Consult appropriate sales personnel for additional information.

Examples of controllers with the secured protocols are shown in the table that follows.

Table 2: Secured Protocol Galaxy Pulsar Edge Example Codes

Part Comcode	Controller Part Number
150041556	NE841E_0I6R_USB_S
150039541	NE841E_3C3R_USB_S
150032047	CP841A_3C3R_S
150036348	NE841E_0I6R_USB_DS

US Export Classification

EAR99, ECCN 5D992

¹ There is a dependency on the number of outputs and inputs.

² Secure Protocols include SNMPv3, IPv6, and HTTPS/SSH/SFTP.

General

This document describes the use of these protocols from a basic configuration perspective using the web pages.

Once logged into the controller's web interface the majority of features, thresholds, and options can be configured by accessing the "Settings" tab (screen shot below). Almost all standard configuration changes take effect without the controller requiring a reboot. Configuration changes involving IP addresses and protocol operational mode variable items do require a reboot. In both cases, it is necessary to allow the controller to run for at least a minute and a half following a saved change to ensure the change has been saved to non-volatile memory before powering the unit down or any rebooting operation. This delay allows sufficient time for all saved changes to be written to non-volatile storage.

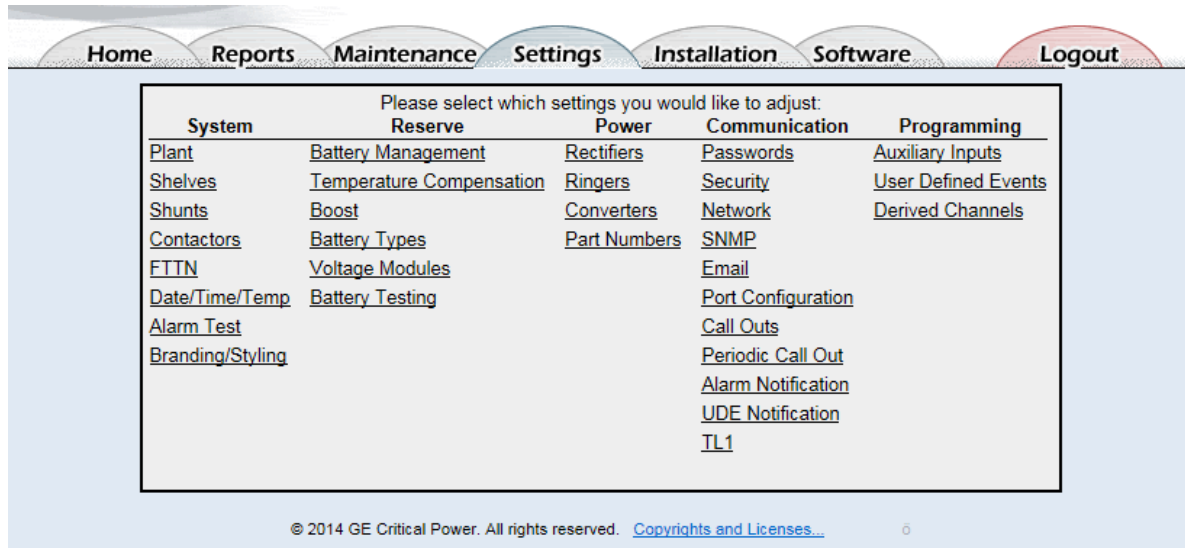


Figure 1: Configuration Page For All Settings

Security

One of the applicable configuration screens associated with secured protocols is the "Security" found in *Settings* ► *Communication* ► *Security*. The Security page allows the user to configure various access related features including network related items. For security reasons these fields can only be modified when logged in with Administrative access. The network related items are:

- Port behavior on failed login attempts (number of failed attempts allowed value of 3-10 attempts, time to lock the port value 0 to 5 minutes 1 minute increments).
- Password rules to encourage the use of strong passwords. These include minimum password length (3 to 15 characters) and requirements for the inclusion of different types of characters (≥ one upper case, ≥ one lower case, ≥ one number, and ≥ one special character).
- Individual protocol (network ports) enables to allow the blocking of non-secure protocols

Figure 2: Security Configuration Page

NOTE: Depending on the factory default settings for the controller, unsecured network ports may be disabled.

Internet Protocols (IPv4 And IPv6)

IPv4

The Galaxy Pulsar Edge controller is capable of simultaneous operation using IPv4 and IPv6 protocols. Using IPv4, the controller will utilize a single IPv4 address. This address will be assigned in one of 3 ways depending on the DHCP mode:

1. **DHCP mode Static:** In this configured mode, the Galaxy Pulsar Edge uses a static IPv4 address assigned by the user. The user must supply a subnet mask and a router address.
2. **DHCP mode Client:** In this configured mode, the Galaxy Pulsar Edge controller uses a dynamic IPv4 address assigned by a DHCP server on the network.
3. **DHCP mode Server:** : In this configured mode, the Galaxy Pulsar Edge controller will automatically assign a predefined IPv4 address of 192.168.2.11 to a PC plugged directly into its network port connection. For this reason, the controller MUST NOT be connected to a network while operating in this mode.

Following is an example of the configuration web screen for configuring the IP information. It is found in *Settings ► Network Settings*. The screen is parsed for IPv6 and IPv4 related settings. The Static DHCP mode is selected in the IPv4 section of the given example. The basic required parameter settings for IPv4 (Static IP address, Subnet Mask, and Default Gateway Router IP address) are configured.

The screenshot shows the 'Network Settings' web page. At the top is a navigation bar with links: Home, Reports, Maintenance, Settings, Installation, Software, and Logout. The main content area is titled 'Network Settings' and is divided into two sections: IPv6 and IPv4.

IPv6 Section:

- Current IPv6 Address: 2001:db8:1:2f80:21f4bff:fe00:7027
- Link Local IPv6 Address: fe80::21f4bff:fe00:7027
- Static IPv6 Address: 2001:db8:1:2f80:21f4bff:fe00:7029
- IPv6 Prefix Length: 64
- IPv6 Working Gateway Address: fe80::21d:70ff:feab:e6a1
- IPv6 Static Gateway/Router Address: ::

IPv4 Section:

- Network Port 1**
- Current IP Address: 172.16.10.23
- DHCP: Static Address (dropdown)
- Static IP Address: 172.16.10.23
- Subnet Mask: 255.255.255.0
- Default Gateway/Router: 172.16.10.254
- Domain Name: pwsyst.com
- DNS Server: 0.0.0.0
- Host Name:
- Write Enabled: yes
- Mail Host: 0.0.0.0
- Send Message As:
- Session Timeout: 10 (dropdown) 1-1440 minutes

A 'Submit' button is located at the bottom of the IPv4 section.

Figure 3: Network Settings Page For IPv4 And IPv6

IPv6

The enhanced Galaxy Pulsar Edge supports IPv6. Operating with IPv6, the Edge controller can have multiple IPv6 addresses. It can have Link Local Address and multiple Global Unicast Addresses. These items are shown in the top section of the *Settings ► Network Settings* web screen.

The Galaxy Pulsar Edge controller will have a single Link Local address. This Link Local address is automatically generated by the controller based on its MAC address. It is displayed in the *Settings ► Network Settings* web screen. The link local address can only be used on the local link (subnet) and will not be routed through the network. Browsers will not accept a link local address in a URL.

The controller may also have one or more Global Unicast Address. One of these addresses can be manually entered by the user. Entry of this IPv6 address is in the "Static IPv6 Address" field shown. Another Global address can be automatically generated by the controller using the SLAAC protocol. The SLAAC protocol allows routers to send a router advertisement messages. These messages will supply the router address, the link prefix (subnet) and network options. One of these network options, the autonomous address-configuration flag, will instruct the controller to generate a Global Unicast Address based on the router prefix and the controller's MAC address. This IPv6 address is displayed as the "Current IPv6 Address".

HTTPS (SSL)

The enhanced Secured Galaxy Pulsar Edge controller supports the Hyper-Text Transfer Protocol with SSL Encryption. It is capable of supporting browser access using HTTP and HTTPS. The standard controller is shipped with HTTP enabled and HTTPS disabled. However, specific customer configurations requiring only secured protocols will have HTTP access disabled and HTTPS access enabled. The desired HTTP protocol access is selected by prepending the URL address with the respective "http://" or "https://" to in the browser. If the Galaxy Pulsar Edge controller is accessed using its IPv4 address with HTTPS, the browser will issue a screen indicating a problem with the website's security certificate as shown below.

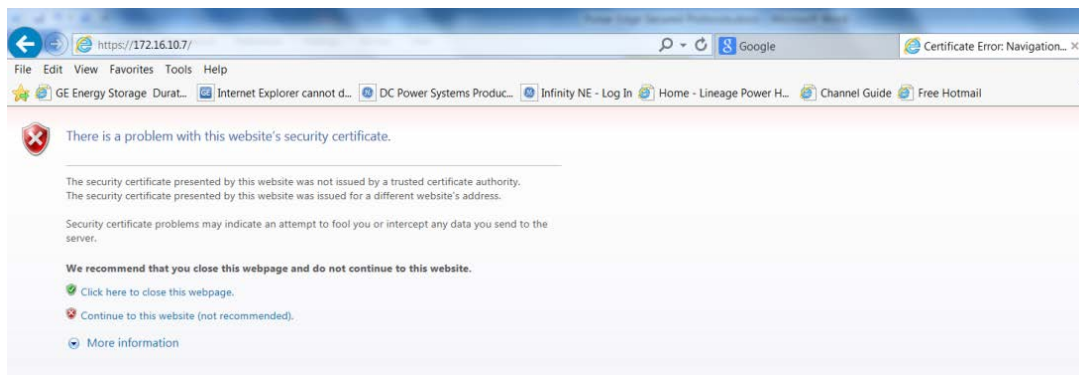


Figure 4: Security Problem Screen Using Explorer

In this case, select "Continue to this website (not recommended)" and the controller login page will be presented. Continue to Login into the controller using the appropriate passwords (lineage, super-user, and administrator by default). The browser will complain about a mismatched address in the certificate if the controller is accessed using its IPv4 address for HTTPS. Clicking on the Certificate error page shows the error as seen below. The controller will be fully accessible using IPv4 and HTTPS with this mismatched address.



Figure 5: Mismatched Address Certificate Error Screen

To enable HTTPS connectivity to the controller without browser warnings in IPv6 the following procedures must be followed:

1. Contact GE Critical Power at the 24/7 technical support contacts at either pe.techsupport@ge.com, <http://www.geindustrial.com/critical-power-technical-support> or 1-877-546-3243 or 1-972-244-9288 (DC Systems Option 2) for the certificate file.
2. Change the file extension to ".crt"
3. Right click on the certificate file ASDC_2048.crt and select: "Install Certificate"
4. When prompted select: "Place all certificates in the following store"
5. Browse to select: "Trusted root certification authorities"

The device certificate created by the controller identifies the controller by its IPv6 address. Whenever the IP address of a controller is changed, it is necessary to reboot the controller. Allow about a minute and a half for all the changes to be stored prior to rebooting. Upon reboot, the controller will create a device certificate for the new IP address. This process may take several minutes. Now the "https:" prepended URL can be used to access error free connection. Note: an IPv6 address must be enclosed in [] when in a URL. Sample web screen follows.

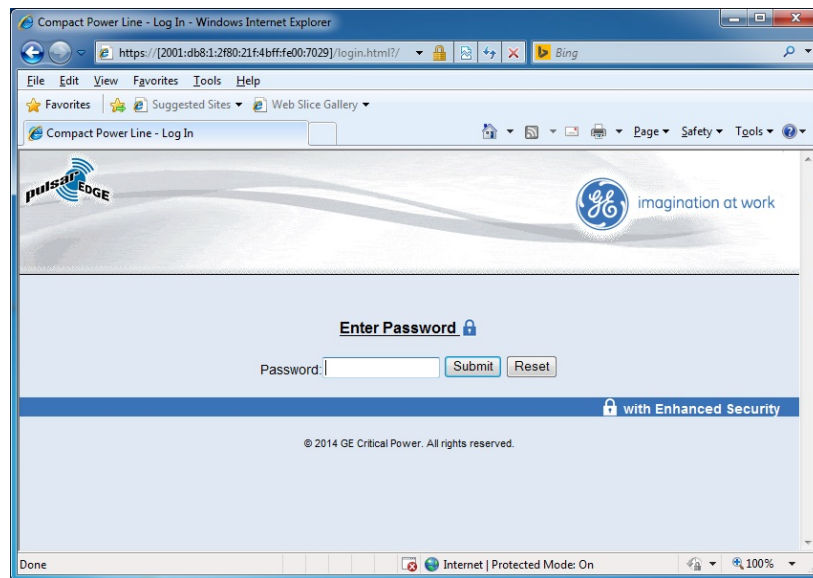


Figure 6: HTTPS Connectivity Over IPv6 Galaxy Pulsar Edge Controller Login Screen

SNMP

In addition to supporting the basic protocols on TCP/IP, the Galaxy Pulsar Edge supports conveying system alarm and control information to a Network Operation Center (NOC) using the Simple Network Management Protocol (SNMP). The Galaxy Pulsar Edge implements the secured SNMPv3 as well as the SNMPv2C agent that is backwards compatible with SNMPv1. The various configuration items for the protocols can be found in the *Settings ► Communication ► SNMP* web screen depicted below.

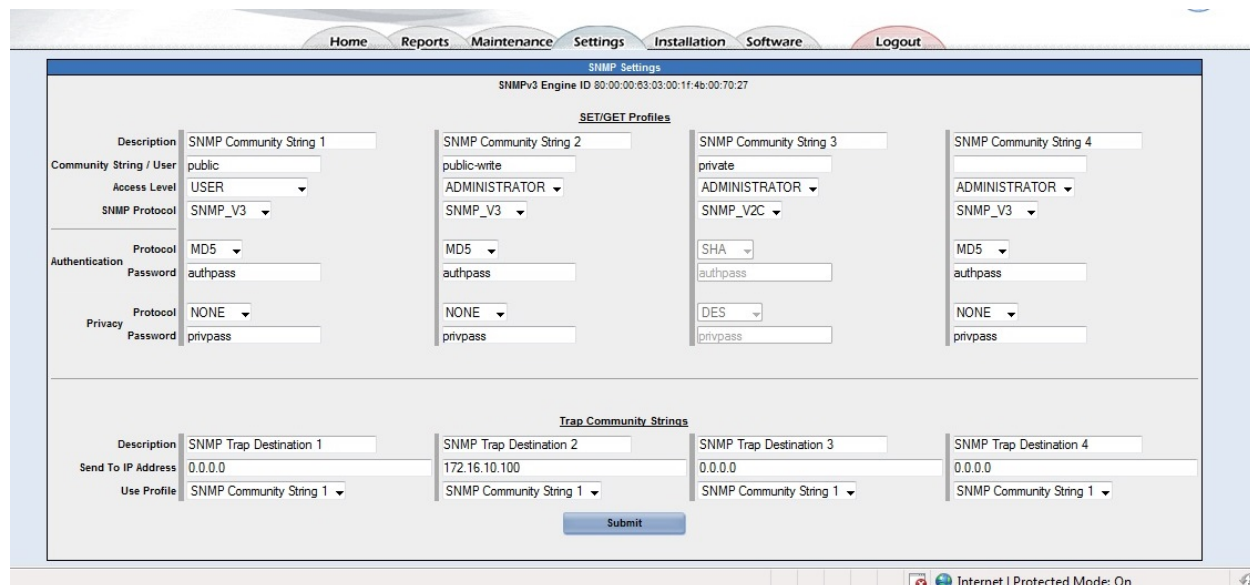


Figure 7: SNMP Settings Screen

For security reasons the SNMPv1/v2c community string and SNMPv3 user information can only be modified when logged in as administrator.

The controller has four SET/GET profiles that can be used as either SNMPv1/v2c community strings or SNMPv3 users. The Community String/User field is the value of community string or username that will be accepted by the controller. Each one of these values must be unique (or blank). The SNMP Protocol field determines how each is used. The Access Level (User, Super-User, and Administrator) field determines which SNMP operations are valid and the scope for each. The choices are:

- *USER* – has read-only access (SNMP GET operation) to data (OIDs) within the controller MIB
- *SUPER-USER* – has read and write access (SNMP SET and GET operations) to OIDs within the controller MIB
- *ADMINISTRATOR* – has read and write access to all OIDs supported by the controller

SNMPv3 users have additional protocol and password fields to support authentication and privacy. (These fields are only accessible if the SNMPv3 protocol is selected).

Authentication protocols are NONE, MD5 and SHA. Privacy protocols are NONE, DES and AES 128-bit.

Whenever the SET/GET profiles are modified the controller will require about 15 seconds before the changes take effect. This allows the controller type to perform the calculations necessary to create new crypto keys.

Four Trap Community String entries allow the user to specify a target IP address (IPv4 or IPv6) for alarm notifications (Traps) and one of the SET/GET Profiles to be used with the trap.

SFTP

The Galaxy Pulsar Edge implements the SSH File Transfer Protocol (also Secure File Transfer Protocol, or SFTP) to provide file access, file transfer, and file management functionalities over any reliable data stream. WinSCP, an open source free SFTP client, FTP client, WebDAV client and SCP client for Windows, was used to test the file transfer capability between the Galaxy Pulsar Edge controller and a remote computer. This software can be downloaded at <http://winscp.net/eng/download.php>.

By default WinSCP attempts to use a temporary file to allow file transfers to be interrupted and resumed. The Pulsar Edge controller's file system does not allow the creation of temporary files, so the feature must be disabled in WinSCP. Disable this feature by going to *Options ► Preferences ► Endurance* in WinSCP and check the disable for the "transfer resume/transfer to temporary file". Sample WinSCP screen shots follow.

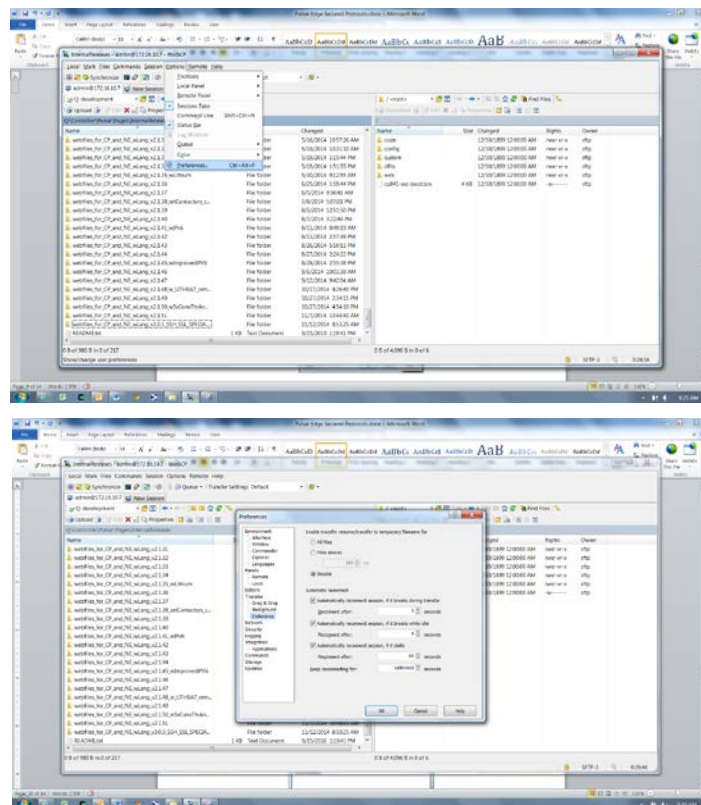


Figure 8: Sample WinSCP Configuration Screen For Disable

When logging into the controller using WinSCP, as with FTP, the username is not validated unless the controller has the "User Name and Password" login method enabled (*Settings ► Passwords*).

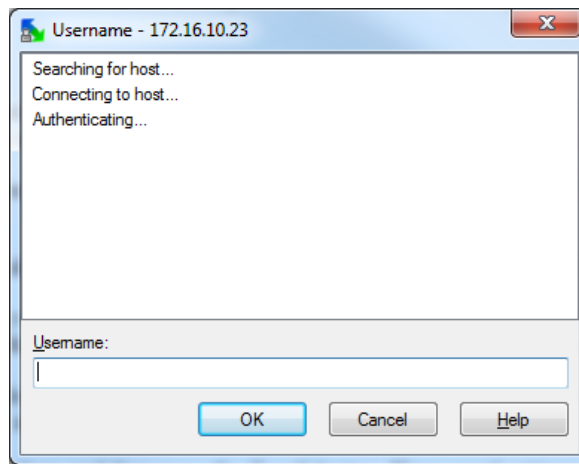


Figure 9: WinSCP Login Screen

When connecting to a controller for the first time WinSCP will alert the user to store the controller's security key in the key cache. Press Yes. This key will remain valid until the controller's IP address is modified.

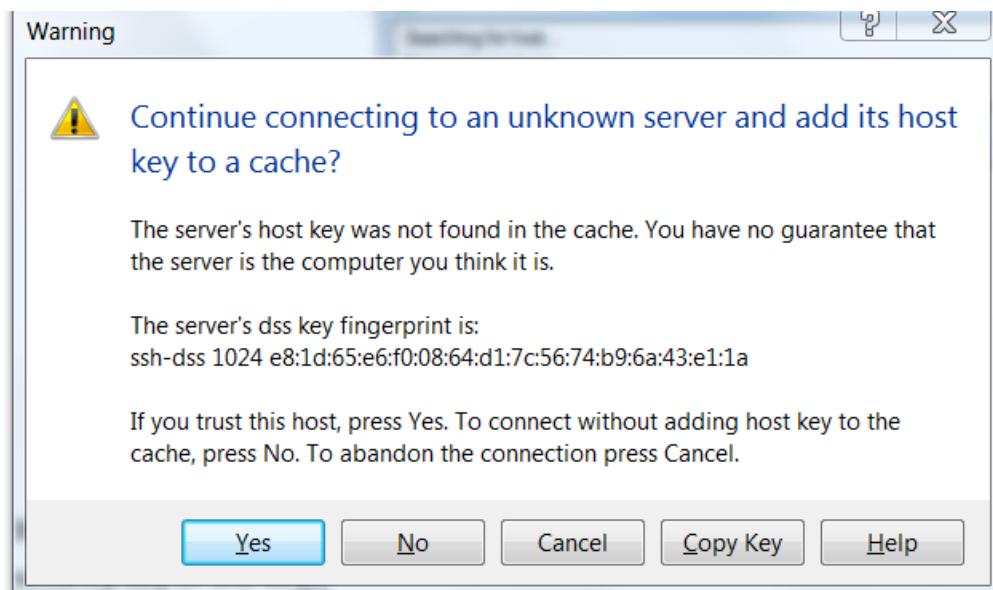


Figure 10: WinSCP Security Key Warning Screen

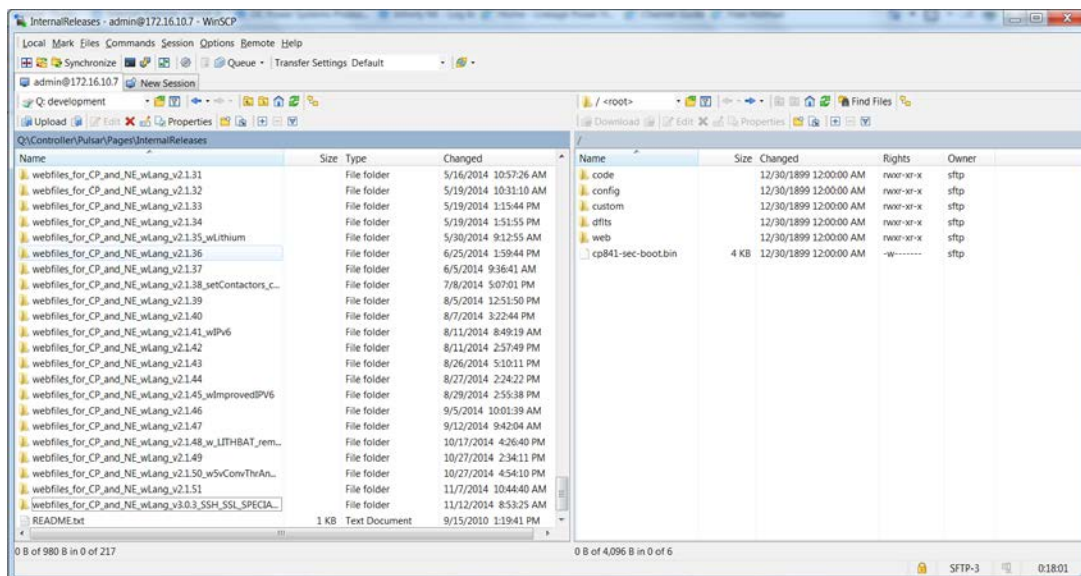


Figure 11 WinSCP SFTP Screen Example

SSH

The Galaxy Pulsar Edge controller supports the Secure Shell (SSH) cryptographic network protocol for secure data communication, remote command-line login, remote command execution, and other secure network services between itself and a networked computer. It is a replacement for Telnet that offers encryption. The controller's SSH implementation has been tested using PuTTY. PuTTY is an SSH and telnet client, developed originally by Simon Tatham for the Windows platform. It is open source software that is available with source code and is developed and supported by a group of volunteers. Putty can be downloaded at <http://www.putty.org/> . A typical download is the "putty.exe" executable that covers the Telnet and SSH client.

When connecting to the Galaxy Pulsar Edge controller for the first time, PuTTY will alert the user to store the controller's security key in the key cache (sample screen below). Select "Yes", enter a login, and the controller password, to access the SSH server (the controller). This key will remain valid until the controller's IP address is modified.

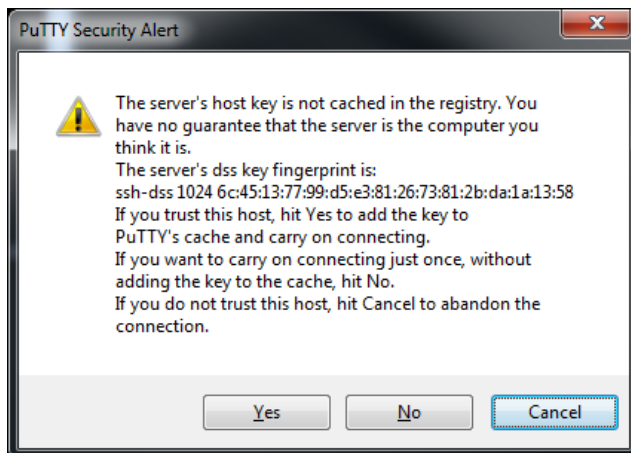


Figure 12: PuTTY Security Key Warning Screen

Below is a sample controller's screen once the controller's SSH Server has been accessed. Standard T1.317 commands can be used.

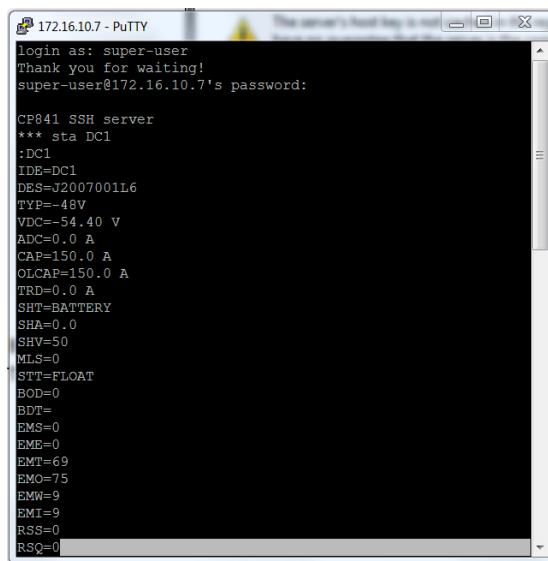


Figure 13: PuTTY SSH Pulsar Edge Login Example Screen

Table 3: Revision History

Revision	Date	Description	Owner
1	11/19/2014	Initial Release	J. Brooke/R. Davis
2	07/27/2015	Minor edits and reformat	J. Brooke/R. Davis