CTPView Security Implementation Guide

Release 3.4

Revised: 08-Mar-2010

Table of Contents

Introduction 3

Configuring a New CTPView Server 5

- **Change the BIOS Menu Password** 5
- **Change the Server's Root Account Password** 5
- **Change the GRUB Boot Loader Password** 6
- **Change the MySQL Apache Account Password** 6
- **Change the MySQL Administrator Password** 6
- **Configuring Network Access** 7
- **Updating the CTPView Software** 7
- **Create New Users** 7
- **Delete Default System Administrator Account** 7
- **Logging into the CTPView Web UI** 7
- **Create New User Accounts** 8
- **Delete Default Global_Admin Account** 8
- **Add Login Banner** 8
- **Configure AIDE (Advanced Intrusion Detection Environment)** 9
- **Configure SWATCH (Log Watcher)** 9
- **Configure Two-Factor Authentication** 9
- **Install Anti Virus Software** 9
- **Baseline Files with SUID Bit Set** 10
- **Baseline Files with SGID Bit Set** 10

Discussion of Security Enhancements in CTPView 11

Discussion of Server File System Monitoring 13

Discussion of CTPView Logging 14

- **Summary of Logs** 15

Installation of McAfee Anti-Virus Software 16

Configuration of AIDE (Advanced Intrusion Detection Environment) 17

Configuration of Swatch (Log Watcher) **18**
AAA Functions (Authentication, Authorization and Accounting) **19**
CAC/PKI Configuration **20**
RADIUS/RSA SecurID Configuration **22**
SSH Options **23**
SSH – CAC/PKI **23**
SSH – RADIUS/RSA **24**
SSH – Local User/Pass **24**
HTTPS Options **24**
HTTPS – CAC/PKI **24**
HTTPS – RADIUS/RSA **25**
HTTPS – Local User/Pass **25**

Steel-Belted RADIUS (SBR) Server Configuration **26**
Configure RADIUS/RSA Settings on the CTPView Server **26**
Configure the SBR Server's Dictionary Files **26**
Configure the SBR Server's Authentication Policies **27**
Add CTPView as a RADIUS Client on an SBR Server **28**
Add CTPView Users to an SBR Server: **28**

RSA SecurID Appliance Configuration **28**
Configure RADIUS/RSA Settings on the CTPView Server **29**
Configure the SBR Server's Dictionary Files **29**
Configure the SBR Server's Authentication Policies **30**
Add CTPView as a RADIUS Client on an SBR Server **30**
Add CTPView Users to an SBR Server: **31**
Assign SecurID Tokens to CTPView Users **31**

How To Use CAC Smart Cards For SSH Access To CTPView **31**
ActiveClient configuration – Initial procedure: **32**
Putty-CAC Configuration – For Each Remote Host: **32**

Introduction

This guide provides additional detail on the security related features introduced or modified in this release. See the Release Notes for a description of all enhancement and bug fixes contained in the release you are installing.

The full range of security features are only available on CTPView servers running the Juniper customized CentOS 5.3 operating system.

The first release of CTPView which incorporated the enhanced security features was 3.4R2-p1 and required the server be running CentOS as its operation system. Beginning with release 3.4R3 previous installations of CTPView on systems using the Fedora Core 4 or Fedora 9 operating systems may install new CTPView software without upgrading their operating system, but not all new security features will be available.

If you wish to update the OS on your existing server to CentOS, contact your Juniper representative for assistance.

If you are updating your server to CentOS you can save and transfer your current server settings and data files to your rebuilt server using our backup utility.

To save and restore configuration and data files:

- Upgrade you current server to the latest release of CTPView software.
- Save your current server's configuration and data files using the backup utility found in the cli menu > Backup Functions.
- Rebuild your server with a clean installation of the Juniper customized CentOS 5.3 using the CDROM media and server build instructions available through your Juniper account representative.
- Update the CTPView software on the rebuilt server to the latest release.
- Restore the server configuration and data files you saved by using the backup utility.

The following supplemental steps must be executed after restoring data from a previous FC4 or FC9 server configuration to a CentOS server in order to complete the upgrade:

- Re-enter the Mail Server's name or IP address on the Email Notifications page of the CTPView browser interface. This one time step is necessary due to the changing of the MTA from Sendmail to Postfix. The path to the page is Server > Administration > Email Notifications > Change Mail Server.

- Re-create the user accounts for CTPView browser access. This one time step is necessary due to the change in structure of the MySQL database to accommodate encryption of the user passwords using AES-256 instead of a MD5 hash.

- Continue the installation process by following the step in the “Configuring a New CTPView Server” section of this guide.

Configuring a New CTPView Server

Change the BIOS Menu Password

For security purposes, change the default password for BIOS menu access. There is no username associated with this account.

During the boot process, while the Dell logo is displayed on the monitor, press F2. The boot process continues, displaying several messages on the screen. Wait until the process pauses and asks for the Setup Password. Enter the default password to continue. See *Appendix B, Default CTPView Accounts and Passwords*.

When you have gained access to the BIOS menu, highlight the line **System Security**, and press Enter. Highlight the line **Setup Password**. (Make sure that you have not selected System Password.) Press Enter, and type your new BIOS password. Press Enter, and then reenter your new password. Press Enter to continue.

Press the Esc key. In the pop-up window highlight the line Save Changes and Exit, and press Enter. The system will now restart.

NOTE: Good security practice requires that the BIOS menu password be changed at least yearly or upon administrator reassignment.

Change the Server's Root Account Password

For security purposes, change the default password for the server's root user account.

After logging in as a System Administrator, type this command:

sudo passwd

Follow the prompts to enter the new password. You must ensure that the password you chose complies with the minimum requirements for password complexity. These are:

Min 15 characters
Min 1 uppercase
Min 1 lowercase
Min 1 numerial
Min 1 other
Not include username
Not include dictionary word
Not include more than 2 adjacent repeating characters

NOTE: Good security practice requires that the root account password be changed at least yearly or on administrator reassignment.

Change the GRUB Boot Loader Password

For security purposes, change the default password for the GRUB Boot Loader menu.

Login to the cli management console as a System Administrator. At the command prompt, type menu. The CTPView Configuration Menu utility will open. Make a note of the CTPView version number displayed in the heading. This will be helpful when you check the Juniper website for software upgrades.

Select GRUB Functions. Then select Change GRUB password, and follow the prompts.

NOTE: Good security practice requires that the GRUB Boot Loader password be changed at least yearly or on administrator reassignment.

Change the MySQL Apache Account Password

For security purposes, change the default password for the MySQL server Apache user account.

While in the main screen of the CTPView Configuration Menu utility, select MySQL Functions. Then select Change MySQL Apache password and follow the prompts.

NOTE: Good security practice requires that the MySQL Apache password be changed at least yearly or on administrator reassignment.

Change the MySQL Administrator Password

For security purposes, change the default password for the MySQL server Administrator account.

While in the main screen of the CTPView Configuration Menu utility select MySQL Functions. Then select Change MySQL Administrator password and follow the prompts.

NOTE: Good security practice requires that the MySQL Administrator password be changed at least yearly or on administrator reassignment.

Configuring Network Access

While in the main screen of the menu utility, select System Configuration. Answer **y** to continue. Select Display Current Configuration. Use Options 2 through 5 to configure the server to operate on your network. Exit the sub-menu to implement your changes.

Updating the CTPView Software

From a computer with access to the Web, use a browser to connect with the Juniper CTP Support site at

https://www.juniper.net/customers/csc/software/ctp/

You need your Juniper support username and password to access this site. If an update to the CTPView software is available, download the new archive along with the release notes. Your current CTPView version is listed in the header of the CLI menu utility.

Create New Users

While in the main screen of the menu utility, select Security Profile > User Management > Add admin shell accounts.

Create a new System Administrator account and other users as required for your operations.

Delete Default System Administrator Account

For security purposes, you must delete the default System Administrator account that which is shipped with the new server.

Log into the server as a System Administrator you created. In the main screen of the menu utility, select Security Profile > User Management > Delete admin shell accounts. Remove the default System Administrator.

Logging into the CTPView Web UI

In the address bar of a browser enter the address

```
https://<your server IP address>
```

Your browser will issue a warning that the security certificate presented by your CTPView server was not issued by a trusted certificate authority. Make the selection to accept the certificate, and continue.

The CTPView login page will appear. Log in as the default CTPView Web UI user. For the default account username and password, see *Appendix B, Default CTPView Accounts and Passwords*.

Create New User Accounts

The new security-enhanced CTPView Web UI introduced with version 2.2R2 allows only one active session per username. If a second user were to attempt to log in using the same username in an active session, both clients' IP addresses and the username would be locked out from access for a preset lockout period. It is therefore imperative that each user have his or her own account and that the default user account not be used for normal access.

After logging into CTPView Web UI for the first time using the default user account, click Admin Center.

Add a new Global_Admin user. Make sure that the user level is set to Global_Admin in order to be able to access the CTPView User Administration Center. Create other additional user accounts as your operations require.

Delete Default Global_Admin Account

After creating a new Global_Admin user account above, log out of CTPView. Then log in using a new Global_Admin user account. In the Admin Center, delete the default Global_Admin Account.

Add Login Banner

This is done through the browser interface. Access the banner page by following these links from the directory frame: Server > Administration > Set Start-up Banner. Paste your organizations approved Login Banner into the input area and click the Submit Changes button.

This login banner will appear whenever access to the server is attempted, whether it be via browser, terminal, console or SSH session.

Configure AIDE (Advanced Intrusion Detection Environment)

You must review and if necessary modify the configuration file for AIDE, located at `/etc/aide.conf`. You must also copy and store the AIDE database(s) on write-protected media in a secure location. See the separate section in this manual for details on the database file locations.

Configure SWATCH (Log Watcher)

Swatch is designed to monitor system activity. In order for Swatch to be useful, it requires a configuration file which contains pattern(s) to look for and action(s) to perform when each pattern is found.

You must review and if necessary modify the configuration files for SWATCH. See the separate section in this manual for details on how SWATCH is configured for the default CTPView installation.

Configure Two-Factor Authentication

CTPView is able to support RSA SecureID and CAC smart card access, in addition to the username/password. If you wish to enable these features, follow the steps detailed in the separate sections of this manual.

Install Anti Virus Software

Obtain, install and configure antivirus software compatible with command line execution on a Linux system. We have successfully installed the McAfee product VirusScan Command Line Scanner. See the section below for information on how we configured our implementation. This software is not packaged with the CTPView server, but must be purchased and installed by the end-user.

Baseline Files with SUID Bit Set

Log into the server shell as a System Administrator and run this command to create the file /tmp/baseline_suid which will contain the ownership, permissions, and location of files with the suid bit set:

```
sudo find / -perm -4000 | xargs ls -l > /tmp/baseline_suid
```

This command must be re-run on a weekly basis and the results checked for unauthorized modifications.

Baseline Files with SGID Bit Set

Log into the server shell as a System Administrator and run this command to create the file /tmp/baseline_sgid which will contain the ownership, permissions, and location of files with the sgid bit set:

```
sudo find / -perm -2000 | xargs ls -l > /tmp/baseline_sgid
```

This command must be re-run on a weekly basis and the results checked for unauthorized modifications.

Discussion of Security Enhancements in CTPView

All of the security enhancements included with CTPView are only available when installed on a system running the CentOS 5.3 operating system. Only the applications necessary to run CTPView are installed. For example, the server has no X-Windows or desktop applications installed.

The previous privileged administrator group of users has been given expanded access to the operating system. This class of user will be referred to as System Administrators. They now have the same privileges as the superuser root, except as noted elsewhere in this document. Many tasks require that 'sudo' be prefix to the task's command when executed by a System Administrator, for example "sudo service network restart".

The previous administrator group of users has also been given greater privileges. Their class is now called Web Managers. They have read/write access to all the CTPView Web UI application directories and files. Web Managers can control certain aspects of the operating system services which support the web interface. For instance, they can restart Apache with the command "sudo service httpd restart".

A new class of users has been created. They are the Auditors. This group has read only access to the log files for the system and applications. Auditors monitor performance, trouble-shoot and look for breaches of security through review of the various logs available on the system. Auditors have aliases to certain tail commands to speed log viewing.

CLI Aliases available to Auditors:

Alias	Command
tmes	tail –f /var/log/messages
tsec	tail –f /var/log/secure
tgui	tail –f /var/log/acorn_gui.log
taudit	tail –f /var/log/audit/audit.log

User Class Access Summary:

User Class	Unix group	Description
System Administrator	server_priv	Access to entire system, root-like privileges
Web Manager	server	Control over web pages and web services
Auditor	server_log	Read access to logs

Users cannot open a new shell after logging in.

The su command has been disabled for all users.

No task necessary for the operation and maintenance of the server requires the use of the root password.

No user can become the superuser root. All necessary root privileges to install, operate and modify the server and CTPView Web application have been assigned to the appropriate user group or groups. Where necessary, System Administrators can obtain enhanced root-like privileges the sudo command.

Default Users on new systems running CentOS as received from Juniper:

	Default Username	User Class	Group Name	Default Password
Shell	juniper_sa	System Administrator	server_priv	CTPView-2-2
Browser	Juniper	CTPView Administrator	Global_Admin	CTPView-2-2

Sendmail has been replaced by Postfix as the mail transport agent. CTPView is configured as a Null-Client. A null-client is a machine that can only send mail. It receives no mail from the network, and it does not deliver any mail locally. The previous Sendmail binary and library file names have been replace with symbolic links pointing to the new Postfix files allowing legacy applications to continue to be used. There are no user visible changes related to this switch.

User passwords for the CTPView Web UI are now stored using AES-256 encryption in the MySQL database. Previous versions of CTPView used an MD5 hash.

System Administrators are reminded to use the Security Profile option of the cli menu when managing system users to ensure compliance with security protocols. The cli commands to add, delete or modify users and groups from the command line have been disabled. System Administrators are allowed to change other user's password.

Discussion of Server File System Monitoring

Each hard drive partition is monitored for amount of free space remaining on the partition. When the percent of use exceeds a configurable trigger point the system reports the information several ways.

The trigger point is settable by CTPView administrators using the Web UI. The path is Server > GUI Settings > Server Capacity Warning Trigger Point. The default value is 90%.

A value exceeding the trigger point is reported several ways:

- When a Global_Admin or Net_Admin user successfully logins using the CTPView Web UI:
    - A detailed list of affected hard drive partitions are displayed on the login page
    - An entry is made to the /var/log/messages log for each affected partition
- Once daily via a cron job. The results of affected partitions are written to the /var/log/messages log.

At any time, a CTPView Web UI Global_Admin or Net_Admin user can view the current information of the server file system from the System Information page. The path is Server > Diagnostics.

You may also make use of the application Swatch to monitor the logs and report instances of a trigger point alarm via an email notification. See the separate section in this guide for more information on Swatch.

Here is a sample of the warning seen on the Web UI login page of a CTPView server running on the CentOS 5.3 OS. The trigger point has been set to 0% so that all partitions are listed.

WARNING
Partition /dev/md2 mounted on / is 20% full
Partition /dev/md11 mounted on /var is 3% full
Partition /dev/md9 mounted on /var/spool is 2% full
Partition /dev/md8 mounted on /yp is 2% full
Partition /dev/md7 mounted on /var/log is 4% full
Partition /dev/md10 mounted on /var/log/audit is 4% full
Partition /dev/md6 mounted on /tmp is 8% full
Partition /dev/md5 mounted on /var/www is 8% full
Partition /dev/md4 mounted on /var/lib/mysql is 5% full
Partition /dev/md3 mounted on /home is 2% full
Partition /dev/md0 mounted on /boot is 12% full

The /var/log/messages entries for above sample appear as this:

```
Jan  3 18:22:15 centos-61 [2289]: Partition /dev/md2 mounted on / is 20% full
Jan  3 18:22:15 centos-61 [2289]: Partition /dev/md11 mounted on /var is 3% full
Jan  3 18:22:15 centos-61 [2289]: Partition /dev/md9 mounted on /var/spool is 2% full
Jan  3 18:22:15 centos-61 [2289]: Partition /dev/md8 mounted on /yp is 2% full
Jan  3 18:22:15 centos-61 [2289]: Partition /dev/md7 mounted on /var/log is 4% full
Jan  3 18:22:15 centos-61 [2289]: Partition /dev/md10 mounted on /var/log/audit is 4% full
Jan  3 18:22:15 centos-61 [2289]: Partition /dev/md6 mounted on /tmp is 8% full
Jan  3 18:22:15 centos-61 [2289]: Partition /dev/md5 mounted on /var/www is 8% full
Jan  3 18:22:15 centos-61 [2289]: Partition /dev/md4 mounted on /var/lib/mysql is 5% full
Jan  3 18:22:15 centos-61 [2289]: Partition /dev/md3 mounted on /home is 2% full
Jan  3 18:22:15 centos-61 [2289]: Partition /dev/md0 mounted on /boot is 12% full
```

Discussion of CTPView Logging

In addition to the normal Linux log files, the CTPView server maintains several logs related to the CTPView Web application. You will find a brief description of these logs below. Where indicated by the keyword “Log msg”, the specified message will be written to the /var/log/messages log when the indicated log is rotated.

Auditors and System Administrators have access to the /var/log directory and sub-directories. They can read the log files and copy the logs to a remote server using the “scp” command. They cannot modify or delete log files.

The logging level of the CTP node management operations can be managed using the CTPView cli menu. The path is menu > Advanced Functions > Set Logging Level. There are three options, production servers should be set to Normal unless you are attempting to resolve a problem:

Normal (Most commands, All errors)
Debug Level 1 (All commands, All errors)
Debug Level 2 (All commands, All output)

You may also configure the server to send logging to one or two remote syslog servers. The path to configure this option is menu > Security Profile > Secure Log Management > Configure remote logging options.

Another method of monitoring log files is using the application Swatch, which is installed on the CTPView server. See the separate section in this guide for more information on Swatch.

Summary of Logs

/var/log/acorn_event.log
Log of Network Monitoring emails reporting CTP node status events
10 backlogs retained
Rotated daily - not if empty
Log msg: ctpview log acorn_event.log rotated

/var/log/acorn_gui.log
Log of CTP node management configuration and query operations
10 backlogs retained
Rotated daily - not if empty
Log msg: ctpview log acorn_gui.log rotated

/var/log/audit/audit.log
Log of audit daemon
10 backlogs retained
Rotated daily
Log msg: ctpview log audit.log rotated

/var/log/cron
Log of cron daemon
10 backlogs retained
Rotated weekly – not if empty
Log msg: ctpview log cron rotated

/var/log/httpd/*log
Logs of various operations of httpd server (Apache server)
10 backlogs of each type retained
Rotated weekly – not if empty
Log msg: none

/var/log/maillog
Log of mail server
10 backlogs retained
Rotated weekly – not if empty
Log msg: ctpview log maillog rotated

/var/log/messages
Log of general message and system related items
10 backlogs retained
Rotated weekly – not if empty
Log msg: ctpview log messages rotated

/var/log/mysqld.log
Log of MySQL server

10 backlogs retained
Rotated weekly – not if empty
Log msg: ctpview log mysqld.log rotated

/var/log/secure
Log of authentications
10 backlogs retained
Rotated weekly – not if empty
Log msg: ctpview log secure rotated

/var/log/snmpd.log
Logs of snmp daemon
10 backlogs retained
Rotated weekly – not if empty
Log msg: none

/var/www/html/acorn/data/ctp_dbase/ctp_upgrade_log.archive
Log of CTP node upgrade operations
10 backlogs retained
Rotated weekly – not if empty
Log msg: ctpview log ctp_upgrade_log.archive rotated

/var/www/html/acorn/ip/iplist_master
Database of CTP node IP Addresses and basic information
14 backlogs retained
Rotated daily – not if empty
Log msg: none

/var/www/html/acorn/server_sync/server_sync_log.archive
Log of CTPView server synchronization operations
10 backlogs retained
Rotated daily – not if empty
Log msg: ctpview log server_sync_log.archive rotated

Installation of McAfee Anti-Virus Software

You are required to obtain and install approved command line antivirus software.

We have successfully installed and tested the McAfee VirusScan Command Line Scanner with CTPView:

http://www.mcafee.com/us/enterprise/products/system_security/servers/virusscan_command_line_scanner_windows_unix.html

You should install the antivirus software in the /yp directory on the CTPView server to as this directory is on its own hard drive partition.

Configuration of AIDE (Advanced Intrusion Detection Environment)

AIDE is an intrusion detection program, more specifically a file integrity checker.

AIDE constructs a database of the files specified in aide.conf, AIDE's configuration file. The AIDE database stores various file attributes including: permissions, inode number, user, group, file size, mtime and ctime, atime, growing size, number of links and link name. AIDE also creates a cryptographic checksum or hash of each file using one or a combination of the following message digest algorithms: sha1, sha256, sha512, md5, rmd160, tiger (gost and whirlpool can be compiled in if mhash support is available). Additionally, the extended attributes acl, xattr and selinux can be used when explicitly enabled during compile time.

Typically, a system administrator will create an AIDE database on a new system before it is brought onto the network. This first AIDE database is a snapshot of the system in it's normal state and the yardstick by which all subsequent updates and changes will be measured. The database should contain information about key system binaries, libraries, header files, all files that are expected to remain the same over time. The database probably should not contain information about files which change frequently like log files, mail spools, proc filesystems, user's home directories, or temporary directories.

When CTPView was installed on the server AIDE was initialized. This first database was saved to the file **`/var/lib/aide/aide.db.new.gz`**.. This initial database file also became the first working AIDE database located at **`/var/lib/aide/aide.db.gz.`**

CTPView uses the default configuration file, located at **`/etc/aide.conf`**. You should review the documentation available in the manpage and at http://www.cs.tut.fi/~rammer/aide/manual.html for help in configuring AIDE for your system.

CTPView is configured to run a database check once each week by an entry in root's crontab file. The results are logged to the file /var/log/aide/aide.log. To manually check the inconsistencies between the current system and the AIDE database, running following command:

```
aide –check
```

After you investigate and fix any unexpected output you can issue the following command to update the AIDE database:

```
aide –update
```

You must copy each updated AIDE database to a write-protected media and store them in a secure location.

Configuration of Swatch (Log Watcher)

Swatch is designed to monitor system activity. In order for Swatch to be useful, it requires a configuration file which contains pattern(s) to look for and action(s) to perform when each pattern is found. Swatch is started during the server boot process.

Changing the log watching process requires that you modify 2 files;

- **`/etc/init.d/swatch`** – This file starts/stops the swatch process that is watching a log.
- **`/etc/swatch/swatch.<log_name>.conf`** – This file contains the patterns and actions for the swatch process.

To modify the swatch configuration for a log:

1. Stop swatch service:
   ```
   sudo service swatch stop
   ```
2. If you want to add or remove a log to watch, open the **`/etc/init.d/swatch`** file and modify the line which defines the variable "WATCH_FILES" to include or exclude the log file.
3. If you are adding a log to watch, create or modify the configuration file located at **`/etc/swatch/swatch.<log_name>.conf`**. Refer to the manpage and existing conf files for help.
4. If you are removing a log being watch, you may leave the existing **`/etc/swatch/swatch.<log_name>.conf`** as it is.
5. Start the swatch service:
   ```
   sudo service swatch start
   ```

To use the mail notification feature in Swatch you must configure the CTPView server for your networks mail server. This is easily done through the CTPView's browser interface. Use your browser to open CTPView. Open the email configuration window by following these links: Server > Administration > Email Notifications. Configure and test your mail server using the Change Mail Server dialog at the top of the page. The rest of the page does not apply to Swatch.

By default CTPView is watching the following logs. However, no actions have been configured in the respective swatch log conf files.

- acorn_gui.log
- aide.log
- audit.log
- cron.conf
- messages
- mysqld.log
- secure
- uvscan

AAA Functions (Authentication, Authorization and Accounting)

The AAA functions for CTPView can be viewed and set in the AAA sub-menu of the cli menu script. Only System Administrators have authorization to set and modify the AAA functions.

Configuration of the CTPView AAA functions has two major components:

- Configuring the global configuration details, for example entering the IP addresses of the RADIUS servers you want to use for authentication.
- Selecting the options which the different authentication methods will use. For example, enabling HTTPS – CAC/PKI with OCSP certificate validation.

For the initial server configuration, and for any subsequent modifications, access to the CTPView server is gained via an SSH session.

CTPView supports three validation mechanisms, which are processed in this order:

1. CAC Smart Card (PKI certificate)
2. RADIUS based database (e.g. RSA SecureID)
3. Locally stored username:password database

The first successful validation of your credentials will end the validation process and grant you access to the server. Failover from one method to the next will occur except when the CAC/PKI method is set to “Required”. Failover refers only as to which method will be used for validation. Once a user is rejected by any method, the login session is terminated. See other sections in this manual for more detailed information on how to configure SSH access options.

Access to the CTP Node Management functions of CTPView is by means of the HTTPS protocol using a browser application on your remote workstation. This is the normal user access method once CTPView has been deployed in a production environment. We support the same three validation mechanisms for HTTPS access as we do for SSH access described above.

You can view a summary of the current settings for the 6 validation mechanisms, and make modifications, by using the CTPView cli menu. The path to the screen is menu > AAA Functions. Initially configuring and later modifying these methods is a multi-step process which is discussed in detail in the following sections.

CAC/PKI Configuration

CTPView is built with a default server certificate installed which is sufficient for testing purposes only. Before deploying the server in a production environment you must obtain and install a server certificate issued by a Trusted Signing CA. If you attempt to access multiple CTPView servers running on CentOS which are still using their default self-signed certificates you may be denied access by your browser because it will detect that multiple servers are presenting certificates with the same serial number.

Obtaining and installing a signed server certificate is a simple process. First, you must create a certificate signing request (CSR) for your server which you will present to the Trusted Signing CA you have selected to use. To start, go to the CAC/PKI Configuration menu. The path is menu > AAA Functions > CAC/PKI Configuration.

In the CAC/PKI Menu, select Create CSR and follow the prompts to enter information about your server and organization. You are required to enter the Encryption Key Size, Common Name, Organization Name and Country. You may also include any combination of these optional fields: Organizational Unit (3 possible fields), State, and City/Town.

The script will generate a random seed to use when creating the CSR by using the timing of keystrokes on your keyboard. The CSR will be a RSA certificate in ascii format (i.e. plain text), using either 1024 or 2048 bit encryption depending on your choice when creating the CSR. The CSR name will be <Common Name>.csr and is created in the /tmp directory on the server. If you want to change any of the information you entered when creating the CSR simply create a new CSR. Creating a CSR has no effect on the configuration or operation of the server.

Send the CSR which you created to your Trusted Signing CA. You may be asked to send the CSR as an email attachment or to paste the CSR into a web form. You can do that by opening the CSR file with a text editor, such as WordPad or vi, then use the copy and paste editing functions to transfer the new certificate request to the web form.

While it is preferred that you have your server CSR signed by a Trusted Signing CA, where that is not possible you may generate a self-signed server certificate using the CTPView CA issued by Juniper Networks. This self-signed certificate will generate an error in client browsers to the effect that the signing certificate authority is unknown and not trusted.

To use the CTPView CA to sign your CSR select Self-Sign CSR from the CAC/PKI Menu. Enter the CSR filename and the utility will create a signed server certificate which you can

then import into the certificate database. No additional Chain of Trust certificates are required to use the CTPView CA. As when creating a CSR, repeating the signing process has no effect on the configuration or operation of the server since a separate process is required to import the certificate.

When the Trusted Signing CA sends you the signed server certificate you will need to import it into your server's certificate database. You will also need to import all of the certificates that make up the Chain of Trust for your new server certificate. These are available from your Trusted Signing CA. Copy all of the certificates into the /tmp directory of the server. They can have any filename and file extension.

In the CAC/PKI Menu, select Import Certificate. You may enter the Chain of Trust and signed CSR certificates in any order, however it is customary to start with the highest level of the Chain of Trust and proceed downward until you enter your signed server certificate.

For each certificate you import you will be asked to enter a unique Nickname. This will be used to identify the certificate. Allowed characters are alphanumeric, space, period, hyphen and underscore.

After submitting the Nickname, you will be asked if the certificate is the signed certificate for this server. If you enter Yes in error, you will need to re-import the correct certificate for the server. You can check which certificate the server is currently using from the List Certificates option of the CAC/PKI Menu.

The CAC/PKI Menu has additional options which allow you to display the contents of an imported certificate in plain text, check the validity of an imported certificate using the installed Chain of Trust certificates, and remove an imported certificate from the server database. Remember that if you remove the certificate the server is currently using for HTTPS client authentication you must import a new server certificate before HTTPS access is restored.

Client CAC/PKI certificates presented to the server via HTTPS are authenticated in one of two ways:

- Checking with the OCSP responder using the URL embedded in the client certificate
- Checking against the locally installed CRL's

The method which is used is selected by you when you enable the service for HTTPS(1st) - CAC/PKI from the main AAA Menu. There is no failover between the OCSP and CRL authentication methods. Ensure that the server will have network access to the OCSP responder before you select that method.

Using the CRL authentication method requires that you import up-to-date revocation lists into the server database. The Trusted Signing CA maintains a CRL for certificates it has signed and then revoked. On a regular basis you should acquire an updated CRL. Check with your security representative for the frequency that your organization requires CRL's to be updated.

Copy the CRL into the /tmp directory of the server. To import the CRL open a menu session and navigate to menu > AAA Functions > CAC/PKI Configuration > Import CRL. Enter the filename of the CRL you placed into the /tmp directory. Unlike when you imported certificates, no Nicknames are used for CRL's. The identifying name for each CRL is embedded within the file. If you are updating a CRL from a Trusted Signing CA which is already installed in the database the existing CRL will be replaced so that only one CRL exists in the database with the same identifying name.

The CAC/PKI Menu has additional options related to CRL's which allow you to list all the imported CRL's, display the contents of an imported CRL in plain text, and remove an imported CRL from the server database.

RADIUS/RSA SecurID Configuration

CTPView 3.4 installed on a server using the CentOS operating system provides RADIUS authenticated user login to the CTPView browser application when used in conjunction with a Steel-Belted RADIUS (SBR) server or a RSA SecurID appliance.

The configuration of the CTPView server for both methods share a common interface and is described in detail in this section. The configuration of the SBR server and RSA SecurID appliance for interoperability with CTPView servers is covered in separate sections of this manual.

To start the CTPView configuration, go the RADIUS/RSA SecurID Configuration menu. The path is menu > AAA Functions > RADIUS/RSA SecurID Configuration. Select the Add/Update Web UI RADIUS Template Accounts option. This action is only required once, during the initial setup of CTPView as a RADIUS client. However, repeating this step will have no detrimental effect on the RADIUS configuration. You will need to input the password for the MySQL Administrator account to complete this step.

The next step is to configure the CTPView server as a RADIUS client. These settings are compatible with Juniper Steel-Belted RADIUS or with RSA SecurID for 2-factor authentication. See the separate chapters in this manual for CTPView specific information on SBR and SecurID configuration help.

From the RADIUS/RSA SecurID Configuration menu select the View/Set RADIUS Servers option. The currently configured RADIUS servers are displayed. Answer "y" if you want to add, remove or modify a server on the list. It is important to note that you will be required to re-enter ALL RADIUS servers when making modifications to the server list. When prompted by the script, enter the RADIUS server's address, the shared secret, the timeout period in seconds and number of connection retries.

The default configuration of CTPView uses 1812 as the RADIUS destination port. You may change to another port using the View/Set RADIUS Port option in the RADIUS/RSA SecurID Configuration menu.

When RADIUS is enabled, the order of user authentication is RADIUS then local username:password if no RADIUS server is available. If multiple servers are defined they are tried in a round robin fashion if one server is not answering. You can define up to 10 RADIUS servers.

SSH Options

Each of the three methods of SSH authentication has its own configuration menu, which are accessed from the main AAA Menu. The current settings for each method are displayed are the main AAA Menu screen. Select the option on the main AAA Menu to configure the individual methods.

SSH – CAC/PKI

To enable SSH – CAC/PKI method for user access you must set the SSH CAC/PKI daemon to Enabled. Disabling the daemon will not remove the CAC/PKI public certificates from the server. To restrict all users to the CAC/PKI method of access, you need to disable the RADIUS/RSA and Local User/Pass options. Otherwise, users without valid CAC/PKI certificates attempting access will failover to those methods.

Each CAC/PKI user must have an account on the CTPView server. To add a user, or to check which users have accounts, use the CTPView cli menu. The path is menu > Security Profile > User Management. The username for the CTPView account MUST match exactly the CAC username (sometimes listed as CN or Common Name).

The System Administration must import, by the copy and paste method, the CAC/PKI public certificate for each CAC/PKI user. Select the option “Enable SSH CAC/PKI for a user” and follow the prompts to import the user’s certificate. See the section “How to Use CAC Smart Cards for SSH Access to CTPView and CTP Nodes” in this manual for help in obtaining a user’s public certificate from a CAC card. Multiple certificates may be entered for a single user. CTPView does not check if the imported certificates are on the Trusted Signing CA’s revocation list.

Disabling a user from using the SSH - CAC/PKI method of access will remove all the public certificates for that user from the server. You will need to re-import the certificates when you re-enable the user.

You can view a user’s imported certificates by selecting the option “Check a user's setting”.

SSH – RADIUS/RSA

Each RADIUS/RSA user must have an account on the CTPView server. To add a user, or to check which users have accounts, use the CTPView cli menu. The path is menu > Security Profile > User Management. The username for the CTPView account MUST match exactly the RADIUS/RSA username.

Simply choose to enable or disable the RADIUS/RSA method. There is no configuration required for the individual users. To block a specific user from gaining access, you must disable that user on the RADIUS/RSA server or delete that user's account for the CTPView server using the User Management menu.

To require the RADIUS/RSA method of access, you must disable the Local User/Pass options. Otherwise, users who are not validated using the RADIUS/RSA method will failover to the Local User/Pass method.

SSH – Local User/Pass

Simply choose to enable or disable the Local User/Pass method. There is no configuration required for the individual users. To block a specific user from gaining access, you must delete that user's account for the CTPView server using the User Management menu.

If you elect to disable SSH access using the user/pass method be sure that an alternate method of access, such as CAC/PKI or RADIUS/RSA, is operational before proceeding with this selection. Otherwise you may lose all remote access to the server shell. In that event, you would need to connect to the server via the console port to re-establish shell access to the system.

HTTPS Options

Each of the three methods of HTTPS authentication has its own configuration menu, which is accessed from the main AAA Menu. The current settings for each method are displayed on the main AAA Menu screen. Select an option from the main AAA Menu to configure the individual methods.

HTTPS – CAC/PKI

You can enable or disable HTTPS – CAC/PKI access. If enabled, you can also set the method to be either Required or Optional. If set to Required, the only means of

access to the CTPView Web UI is with a valid CAC/PKI login. A setting of Optional will allow other login methods to be used.

CTPView will check if the user certificate that is presented is on the Trusted Signing CA's revocation list. You designate whether the revocation check is via an OCSP responder or a local CRL. See the section "CAC/PKI Configuration" in this manual for information on how to import CRL's into the CTPView certificate database.

There is no failover between the OCSP and CRL methods. If the OCSP responder is not able to be accessed by CTPView, the CAC/PKI validation will fail. If the Trusted Signing CA's CRL does not exist in the CTPView certificate database, the CAC/PKI certificate validation will proceed.

Each CAC/PKI user must have an account in the CTPView Web UI database. A Global Admin can add a user, or check which users have accounts, by accessing the CTPView Web UI via a browser and going into the Admin Center section. The username for the CTPView Web UI account MUST match exactly the CAC username (sometimes listed as CN or Common Name).

The Chain of Trust certificates for a user's CAC/PKI certificate must be imported into the CTPView certificate database for the user to be validated. See the section "CAC/PKI Configuration" in this manual for information on how to import Chain of Trust certificates into the CTPView certificate database.

HTTPS – RADIUS/RSA

Simply choose to enable or disable the RADIUS/RSA method. There is no configuration required for the individual users. The user does not need to have an account in the CTPView Web UI database. To block a specific user from gaining access, you must disable that user on the RADIUS/RSA.

To require the RADIUS/RSA method of access, you must disable the Local User/Pass options. Otherwise, users who are not validated using the RADIUS/RSA method will failover to the Local User/Pass method.

HTTPS – Local User/Pass

Simply choose to enable or disable the Local User/Pass method. There are many options available for controlling user access to the CTPView Web UI. These options can be accessed by a Global Admin via the CTPView Web UI in the Admin Center.

If you elect to disable HTTPS access using the user/pass method be sure that an alternate method of access, such as CAC/PKI or RADIUS/RSA, is operational before proceeding with this selection. Otherwise you may lose all remote access to the

CTPView Web UI. In that event, you would need to connect to the server via SSH to re-establish HTTPS access to the system.

Steel-Belted RADIUS (SBR) Server Configuration

CTPView 3.4 installed on a server using the CentOS operating system provides RADIUS authenticated user login to CTPView via SSH and HTTPS when used in conjunction with a Steel-Belted RADIUS (SBR) server.

To enable this feature you must perform the following steps:

1. "Configure RADIUS/RSA Settings on the CTPView Server"
2. "Configure the SBR Server's Dictionary Files"
3. "Configure the SBR Server's Authentication Policies
4. "Add CTPView as a RADIUS Client on an SBR Server
5. "Add CTPView users to an SBR Server:"

The order of user authentication is:

1. SBR server
2. Local CTPView application

You can configure your SBR server to authenticate both Native and SecurID users. The order of authentication between these two categories of users is set on the SBR server. The same user (that is, user ID) may be added to both the SBR server and the local CTPView application.

See the "AAA Functions" section of this manual for more information on using this method of authentication and authorization.

We have tested this feature using SBR release 6.1. This documentation is also based on that release.

Configure RADIUS/RSA Settings on the CTPView Server

To configure RADIUS settings on the CTPView server see the section "RADIUS/RSA SecurID Configuration" in this manual.

Configure the SBR Server's Dictionary Files

To configure the SBR server's dictionary files:

1. Log in to the SBR server as an administrator.

2. Open the file C:\Program Files\Juniper Networks\Steel-Belted RADIUS\Service\juniper.dct and append the following new block of text to the bottom of the file:

```
#########################################################################
# CTP Specific Attributes
#########################################################################
ATTRIBUTE Juniper-CTP-Group Juniper-VSA(21, integer) r
VALUE Juniper-CTP-Group Read_Only 1
VALUE Juniper-CTP-Group Admin 2
VALUE Juniper-CTP-Group Privileged_Admin 3
VALUE Juniper-CTP-Group Auditor 4
ATTRIBUTE Juniper-CTPView-APP-Group Juniper-VSA(22,integer) r
VALUE Juniper-CTPView-APP-Group Net_View 1
VALUE Juniper-CTPView-APP-Group Net_Admin 2
VALUE Juniper-CTPView-APP-Group Global_Admin 3
ATTRIBUTE Juniper-CTPView-OS-Group Juniper-VSA(23, integer) r
VALUE Juniper-CTPView-OS-Group Web_Manager 1
VALUE Juniper-CTPView-OS-Group System_Admin 2
VALUE Juniper-CTPView-OS-Group Auditor 3
#########################################################################
# CTP Specific Attributes
#########################################################################
```

3. Open the file C:\Program Files\Juniper Networks\Steel-Belted RADIUS\Service\vendor.ini and locate the block of text beginning with the line:
   vendor-product = Juniper M/T Series
4. Add the following new block of text after the Juniper M/T Series block you located above:
   vendor-product = Juniper CTP Series
   dictionary = Juniper
   ignore ports = no
   port-number-usage = per-port-type
   help-id = 2000
5. Restart the Steel-Belted RADIUS service on the server.

Configure the SBR Server's Authentication Policies

To configure the SBR server's authentication policies:

1. Launch the Steel-Belted RADIUS Administrator application from your web browser by typing http://<SBR_IP_ADDRESS>:1812 in the address bar. Click the **Launch** button when the page loads.

2. Select the **Steel-Belted RADIUS > Authentication Policies > Order of Methods** link in the directory frame. Ensure that **Native User** is listed under the section **Active Authentication Methods**.

Add CTPView as a RADIUS Client on an SBR Server

To add CTPView as a RADIUS client on an SBR server:

1. Launch the Steel-Belted RADIUS Administrator application from your web browser by typing http://<SBR_IP_ADDRESS>:1812 in the address bar. Click on the Launch button when the page loads.
2. Select the **Steel-Belted RADIUS > RADIUS Clients** link in the directory frame. Add your CTPView server as a client. In the Make or model field, select Juniper CTP Series from the drop-down menu.

Add CTPView Users to an SBR Server:

To add CTPView users to an SBR server:

1. Launch the Steel-Belted RADIUS Administrator application from your web browser by typing http://<SBR_IP_ADDRESS>:1812 in the address bar. Click on the Launch button when the page loads.
2. Select the **Steel-Belted RADIUS > Users > Native** link in the directory frame. Add a user using the **Add Native User** dialog box.
3. In the Attributes section, click on the **Return List** tab and select the **Add** button. A new dialog box titled **Add Return List Attribute** will open.
    1. In the Attributes section select **Juniper-CTPView_APP-Group**.
    2. In the Value section select the authorization level of the user you are adding. The choices are:
        - Global_Admin
        - Net_Admin
        - Net_View

        See the CTPView documentation for more information about the properties of each of these authorization levels.

RSA SecurID Appliance Configuration

CTPView 3.4 installed on a server using the CentOS operating system provides two-factor authenticated user login to CTPView via SSH and HTTPS when used in conjunction with an

RSA SecurID appliance. The RSA appliance incorporates a Steel-Belted RADIUS (SBR) server, making the configuration here very similar to systems using SBR only.

To enable this feature you must perform the following steps:

1. "Configure RADIUS/RSA Settings on the CTPView Server"
2. "Configure the SBR Server's Dictionary Files"
3. "Configure the SBR Server's Authentication Policies"
4. "Add CTPView as a RADIUS Client on an SBR Server"
5. "Add CTPView users to an SBR Server"
6. "Assign SecurID tokens to CTPView users"

The order of user authentication is:

1. SBR server
2. Local CTPView application

You can configure your SBR server to authenticate both Native and SecurID users. The order of authentication between these two categories of users is set on the SBR server. The same user (that is, user ID) may be added to both the SBR server and the local CTPView application.

See the "AAA Functions" section of this manual for more information on using this method of authentication and authorization.

We have tested this feature using SBR release 6.1. This documentation is also based on that release.

Configure RADIUS/RSA Settings on the CTPView Server

To configure RADIUS settings on the CTPView server see the section "RADIUS/RSA SecurID Configuration" in this manual.

Configure the SBR Server's Dictionary Files

To configure the SBR server's dictionary files:

1. Log in to the SBR server as an administrator.
2. Open the file C:\Program Files\Juniper Networks\Steel-Belted RADIUS\Service\juniper.dct and append the following new block of text to the bottom of the file:

```
##########################################################################
# CTP Specific Attributes
##########################################################################
ATTRIBUTE Juniper-CTP-Group Juniper-VSA(21, integer) r
VALUE Juniper-CTP-Group Read_Only 1
```

```
VALUE Juniper-CTP-Group Admin 2
VALUE Juniper-CTP-Group Privileged_Admin 3
VALUE Juniper-CTP-Group Auditor 4
ATTRIBUTE Juniper-CTPView-APP-Group Juniper-VSA(22,integer) r
VALUE Juniper-CTPView-APP-Group Net_View 1
VALUE Juniper-CTPView-APP-Group Net_Admin 2
VALUE Juniper-CTPView-APP-Group Global_Admin 3
ATTRIBUTE Juniper-CTPView-OS-Group Juniper-VSA(23, integer) r
VALUE Juniper-CTPView-OS-Group Web_Manager 1
VALUE Juniper-CTPView-OS-Group System_Admin 2
VALUE Juniper-CTPView-OS-Group Auditor 3
#########################################################################
# CTP Specific Attributes
#########################################################################
```

3. Open the file C:\Program Files\Juniper Networks\Steel-Belted RADIUS\Service\vendor.ini and locate the block of text beginning with the line:
   vendor-product = Juniper M/T Series
4. Add the following new block of text after the Juniper M/T Series block you located above:
   vendor-product = Juniper CTP Series
   dictionary = Juniper
   ignore ports = no
   port-number-usage = per-port-type
   help-id = 2000
5. Restart the Steel-Belted RADIUS service on the server.

Configure the SBR Server's Authentication Policies

To configure the SBR server's authentication policies:

1. Launch the Steel-Belted RADIUS Administrator application from your web browser by typing http://<SBR_IP_ADDRESS>:1812 in the address bar. Click the **Launch** button when the page loads.
2. Select the **Steel-Belted RADIUS > Authentication Policies > Order of Methods** link in the directory frame. Ensure that **Native User** is listed under the section **Active Authentication Methods**.

Add CTPView as a RADIUS Client on an SBR Server

To add CTPView as a RADIUS client on an SBR server:

1. Launch the Steel-Belted RADIUS Administrator application from your web browser by typing http://<SBR_IP_ADDRESS>:1812 in the address bar. Click on the Launch button when the page loads.
2. Select the **Steel-Belted RADIUS > RADIUS Clients** link in the directory frame. Add your CTPView server as a client. In the Make or model field, select Juniper CTP Series from the drop-down menu.

Add CTPView Users to an SBR Server:

To add CTPView users to an SBR server:

1. Launch the Steel-Belted RADIUS Administrator application from your web browser by typing http://<SBR_IP_ADDRESS>:1812 in the address bar. Click on the Launch button when the page loads.
2. Select the **Steel-Belted RADIUS > Users > SecurID** link in the directory frame. Add a user using the **Add SecurID** dialog box.
3. In the Attributes section, click on the **Return List** tab and select the **Add** button. A new dialog box titled **Add Return List Attribute** will open.
    3. In the Attributes section select **Juniper-CTPView_APP-Group**.
    4. In the Value section select the authorization level of the user you are adding. The choices are:
        - Global_Admin
        - Net_Admin
        - Net_View

        See the CTPView documentation for more information about the properties of each of these authorization levels.

Assign SecurID Tokens to CTPView Users

To assign SecurID tokens to CTPView users, launch the RSA Authentication Manager Host Mode application on the RSA SecurID appliance. From the menu bar, select **User > Add User**. At a minimum, complete these required fields:

- Last Name
- Default Login
- Required to Create a PIN
- Assign Token.

The first time a new user logs in to CTPView, he or she must use the SecurID token Passcode as the password. The user will be prompted to create a PIN. Thereafter, the user must log in using the PIN+Passcode as the password.

How To Use CAC Smart Cards For SSH Access To CTPView

You will need two middleware applications and a smart card reader installed on your WinXP workstation.

The two applications are:

- ActiveClient 6.1 for Common Access Cards from Actividentiy http://www.actividentity.com/products/securityclients/ActivClientforCommonAccessCards/
- Putty-CAC from Dan Risacher http://www.risacher.org/putty-cac/putty.exe or for DoD users from https://software.forge.mil/sf/projects/community_cac.

In order to ensure that users are authenticated using CAC for secure shell connections, you will be instructed to disable username:password SSH access to the nodes. This will prevent other SSH client software on the WinXP workstation which is not CAC capable from being used to by-pass CAC authentication.

The card reader we use is the SCR3310v1 USB Smart Card Reader from SCM Microsystems http://www.scmmicro.com/security/view_product_en.php?PID=4 . Install this device before configuring the ActiveClient. To install the correct driver for your system, attach the reader to your workstation then let WinXP automatically download the driver from the web.

ActiveClient configuration – Initial procedure:

1. Install the software using the default settings.
2. Attach the card reader and insert your CAC card.
3. Start the ActiveClient application.
4. From the menu toolbar, select Tools > Advanced > Configuration. Make these changes, if different from current settings:
    a. Behavior when the card is removed => logoff
    b. Make certificates available to Windows on card insertion => Yes
    c. Remove certificates from Windows on logoff => Yes
    d. Remove certificates from Windows on smart card removal => Yes
5. You may need to reboot your system for the changes to be in effect, you will receive a message if this is the case.
6. Return to the Home screen. In the right pane, double-click on the Smart Card Info icon.
7. Note field labeled “User Name”. This is the same name that is referred to as “Common Name” or “CN” within the CAC certificates.
8. If you made changes to the Advanced Configuration menus that require a system reboot, do it now.

Putty-CAC Configuration – For Each Remote Host:

1. This application is a stand-alone executable. Simply place the file in any folder. For convenience we suggest you add shortcuts from the file to your desktop and quick start taskbar.
2. Open Putty-CAC.
3. In the Category pane select Connection > SSH > Pkcs11.
4. Select the 'Attempt "PKCS#11 smardcard" auth (SSH-2)' checkbox
5. Use the Browse button to complete the input field for "PKCS#11 library for authentication". The file to enter when using ActiveClient is "C:\WINDOWS\system32\acpkcs211.dll".
6. Select the "Token label" for ActiveClient: "Actividentity ActiveClient 0" if you only have one reader attached.
7. Pause a few seconds to allow Putty-CAC to read the CAC card.
8. Select the "Certificate label" to use from the drop down menu.
9. In the Category pane select Session > Logging. For the initial setup we will enable logging in order to read the public key of the user. After setup is complete you can set the logging to "None".
10. Select the "SSH packets" radio button.
11. Select a log file location using the Browse button.
12. Select the "Ask the user every time" radio button.
13. In the Category pane select Session.
14. Enter the IP address of the remote box.
15. By default, Port 22 and SSH connection should already be selected.
16. Enter a name for this connection in the "Saved Sessions" field.
17. Click the Save button.
18. Click the Open button.
19. At the login prompt type the User Name from your CAC card that we found in the ActiveClient section above.
20. The login will fail with the message "Server refused our key". Close the Putty-CAC session.
21. Open the putty.log file in a text editor such as WordPad.
22. Locate the user's public key by searching for the word "token-key". Copy and save the key which starts with "ssh-rsa" and ends with "token-key". We will copy this key string to the remote box. If you have multiple remote hosts to configure, use this same token-key for the additional hosts and skip steps 18 thru 22.
23. Log into the CTPView shell as a System Administrator.
24. Add a new user, using the shell menu utility and this user's User Name. The path to adding a user on CTPView is menu > Security Profile > User Management > Add admin shell accounts.
25. Import the user's public key into CTPView using the cli menu > AAA Functions > SSH – CAC/PKI > Enable SSH CAC/PKI for a user option. See the separate section in the manual for more information on using this option.
26. Return to Putty-CAC on your workstation. Load the Saved Session you created above and click the Open button. At the login prompt enter this user's User Name. You will be prompted for the "Passphrase for smartcard". i.e. the PIN.
27. You should now be connected.

To disable the username:password method of SSH authentication on a host, use the cli menu > AAA Functions > SSH – Local User/Pass option. See the separate section in the manual for more information on using this option. Be aware that after making this change all users will be required to use CAC card access. If that method should fail you must have physical access to the node to log in.

You can require that SSH access to CTPView only originate from authorized workstations. There is a cli menu option for this. The path is menu > System Configuration > Configure Access IP Filtering.