CTPView Management System

Security Deployment Guide

Release 9.0R1
May 2019

TABLE OF CONTENTS

Introduction ................................................................................................................................................ 5
Security Level ........................................................................................................................................ 6
  Security Level Description for Web UI ...................................................................................................................... 6
  low ....................................................................................................................................................................................... 6
  high .............................................................................................................................................................................. 6
  Security Level Description for OS ....................................................................................................................... 6
  very-low ....................................................................................................................................................................... 6
  low ....................................................................................................................................................................................... 6
  high .............................................................................................................................................................................. 6
  Allowed Attribute Ranges ........................................................................................................................................... 7
  Updating Existing User Accounts .............................................................................................................................. 8
    Web UI .......................................................................................................................................................................... 8
    OS ................................................................................................................................................................................ 8
Configuring a New CTPView Server ........................................................................................................ 9
  Default Password ........................................................................................................................................................ 9
  Change the BIOS Menu Password ............................................................................................................................ 9
  Change the Server’s Root Account Password ........................................................................................................... 9
  Review System Security Level ................................................................................................................................... 9
  Change the GRUB Boot Loader Password ............................................................................................................. 10
  Change the MySQL Apache Account Password .................................................................................................... 10
  Change the MySQL Administrator Password ......................................................................................................... 10
  Configuring Network Access ......................................................................................................................................... 10
  Updating the CTPView Software ................................................................................................................................... 11
  Create New Users ..................................................................................................................................................... 11
  Delete Default System Administrator Account ..................................................................................................... 11
Logging into the CTPView Web UI ........................................................................................................................... 11
Create New User Accounts ............................................................................................................................................ 11
Delete Default Global_Admin Account ......................................................................................................................... 12
Add Login Banner ..................................................................................................................................................... 12
Configure AIDE (Advanced Intrusion Detection Environment) ............................................................................. 12
Configure SWATCH (Log Watcher) ........................................................................................................................ 12
Configure Two-Factor Authentication .......................................................................................................................... 12
Install Anti Virus Software ........................................................................................................................................ 12
Baseline Files with SUID Bit Set .............................................................................................................................. 12
Baseline Files with SGID Bit Set .............................................................................................................................. 12

Discussion of Security Enhancements in CTPView .............................................................................................. 13
Security Related Enhancements in CTPView 7.2R1 .............................................................................................. 14

Discussion of Server File System Monitoring ...................................................................................................... 15
WARNING .................................................................................................................................................................. 15

Discussion of CTPView Logging ............................................................................................................................ 15
Summary of Logs ................................................................................................................................ 15
/var/log/acorn_event.log ................................................................................................................................................. 15
/var/log/acorn_gui.log ..................................................................................................................................................... 15
/var/log/audit/audit.log .................................................................................................................................................... 15
/var/log/cron ..................................................................................................................................................................... 15
/var/log/httpd/*log ............................................................................................................................................................ 15
/var/log/maillog ................................................................................................................................................................ 15
/var/log/messages ..................................................................................................................................................... 15
/var/log/mysqld.log .......................................................................................................................................................... 15
/var/log/secure .......................................................................................................................................................... 15
/var/log/snmpd.log .......................................................................................................................................................... 15
/var/www/html/acorn/data/ctp_dbase/ctp_upgrade_log.archive .............................................................................. 15
/var/www/html/acorn/ip/iplist_master ........................................................................................................................... 15
/var/www/html/acorn/server_sync/server_sync_log.archive .................................................................................... 15

Installation of Anti-Virus Software ......................................................................................................... 17
Configuration of AIDE (Advanced Intrusion Detection Environment) ................................................................. 18
### AAA Functions (Authentication, Authorization and Accounting)

<table>
<thead>
<tr>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>CAC/PKI Configuration (HTTPS)</td>
<td>19</td>
</tr>
<tr>
<td>RADIUS/RSA SecurID Configuration (SSH and HTTPS)</td>
<td>20</td>
</tr>
<tr>
<td>TACACS+ Configuration (SSH and HTTPS)</td>
<td>22</td>
</tr>
<tr>
<td>SSH Options</td>
<td>23</td>
</tr>
<tr>
<td>SSH – CAC/PKI</td>
<td>23</td>
</tr>
<tr>
<td>SSH – RADIUS/RSA</td>
<td>24</td>
</tr>
<tr>
<td>SSH – TACACS+</td>
<td>24</td>
</tr>
<tr>
<td>SSH – Local User/Pass</td>
<td>24</td>
</tr>
<tr>
<td>HTTPS Options</td>
<td>25</td>
</tr>
<tr>
<td>HTTPS – CAC/PKI</td>
<td>25</td>
</tr>
<tr>
<td>HTTPS – RADIUS/RSA</td>
<td>25</td>
</tr>
<tr>
<td>HTTPS – TACACS+</td>
<td>25</td>
</tr>
<tr>
<td>HTTPS – Local User/Pass</td>
<td>25</td>
</tr>
</tbody>
</table>

### Steel-Belted RADIUS (SBR) Server Configuration

<table>
<thead>
<tr>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure RADIUS/RSA Settings on the CTPView Server or CTP Device</td>
<td>26</td>
</tr>
<tr>
<td>Configure the SBR Server’s Dictionary Files</td>
<td>26</td>
</tr>
<tr>
<td>SBR Enterprise release 6.1.3 or earlier</td>
<td>26</td>
</tr>
<tr>
<td>SBR Carrier release 7.2.3 or earlier</td>
<td>27</td>
</tr>
<tr>
<td>Configure the SBR Server’s Authentication Policies</td>
<td>27</td>
</tr>
<tr>
<td>Add CTPView or CTP as a RADIUS Client on an SBR Server</td>
<td>28</td>
</tr>
<tr>
<td>Add CTPView or CTP Users to an SBR Server</td>
<td>28</td>
</tr>
</tbody>
</table>

### RSA SecurID Appliance Configuration

<table>
<thead>
<tr>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure RADIUS/RSA Settings on the CTPView Server or CTP Device</td>
<td>29</td>
</tr>
<tr>
<td>Configure the SBR Server’s Dictionary Files</td>
<td>29</td>
</tr>
<tr>
<td>SBR Enterprise release 6.1.3 or earlier</td>
<td>30</td>
</tr>
<tr>
<td>SBR Carrier release 7.2.3 or earlier</td>
<td>31</td>
</tr>
<tr>
<td>Configure the SBR Server’s Authentication Policies</td>
<td>32</td>
</tr>
<tr>
<td>Add CTPView or CTP as a RADIUS Client on an SBR Server</td>
<td>32</td>
</tr>
<tr>
<td>Add CTPView or CTP Users to an SBR Server</td>
<td>32</td>
</tr>
</tbody>
</table>
TACACS+ Server Configuration

For HTTPS access to CTPView, the attributes and their values are

For SSH access to CTPView, the attributes and their values are

For SSH access to CTP devices, the attributes and their values are

Configure the TACACS+ Server's configuration Files

Add CTPView or CTP Users to a TACACS+ Server

How To Use CAC Smart Cards For SSH Access To CTPView

ActiveClient configuration – Initial procedure

Putty-CAC Configuration – For Each Remote Host

UC APL Required Information

Conditions Of Fielding

Mitigation Strategies
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 server running CentOS 7.5 (version 1804).

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, the security enhanced CTPView software can be installed on systems using the Fedora Core 4 or Fedora 9 operating systems, however not all new security features will be available.

Currently CTPView 9.0R1 support is available on CentOS 7.5 v1804. So, to build CTPView 9.0R1, please follow the instructions in CTPView 9.0R1 release notes or contact JTAC for assistance.
Security Level

CTPView provides a configurable set of security related features that an administrator can use to change the overall security level of the system. These features include the ability to modify username and password limitations, login restrictions, inactivity periods and access to diagnostic utilities. The options are assembled into pre-packaged groupings called Security Levels. On CTPView the Web UI and the system OS have their own, separate Security Level setting. System administrators can modify the Security Level settings using the CLI menu utility.

CTPView servers are delivered with the Security Levels for the Web UI and the OS set to Low. All the security certifications which have been earned by the CTPView Management System require that the Security Levels remain at the high level. Additionally, to assure compliance with these certifications, the high-level security feature requirements delineated in the other sections of this guide must also be complied with.

In CTPView installations where you do not require a high level of network security, such as a lab environment, you may choose to adopt a less stringent security setting. Changes in Security Levels can be performed at any time; however it is simplest when done during the initial installation, and before user accounts are added. The procedure for switching Security Level settings is covered in the next section of this guide.

Security Level Description for Web UI

**low**
- Enables permissive username/password restrictions

**high**
- Enables elevated username/password restrictions

Security Level Description for OS

**very-low**
- Enables root login
- Disables session inactivity timeout
- Enables default OS username/password restrictions
- Enables single-user mode login
- Installs tcpdump and hdparm utilities
  (These files must exist in the /tmp directory)

**low**
- Disables root login
- Disables session inactivity timeout
- Enables default OS username/password restrictions
- Enables single-user mode login
- Installs tcpdump and hdparm utilities
  (These files must exist in /tmp directory)

**high**
- Disables root login
- Enables session inactivity timeout
- Enables elevated username/password restrictions
- Disables single-user mode login
- Removes tcpdump and hdparm utilities

**NOTE:** When the OS security level is set to high in CTPView, the CTPView OS user account gets locked if the user does not log in for 35 days.
**Allowed Attribute Ranges**

The allowed ranges of password and user account parameters for different Security Levels are shown in the table below.

Changing the Security Level does not change the attributes of the password or account for existing users. Those parameters can be updated using the procedures described in the next section of this guide.

<table>
<thead>
<tr>
<th>Allowed Attribute Range</th>
<th>Web UI</th>
<th>OS</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Units</strong></td>
<td>high</td>
<td>low</td>
</tr>
<tr>
<td><strong>Password Properties</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Min Length</td>
<td>char</td>
<td>15 - 64</td>
</tr>
<tr>
<td>Max Length</td>
<td>char</td>
<td>15 - 64</td>
</tr>
<tr>
<td>Min Lower Case</td>
<td>char</td>
<td>1 - 10</td>
</tr>
<tr>
<td>Min Upper Case</td>
<td>char</td>
<td>1 - 10</td>
</tr>
<tr>
<td>Min Digits</td>
<td>char</td>
<td>1 - 10</td>
</tr>
<tr>
<td>Min Other</td>
<td>char</td>
<td>1 - 10</td>
</tr>
<tr>
<td>Contains username</td>
<td>--</td>
<td>no</td>
</tr>
<tr>
<td>Checked with cracklib library</td>
<td>--</td>
<td>yes</td>
</tr>
<tr>
<td>Min required new characters</td>
<td>number</td>
<td>5</td>
</tr>
<tr>
<td>Allowed authentication retries</td>
<td>--</td>
<td>1 - 3</td>
</tr>
<tr>
<td>Lockout after login failure</td>
<td>sec</td>
<td>60 - indefinite</td>
</tr>
</tbody>
</table>

| **Account Properties** |        |     |      |              |
| Password reuse limit   | number | 10 - 20, never | 1 - 20, never | 10 | 10 |
| Max time between logins | days | 0 - 60 | 0 - 365 | n/a | n/a |
| Min time between password changes | days | 1 - 30 | 0 - 30 | 1 - 60 | 0 - 99999 |
| Max time new password is valid | days | 5 - 60 | 5 - 365 | 1 - 60 | 1 - 99999 |
| Time start warnings before password expiring | days | 0 - 14 | 0 - 14 | 1 - 7 | 1 - 7 |
| Time after password expiring when access prohibited | days | 14 - 59 | 14 - 59 | 0 - 14 | 0 - 99999 |
Updating Existing User Accounts

Changing the Security Level does not change the attributes of the password or account for existing users. Those parameters can be updated using the procedures described below.

Web UI

Login to the Web UI as a Global Admin and go to the Admin Center.

Modify these global attributes:
- Select Passwords > Password Reuse Limit.
- Select Passwords > Modify Password Requirements.

The easiest way to update the password attributes of existing users is to modify the Groups attributes.
- Select Groups > Modify Group Properties.
  For each Group which you have created on your system adjust the parameters within the new ranges. Make sure to check the “Update current members” checkbox before submitting the form.
- Alternatively, you could individually modify the password requirements on each user account.

OS

Login to the CLI management console as a System Administrator. At the command prompt, type menu. The CTPView Configuration Menu utility will open. Go to Security Profile > Password Management.

Modify these global attributes:
- Select Manage password requirements

Each user must be updated individually for password expiration; there is no group option as in the Web UI. Enter the user name and you will be prompted to enter new values for each of the password parameters.
- Select Manage password expiration details.
Configuring a New CTPView Server

**Default Password**

The default value for ALL passwords on a new CTPView server is **CTPView-2-2**.

**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, when startup dialog is first 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 current BIOS password to continue.

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**: The steps described above are for the Dell R200 server. If you have a different server, refer to our document *CTPView Server with Custom CentOS Build Instructions* for the steps appropriate for your hardware.

**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. The password checking utilities do not enforce compliance when changing the root account password. It is the System Administrator’s responsibility to ensure that the new password complies with the minimum requirements for password complexity.

It is strongly recommended that the new root password meet the High Security Level attributes described in the Security Level section above.

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

**Review System Security Level**

See the main Security Level section above for an overview of this feature.

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 **Security Profile > Modify Security Level > View current security level** to view the current security level of the server.

Use the options in the Security Level Menu to set your server to the desired Web UI and OS security levels.

Changing the Security Level sets the allowed ranges of password and user account attributes from which the System Administrator can select from when creating new user accounts. It does not change the settings on existing user accounts.

**NOTE**: Good security practice requires that the Security Level be set to **high** in production servers.

**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.

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 submenu 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.

NOTE: Access to user accounts will become locked if passwords are allowed to expire. Users will avoid this condition if they login in to the server before their maximum password age is reached. The default maximum age is 99999 days.

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 Juniper.

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 attempt to log in to the server originating from a different IP address used the same username as 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.
NOTE: The lockout period is configurable from the Web UI Admin Center.

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 Juniper account.

Add Login Banner

This is done through the Web UI. 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 SecurID and CAC/PKI smart card access, in addition to username/password authentication. 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 Vexira Antivirus for Linux product with CTPView. See the separate section in this manual 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
Juniper Public

/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

The full scope of the security enhancements available with CTPView can only be enabled when installed on a system running the CentOS 7.5 (v1804) operating system. Only the applications/packages necessary to run CTPView are installed as part of CTPView installation. For example, the server has no X-Windows or desktop applications installed.

The privileged administrator group of users in pre-3.4R3 distributions of CTPView 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 use of sudo creates an audit trail which can be traced back to a specific user. This is not possible if a user was allowed to su to the root account.

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 System Administrators and Auditors:

<table>
<thead>
<tr>
<th>Alias</th>
<th>Expanded Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>tmes</td>
<td>tail –f /var/log/messages</td>
</tr>
<tr>
<td>tsec</td>
<td>tail –f /var/log/secure</td>
</tr>
<tr>
<td>tgui</td>
<td>tail –f /var/log/acorn_gui.log</td>
</tr>
<tr>
<td>taudit</td>
<td>tail –f /var/log/audit/audit.log</td>
</tr>
</tbody>
</table>

User Class Access Summary:

<table>
<thead>
<tr>
<th>User Class</th>
<th>Unix group</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Administrator</td>
<td>server_priv</td>
<td>Access to entire system, root-like privileges</td>
</tr>
<tr>
<td>WebManager</td>
<td>server</td>
<td>Control over web pages and web services</td>
</tr>
<tr>
<td>Auditor</td>
<td>server_log</td>
<td>Read access to logs</td>
</tr>
</tbody>
</table>

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 UI have been assigned to the appropriate user group or groups. Where necessary, System Administrators can obtain enhanced root-like privileges the sudo command.

There are two default Users on new systems running CentOS as received from Juniper. Using these two accounts you can create new users and perform preliminary server and Web UI configuration.

<table>
<thead>
<tr>
<th>Access Method</th>
<th>Default Username</th>
<th>User Class</th>
<th>Group Name</th>
<th>Default Password</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSH / CLI</td>
<td>juniper_sa</td>
<td>System Administrator</td>
<td>server_priv</td>
<td>CTPView-2-2</td>
</tr>
<tr>
<td>Web UI</td>
<td>Juniper</td>
<td>WebManager</td>
<td>Global_Admin</td>
<td>CTPView-2-2</td>
</tr>
</tbody>
</table>

User passwords for the CTPView Web UI are now stored using AES-256 encryption in the MariaDB. 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.

**Security Related Enhancements in CTPView 9.0R1 (carried forward from 7.2R1)**

CTPView behavior is little bit different in CTPView 7.2R1 compared to 7.1 or earlier releases. Following are the changes that are made for all security levels to meet the JITC requirements:

- The CTPView web server page will now display a customizable click-through banner at logon which prevents further activity on the information system unless and until the user executes a positive action to manifest agreement by clicking on a box indicating OK”.
- IP ACL operations for accessing CTPView web app can now be managed from menu by going to menu -> MySQL Functions -> IP ACL Function.
- RC4 ciphers are now removed from the nss and ssl configuration.
- Session.gc_maxlifetime is now set to 900 seconds (15 minutes) in CTPView server’s /etc/php.ini file.
- ServerSignature directive is now set to “Off” in CTPView server’s httpd.conf file.
- All the perl scripts in CTPView will now have TAINt option enabled.
- The CTPView GUI user login authentication is now implemented through OpenSSL instead of NSS.
- The transaction isolation setting is now changed to REPEATABLE-READ in mysql configuration file.
- PAM_faildelay rule is now added in CTPView server’s /etc/pam.d/system-auth file.
- Auditd logging is now enabled for all commands that are run in CTPView.
- Snmpd daemon is now started in CTPView.
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 Web UI administrators using the Web UI. The path is Server > GUI Settings > Server Capacity Warning Trigger Point. The default value is 90%.

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.

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 > 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 daily – 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 daily – not if empty
Log msg: none

/var/log/maillog

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

/var/log/messages

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

/var/log/mariadb.log

Log of MariaDB server
10 backlogs retained
Rotated daily – not if empty
Log msg: ctpview log mysqld.log rotated

/var/log/secure

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

/var/www/html/acorn/data/ctp_dbase/ctp_upgrade_log.archive

Log of CTP node upgrade operations
10 backlogs retained
Rotated daily – 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 Anti-Virus Software

Anti-Virus software which is compatible with the Linux OS and does not require an X-Windows interface is compatible with CTPView.

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, and tiger. 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 its 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.

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 watched, you may leave the existing /etc/swatch/swatch.<log_name>.conf as it is.

5. Start the swatch service:

   `sudo service swatch start`

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 view or modify the AAA functions.

Configuration of the CTPView AAA functions has three major components:

- Configuring the global configuration parameters, for example entering the IP addresses of the RADIUS servers you want to use for authentication.
- Configuring the global configuration parameters, for example entering the IP addresses of the TACACS+ servers you want to use for authentication.
- Then selecting the options which the various access methods will use. For example, enabling HTTPS – CAC/PKI with OCSP certificate validation.

For the initial CTPView server configuration, and for any subsequent modifications, access to the server is gained via an SSH session. The Web UI is the access method normal users will use to manage CTP Nodes once CTPView has been deployed in a production environment.

Three validation mechanisms for SSH and HTTPS access are supported. Validation is processed in this order:

1. CAC Smart Card (PKI certificate)
2. RADIUS* OR TACACS+ based database
3. Locally stored username/password database

   RADIUS also supports “RSA Secure ID” for user authentication.

The first successful validation of your credentials will end the validation process and grant you access to the server.

The sub-sections below contain information on the failover options available for each of the validation methods. In other words, whether the authentication process will end with a validation error or continue to the next validation method.

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 (HTTPS)**

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 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. Note that if you use the CTPView_CA certificate, the self-signed certificate will generate an error in client browsers to the effect that the signing certificate authority is unknown and not trusted. However, you will be able to successfully complete the connection.

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.

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 (SSH and HTTPS)

CTPView installed on a server using the CentOS operating system provides RADIUS authenticated user login when used in conjunction with a compliant RADIUS server. This Guide provides details on configuring a Steel-Belted RADIUS (SBR) server or a RSA SecurID appliance for use with CTPView.

In Release 3.4 we introduced RADIUS access to the CTPView WEB UI. With Release 4.1 we added full support for SSH RADIUS authentication. Both of these RADIUS implementations do not require the user to have a local account on the client device. Previous releases of CTPView only supported an SSH RADIUS implementation which required the user to have a local account on the client device and RADIUS access was not available for the CTPView Web UI.

The CTPView Release 4.1 implementation of SSH RADIUS has been ported to CTPOS Release 6.1. The same SSH RADIUS options described in this Guide are available on a CTP device. There is no HTTPS access to the CTP devices. Configuration of RADIUS on the CTP device is accomplished through the CTPView Web UI. The path is System > Configuration > Node Settings > > RADIUS Settings.

Our SSH RADIUS implementation is PAM based. This enables us to share the RADIUS authentication method with all other access methods on CTPView which are PAM enabled. When the SSH RADIUS method is enabled on CTPView or CTP then console access to that device is also authenticated using RADIUS.

A common RADIUS configuration serves both WEB UI and SSH access methods. The CTPView configuration procedure is described 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. The global RADIUS configuration options are displayed along with their current values.

Select the Initialize 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 for SBR and SecurID configuration help.

Select the 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, and the timeout period in seconds for each RADIUS server.

You can define up to 10 RADIUS servers. If multiple servers are defined the order in which they are tried differing based on whether the user is attempting CTPView access via SSH or via HTTPS. For SSH access the servers are tried in order. For HTTPS access the servers are tried in round-robin fashion. In both cases the process continues until a response is received from a server or the maximum number of tries has been reached for all servers.

The current implementation of RADIUS for HTTPS access does not support IPv6 addresses for the RADIUS server. If you have HTTPS – RADIUS/RSA enabled, you must not have any IPv6 RADIUS server addresses configured. Otherwise the RADIUS authentication feature for HTTPS will not work properly. IPv6 server addresses are supported for SSH - RADIUS/RSA.

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

You may set the number attempts the CTPView server makes to contact the listed RADIUS server with the Retry Attempts option. The allowed range of values is 0 to 9. The retry attempts are made consecutively before moving on to the next server in the list.

When no RADIUS server responds to the login request, the value of the option RADIUS Off-Line Failover determines if the user's login credentials will be passed to the local account login function. If the value of RADIUS Off-Line Failover is set to Not Allowed, then the user will be denied access and the login session will be terminated.

When the RADIUS server responds with a REJECT message to the login request, the value of the option RADIUS Reject Failover determines if the user's login credentials will be passed to the local account login function. Two examples of when a REJECT message would be received are an invalid password or the user does not have an account on the RADIUS server. If the value of RADIUS Reject Failover is set to Not Allowed, then the user will be denied access and the login session will be terminated.

**NOTE**: Either RADIUS or TACACS+ can be enabled for the user authentication and authorization. User needs to disable one to enable other.

**TACACS+ Configuration (SSH and HTTPS)**

CTPView installed on a server using the CentOS operating system provides TACACS+ authenticated user login when used in conjunction with a compliant TACACS+ server. This Guide provides details on configuring a TACACS+ server for use with CTPView.

With CTPView 4.4 release, we added full support for TACACS+ authentication. TACACS+ implementation do not require the user to have a local account on the client device. This is also applicable to CTPView 9.0R1.

The CTPView Release 4.4 implementation of SSH TACACS+ has been ported to CTPOS Release 6.4. The same SSH TACACS+ options described in this Guide are available on a CTP device. There is no HTTPS access to the CTP devices. Configuration of TACACS+ on the CTP device is accomplished through the CTPView Web UI. The path is System > Configuration > Node Settings > > TACACS+ Settings.

Our SSH TACACS+ implementation is PAM based. This enables us to share the TACACS+ authentication method with all other access methods on CTPView which are PAM enabled. When the SSH TACACS+ method is enabled on CTPView or CTP then console access to that device is also
A common TACACS+ configuration serves both WEB UI and SSH access methods. The CTPView configuration is described in this section. The configuration of the TACACS+ server is covered in “TACACS+ Server Configuration” section.

To start the CTPView configuration, go the TACACS+ Configuration menu. The path is menu > AAA Functions > TACACS+ Configuration. The global TACACS+ configuration options are displayed along with their current values.

Select the Initialize Web UI TACACS+ Template Accounts option. This action is only required once, during the initial setup of CTPView as a TACACS+ client. However, repeating this step will have no detrimental effect on the TACACS+ configuration. You will need to input the password for the MySQL Administrator account to complete this step.

To add the CTPView, select the Servers option under TACACS+ configuration menu. The currently configured TACACS+ 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 TACACS+ servers when making modifications to the server list. When prompted, enter the TACACS+ server’s address and the shared secret for each TACACS+ server.

You can define up to 10 TACACS+ servers. If multiple servers are configured, then they will be tried in the same order in which they are defined.

The current implementation of TACACS+ supports both IPV4 and IPv6 for SSH as well as for HTTPS.

The default configuration of CTPView uses 49 as the TACACS+ destination port. You may change this to another port using the Destination Port option in the TACACS+ Configuration menu.

You may set the Time out value, the CTPView server takes to contact the listed TACACS+ server. The allowed range of values is 1 to 60.

When no TACACS+ server responds to the login request, the value of the option TACACS+ Off-Line Failover determines if the user’s login credentials will be passed to the local account login function. If the value of TACACS+ Off-Line Failover is set to Not Allowed, then the user will be denied access and the login session will be terminated.

When the TACACS+ server responds with authentication fail message to the login requested with ‘Invalid username/password’ message, the value of the option TACACS+ Reject Failover determines if the user’s login credentials will be passed to the local account login function. Two examples of when an authentication fail message would be received are an invalid password or the user does not have an account on the TACACS+ server. If the value of TACACS+ Reject Failover is set to Not Allowed, then the user will be denied access and the login session will be terminated.

NOTE: Either RADIUS or TACACS+ can be enabled for the user authentication and authorization. User needs to disable one to enable other.

**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 users 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 to the CTPView server, or to check which users have accounts, use the Security Profile option in CTPView CLI menu. The path is menu > Security Profile > User Management. The username for the CTPView account MUST exactly match the CAC username (sometimes listed as CN or Common Name).

The System Administrator must import, by the copy and paste method, the CAC/PKI public certificate for each CAC/PKI user. From the AAA Functions > SSH (1st) - CAC/PKI menu 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 during SSH authentication.

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**

Beginning with CTPView Release 4.1 users are not required to have a local user account on the CTPView server. This is also applicable to CTPView 9.0R1.

For CTPView Release 4.0 and earlier, 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.

See the general RADIUS discussion above for details on configuring the failover behavior of RADIUS.

**SSH – TACACS+**

Beginning with CTPView Release 4.4, users can be authenticated using the TACACS+ server also in the same way as authenticated using the RADIUS/RSA server. This is also applicable to CTPView 9.0R1.

Simply choose to enable or disable the TACACS+ option. The path is menu > AAA Functions > SSH(2nd) RADIUS/RSA: Disabled, TACACS+: - Disabled - Rem Acct > TACACS+. There is no configuration required for the individual users. To block a specific user from gaining access, you must disable that user on the TACACS+ server.

You may set the Time out value, the CTPView server takes to contact the listed TACACS+ server. The allowed range of values is 1 to 60.

You can see the section “TACACS+ Configuration (SSH and HTTPS) above for details on configuring the failover behavior of TACACS+.

**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 Security Profile > User Management menu.

If you elect to disable SSH access using the user/pass method is sure that an alternate method of access, such as CAC/PKI, RADIUS/RSA and TACACS+, 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.
HTTPSOptions

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 CAC/PKI 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 for failover to the next configured login methods.

CTPView will check if the user PKI certificate 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 certificatedatabase.

There is no failover between the OCSP and CRL methods. If designate the OCSP method of revocation checking and 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

You can 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 server.

See the general RADIUS discussion above for details on configuring the failover behavior of RADIUS.

HTTPS – TACACS+

You can choose to enable or disable the TACACS+ 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 TACACS+ server.

You can see the section “TACACS+ Configuration (SSH and HTTPS) above for details on configuring the failover behavior of TACACS+.

HTTPS – Local User/Pass

You can 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, RADIUS/RSA or TACACS+, 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. Enhancements for the SSH method were added in CTPView Release 4.1. This is also applicable to CTPView 9.0R1.

CTP devises running CTPOS 6.1 or later also have the same enhanced SSH RADIUS authentication as CTPView Release 4.1 or later. This section of the Guide is applicable to configuring a RADIUS server for either CTPView or CTP user authentication.

To enable this feature, you must perform the following steps:

1. “Configure RADIUS/RSA Settings on the CTPView Server or CTP device”
2. “Configure the SBR Server’s Dictionary Files”
3. “Configure the SBR Server’s Authentication Policies”
4. “Add CTPView or CTP as a RADIUS Client on an SBR Server”
5. “Add CTPView or CTP users to an SBR Server:”

The order of user authentication, subject to the configuration of the client device, is:

1. SBR server
2. Local user account

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.

Configure RADIUS/RSA Settings on the CTPView Server or CTP Device

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

SBR Enterprise release 6.1.4 and SBR Carrier release 7.2.4 already include the requisite CTP-series/CTPView RADIUS attributes. Skip this step if you are using either of these or later releases.

SBR Enterprise release 6.1.3 or earlier:

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
```
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.

SBR Carrier release 7.2.3 or earlier:

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

2. Create a new file C:\Program Files\Juniper Networks\Steel-Belted RADIUS\Service\juniperctp.dct and copy the following text into it:

   #################################################################
   # Juniperctp.dct - Radius dictionary for Juniper CTP Series devices
   # (See README.DCT for more details on the format of this file)
   #################################################################
   # Use the Radius specification attributes
   #
   @radius.dct
   #################################################################
   # CTP Specific Attributes
   #################################################################

   MACRO Juniper-VSA(t,s) 26 [vid=2636 type1=%t% len1=+2 data=%s%
   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-GroupNet_View 1
   VALUE Juniper-CTPView-APP-GroupNet_Admin 2
   VALUE Juniper-CTPView-APP-GroupGlobal_Admin 3
   VALUE Juniper-CTPView-APP-GroupNet_Diag 4
   ATTRIBUTE Juniper-CTPView-OS-Group-Juniper-VSA(23, integer)r
   VALUE Juniper-CTPView-OS-GroupWeb_Manager 1
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 = Juniperctp
   ignore ports = no
   port-number-usage= per-port-type
   help-id = 2000

5. Open the file C:\Program Files\Juniper Networks\Steel-Belted RADIUS\Service\dictiona.dcm and locate the line “@juniper.dct”.

6. Insert the following new line, then save the change.

   @juniperctp.dct

7. 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 or CTP 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 dropdown menu.

Add CTPView or CTP 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.
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. There are 3 CTP/CTPView groups available to which a user can be assigned. A single user can be assigned to any or all the available groups. The user’s level of authorization is configured separately in each assigned group.

For HTTPS access to CTPView, in the Attributes section select Juniper-CTPView-APP-Group.

In the Value section select the authorization level of the user you are adding. The choices are:
- Global_Admin
- Net_Admin
- Net_View
- Net_Diag

For SSH access to CTPView, in the Attributes section select Juniper-CTPView-OS-Group.

In the Value section select the authorization level of the user you are adding. The choices are:
- Auditor
- System_Admin
- Web_Manager

For SSH access to CTP devices, in the Attributes section select Juniper-CTP-Group.

In the Value section select the authorization level of the user you are adding. The choices are:
- Admin
- Auditor
- Privileged_admin
- Read_Only

See the CTPView and CTP 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. Enhancements for the SSH method were added in CTPView Release 4.1. This is also applicable to CTPview9.0R1.

CTP devices running CTPOS 6.1 or later also have the same enhanced SSH RADIUS authentication as CTPView Release 4.1 or later. This section of the Guide is applicable to configuring a RADIUS server for either CTPView or CTP user authentication.

To enable this feature, you must perform the following steps:

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

The order of user authentication, subject to the configuration of the client device, is:
1. SBR server
2. Local user account

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.

**Configure RADIUS/RSA Settings on the CTPView Server or CTP Device**

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**

SBR Enterprise release 6.1.4 and SBR Carrier release 7.2.4 already include the requisite CTP-series/CTPView RADIUS attributes. Skip this step if you are using either of these or later releases.

**SBR Enterprise release 6.1.3 or earlier:**

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
VALUE Juniper-CTPView-APP-Group Net_Diag 4
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
```

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:

```
# CTP Specific Attributes
```

SBR Enterprise release 6.1.3 or earlier:

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
VALUE Juniper-CTPView-APP-Group Net_Diag 4
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
```

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:
5. Restart the Steel-Belted RADIUS service on the server.

SBR Carrier release 7.2.3 or earlier:

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

2. Create a new file \Program Files\Juniper Networks\Steel-Belted RADIUS\Service\juniperctp.dct and copy the following text into it:

```plaintext
# Juniperctp.dct - Radius dictionary for Juniper CTP Series devices
# (See README.DCT for more details on the format of this file)
# Use the Radius specification attributes
#
@radius.dct
```

```plaintext
# CTP Specific Attributes

MACRO Juniper-VSA(t,s) 26 [vid=2636 type1=%t% len1=+2 data=%s%]
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
VALUE Juniper-CTPView-APP-Group Net_Diag 4
```

3. Open the file \Program Files\Juniper Networks\Steel-Belted RADIUS\Service\vendor.ini and locate the block of text beginning with the line:

   ```plaintext
   vendor-product = Juniper M/T Series
   dictionary = Juniper
   ignore ports = no
   port-number-usage = per-port-type
   help-id = 2000
   ```

4. Add the following new block of text after the Juniper M/T Series block you located above:

   ```plaintext
   vendor-product = Juniper CTP Series
dictionary = Juniperctp
ignore ports = no
port-number-usage = per-port-type
```
5. Open the file C:\Program Files\Juniper Networks\Steel-Belted RADIUS\Service\dictionary.dcm and locate the line “@juniper.dct”.

6. Insert the following new line, then save the change.

@juniperctp.dct

7. 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 or CTP 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 or CTP 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. There are 3 CTP/CTPView groups available to which a user can be assigned. A single user can be assigned to any or all the available groups. The user’s level of authorization is configured separately in each assigned group.

For HTTPS access to CTPView, in the Attributes section select Juniper-CTPView-APP-Group.

In the Value section select the authorization level of the user you are adding. The choices are:

- Global_Admin
- Net_Admin
- Net_View
- Net_Diag
For SSH access to CTPView, in the Attributes section select **Juniper-CTPView-OS-Group**.

In the Value section select the authorization level of the user you are adding. The choices are:

- Auditor
- System_Admin
- Web_Manager

For SSH access to CTP devices, in the Attributes section select **Juniper-CTP-Group**.

In the Value section select the authorization level of the user you are adding. The choices are:

- Admin
- Auditor
- Privileged_admin
- Read_Only

See the CTPView and CTP documentation for more information about the properties of each of these authorization levels.
TACACS+ Server Configuration

CTPView 9.0R1 installed on a server using the CentOS operating system provides TACACS+ authenticated user login to CTPView via SSH and HTTPS when used in conjunction with a TACACS+ server.

To enable this feature, you must perform the following steps:

1. Configure the TACACS+ Server’s configuration Files
2. Add CTPView or CTP users to an TACACS+ Server

The order of user authentication, subject to the configuration of the client device is:

1. TACACS+ server
2. Local user account

The same user may be added to both the TACACS+ server and the local CTPView application.

Any TACACS+ server compliance to TACACS+ RFC 'draft-grant-tacacs-02.txt' version 1.78 can be used.

TACACS+ server version v1.2 can be downloaded from http://tacacs.net/download.asp.

This version of TACACS+ server contains the four configuration files:

a) Authentication.xml - This file is used to add a new user on TACACS+ server.

To add a new user, you must add the new ‘UserGroup’ under ‘UserGroups’ tag: -

```
<UserGroup>
  <Name>TACACS_User1</Name>
  <AuthenticationType>File</AuthenticationType>
  <Users>
    <User>
      <Name>TACACS_User1</Name>
      <LoginPassword ClearText="PASSWORD" DES=""></LoginPassword>
    </User>
  </Users>
</UserGroup>
```

b) Authorization.xml - This file is used to set the authorization level for the users.

To add the authorization level for the user added in the authentication file above, you need to add ‘Authorization’ tag under ‘Authorizations’ tag: -

```
<Authorization>
  <UserGroups>
    <UserGroup>TACACS_User1</UserGroup>
  </UserGroups>
  <Services>
    <Service>
      <Set>service=juniper_ctp_srvc</Set>
      <Set>protocol=unknown</Set>
      <Set>juniper_ctpview_https=1</Set>
    </Service>
  </Services>
</Authorization>
```
The service used for TACACS+ is \textit{juniper_ctp_srvc}. User can't change this service type and have to use this service only to access TACACS+. The protocol used for the TACACS+ is unknown. You cannot change the protocol values too.

To assign the authorization level, there are 3 CTP/CTPView groups available to which a user can be assigned.

\begin{itemize}
  \item [a)] CTP Device CLI - SSH
  \item [b)] CTPView CLI - SSH
  \item [c)] CTPView Web - HTTPS
\end{itemize}

A single user can be assigned to any or all the available groups. The user’s level of authorization is configured separately in each Set tag under Service tag.

\textbf{For HTTPS access to CTPView, the attributes and their values are: -}

In the Set tag under Service tag add the authorization level of the user you are adding. The choices are:

\begin{itemize}
  \item \texttt{"juniper_ctpview_https=1"} (Global_Admin)
  \item \texttt{"juniper_ctpview_https=2"} (Net_Admin)
  \item \texttt{"juniper_ctpview_https=3"} (Net_View)
  \item \texttt{"juniper_ctpview_https=4"} (Net_Diag)
\end{itemize}

\textbf{For SSH access to CTPView, the attributes and their values are: -}.

In the Set tag under Service tag add the authorization level of the user you are adding. The choices are:

\begin{itemize}
  \item \texttt{"juniper_ctpview_cli=1"} (WebManager)
  \item \texttt{"juniper_ctpview_cli=2"} (System Admin)
  \item \texttt{"juniper_ctpview_cli=3"} (Auditor)
\end{itemize}

\textbf{For SSH access to CTP devices, the attributes and their values are: -}

In the Set tag under Service tag add the authorization level of the user you are adding. The choices are:

\begin{itemize}
  \item \texttt{"juniper_ctp_cli=1"} (Read_Only)
  \item \texttt{"juniper_ctp_cli=2"} (Admin)
  \item \texttt{"juniper_ctp_cli=3"} (Privileged_admin)
  \item \texttt{"juniper_ctp_cli=4"} (Auditor)
\end{itemize}

c) Clients.xml – This file is used to add the secret key and the domains that can use the TACACS+ server’s service.

d) Tacplus.xml – This file contains the remote port number and the IPV4/IPv6 IP address assigned to TACACS+ server.

The steps to configure the TACACS+ configuration files are described in the next section.

\textbf{Configure the TACACS+ Server’s configuration Files:}

1. Log in to the TACACS+ server as an administrator.

2. Open the file tacplus.xml and modified the block of text in the file:

\begin{verbatim}
<Port>49</Port>
\end{verbatim}
49 is the default port for the TACACS+. You can change the port number also.

In LocalIP tag, you need to mention the IP of your TACACS+ server machine. You can give IPV4 or IPV6 IP address.

**NOTE**: For IPV6 address, both the TACACS+ server machine and CTPView Server/CTP Device must support IPV6.

3. Restart the TACACS+ service on the server.

**Add CTPView or CTP Users to a TACACS+ Server:**

In TACACS+, the authentication and authorization is separately handled using different files.

Please find below the snapshot when two users **TACACS_User1** and **TACACS_user2** with password **password1** and **password2** are configured.

**Authentication.xml**:

```xml
  <UserGroups>
    <UserGroup>
      <Name>TACACS_User1</Name>
      <AuthenticationType>File</AuthenticationType>
      <Users>
        <User>
          <Name>TACACS_User1</Name>
          <LoginPassword ClearText="" DES=""/>
        </User>
      </Users>
    </UserGroup>
    <UserGroup>
      <Name>TACACS_User2</Name>
      <AuthenticationType>File</AuthenticationType>
      <Users>
        <User>
          <Name>TACACS_User2</Name>
          <LoginPassword ClearText="" DES=""/>
        </User>
      </Users>
    </UserGroup>
  </UserGroups>
</Authentication>
```
Authorization.xml:

```xml
<?xml version="1.0" encoding="utf-8"?>
<Authorizations xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xmlns:xsd="http://www.w3.org/2001/XMLSchema">
    <Authorizations>
    <Authorization>
        <UserGroups>
            <UserGroup>TACACS_User1</UserGroup>
        </UserGroups>
        <Services>
            <Service>
                <Set>service=juniper_ctp_srvc</Set>
                <Set>protocol=unknown</Set>
                <Set>juniper_ctpview_https=1</Set>
            </Service>
        </Services>
    </Authorization>
    <Authorization>
        <UserGroups>
            <UserGroup>TACACS_User2</UserGroup>
        </UserGroups>
        <Services>
            <Service>
                <Set>service=juniper_ctp_srvc</Set>
                <Set>protocol=unknown</Set>
                <Set>juniper_ctp_cli=2</Set>
            </Service>
        </Services>
    </Authorization>
    </Authorizations>
</Authorizations>
```

**Note:** You need to re-start the TACACS+ service each and every time you change some configuration in any of the above files.

**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 Actividentity
  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

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. OpenPutty-CAC.
3. In the Category pane select Connection > SSH > Pkcs11.
4. Select the “Attempt “PKCS#11 smartcard” 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.

UC APL Required Information

Conditions Of Fielding

When the system is deployed into an operational environment, the following security measures (at a minimum)
must be implemented to ensure an acceptable level of risk for the site’s Designated Accrediting Authority (DAA):

a. The system must be incorporated in the site’s PKI. If PKI is not incorporated, the following findings will be
included in the site’s architecture:
   • DSN18.10 for CTPView Application (Juniper CTPView Network Management)
   • NET0445 for CTPView Application (Juniper CTPView Network Management)

b. The site must use a SysLog device for auditing purposes.

c. IP forwarding is enabled between devices with a restrictive Access Control List (ACL). If the system is not
deployed in this manner, then the following findings will be included in the site’s architecture:
   • GEN003600 for all CTP 150’s and CTP 2000’s

d. The site must only use the web interface (CTPView platform) for management. If the solution is managed
in any other way, then the following findings will be applicable to the solution:
   • DSN 13.17 and DSN18.10
   • NET0445

e. The configuration must be in compliance with the Juniper CTP military-unique features deployment guide.
f. The site must register the system in the Systems Networks Approval Process Database
   <https://snap.dod.mil/index.cfm> as directed by the Defense IA/Security Accreditation Work Group
   (DSAWG) and Program Management Office.

Mitigation Strategies

Nonerequired.