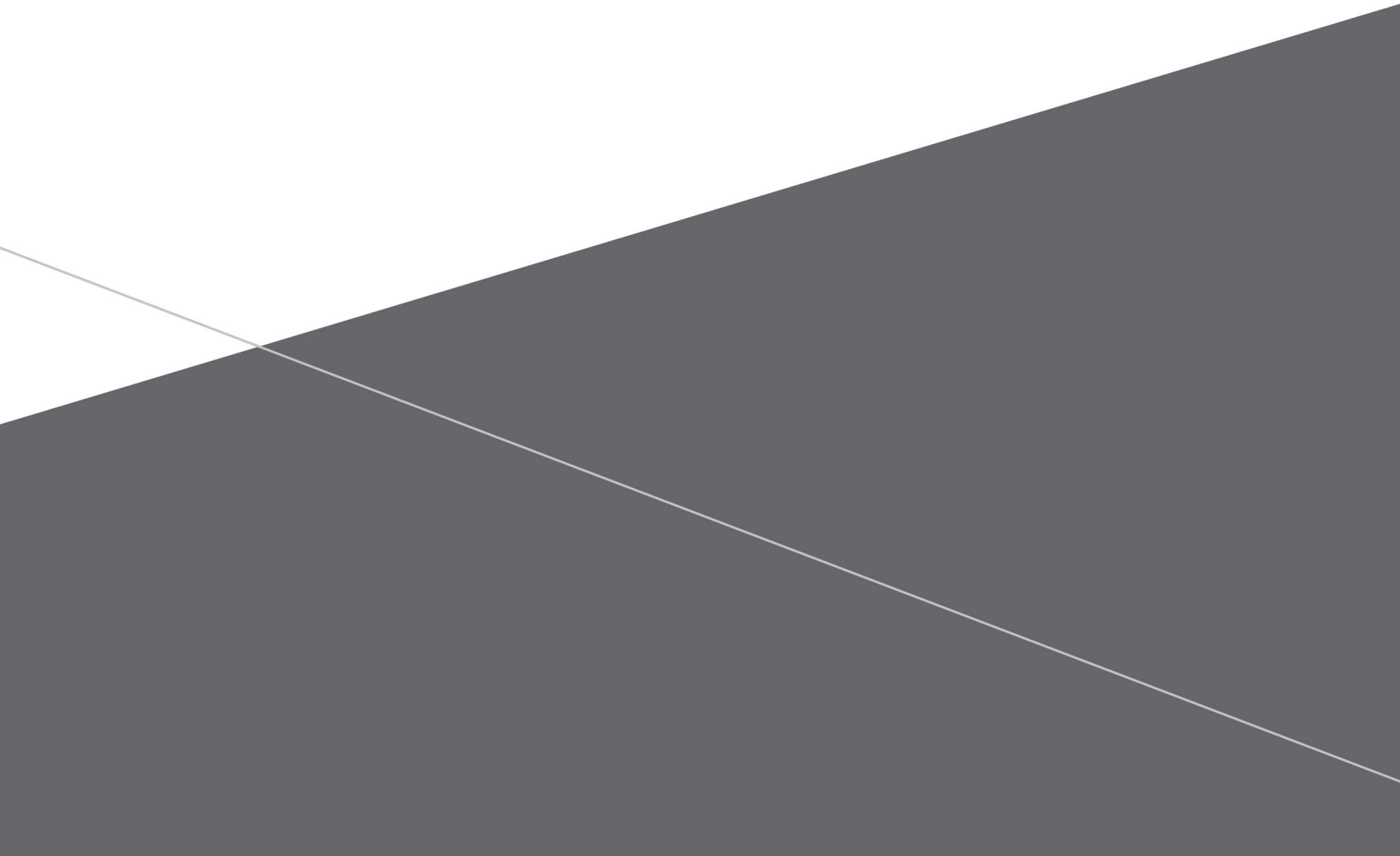


COMMON CRITERIA CONFIGURATION GUIDANCE

ARUBA CLEARPASS POLICY MANAGER

Version 6.11

March 2023



This document serves as a supplement to the official Aruba user guidance documentation, consolidating configuration information specific to the Common Criteria Collaborative Protection Profile for Network Devices (CPP_ND_V2.2e) and Extended Package for Authentication Servers (PP_NDCC_APP_AUTHSVR_EP_V1.0).

This document contains configuration examples from ClearPass Policy Manager. When possible, all examples will be shown using the graphical user interface (Web UI) rather than command line interface (CLI) commands. Instances where no Web UI can be used to configure a setting will use CLI commands.

This document is intended to augment the existing ClearPass Policy Manager User Guide (available at <https://www.arubanetworks.com/techdocs/ClearPass/6.11/PolicyManager/index.htm>). When applicable, the document will direct back to the official User Guide. Common Criteria evaluation was performed against the 6.11 version of the document. Once submitted, this document will be available at:

<https://asp.arubanetworks.com/downloads;products=Aruba%20ClearPass%20Policy%20Manager%20%28CPPM%29>

SUPPORT INFORMATION

For support on your Aruba Networks systems, contact Aruba Technical Support through the Aruba Support Portal (<https://asp.arubanetworks.com/>) web site.

DOCUMENT CHANGE HISTORY

Version	Release Date	Description
1.0	August 2017	Initial approved release ClearPass Policy Manager v6.6.7
1.1	September 2017	Updated to ClearPass Policy Manager v6.6.8
1.2	December 2017	Additional guidance to IPsec settings
2.0	June 2018	Updated to ClearPass Policy Manager v6.7.3
3.0	June 2020	Updated to reflect changes required with NDcPPv2.1 and ClearPass Policy Manager version 6.9
4.0	July 2020	Additional guidance around use of X9.62/SECG curve over 256-bit prime field or NIST/SEGC curve over 521-bit prime field
4.1	August 2022	Removed additional notes from FMT_SMR.2.3
5.0	March 2023	Updated to reflect changes required with NDcPPv2.2e and ClearPass Policy Manager version 6.11. Syslog examples updated throughout.

COPYRIGHT/TRADEMARK INFORMATION

The trademarks, logos and service marks (“Marks”) displayed on this Web Site are the property of Hewlett Packard Enterprise, or other third parties. Users are not permitted to use these Marks without the prior written consent of Aruba, a Hewlett Packard Enterprise company or such third party which may own the Mark.

Hewlett Packard Enterprise’s Marks are valuable assets of the company that signify Hewlett Packard Enterprise’s cutting edge, innovative, and high-quality products. The following is a list of Hewlett Packard Enterprise’s Marks in the United States and certain other countries. This list may not necessarily be complete and all-inclusive. The absence of any mark from this list does not mean that it is not a Hewlett Packard Enterprise mark.

©2023 Hewlett Packard Enterprise Development LP.

Contents	
Support Information	2
Document Change History	2
Copyright/Trademark Information.....	2
Configuration	5
AGD_OPE.1	5
Baseline Setup Requirements.....	6
Passwords and Accounts.....	6
FCS_CKM.1 - Enable FIPS 140-2 Mode.....	6
FCS_CKM.4 – Cryptographic Key Destruction	7
Configure System Time.....	7
Configure Audit Export	8
Establish Password Policy Enforcement.....	11
FIA_X509_EXT.1/Rev (Install Certificates).....	11
Enable Ingress Events Processing	13
Verify Local User Repository is available.....	13
Enable Common Criteria Mode	15
FMT_SMR.2.3	16
FIA_AFL.1.2.....	16
Disable Admin User and Local User Account	16
FTP_ITC.1(1)	18
Add Network Access Devices	20
Configuring RadSec	23
Configure Notifications.....	23
Continued Guidance Configuration	25
FIA_UIA_EXT.1	25
FIA_X509_EXT.1/Rev.....	25
FIA_X509_EXT.2.2	25
FIA_X509_EXT.3.1	25
FPT_TUD_EXT.1.3	26
FMT_SMF.1.1.....	27
FTA_SSL.3 / FTA_SSL.4 / FTA_SSL_EXT.1.1	27
FTA_TAB.1	28
FTP_ITC.1.....	29
FCS_SSHS_EXT.1.2.....	29
FCS_SSHS_EXT.1.4.....	29
FCS_SSHS_EXT.1.5.....	30
FCS_SSHS_EXT.1.6.....	30
FCS_SSHS_EXT.1.7.....	30
FCS_SSHS_EXT.1.8.....	30
FCS_TLSS_EXT.2.1	30
FCS_TLSS_EXT.2.2.....	31
FCS_TLSS_EXT.1.2.....	35

FCS_IPSEC_EXT.1	36
FCS_IPSEC_EXT.1.3	41
FCS_IPSEC_EXT.1.4	41
FCS_IPSEC_EXT.1.5	41
FCS_IPSEC_EXT.1.6	42
FCS_IPSEC_EXT.1.7	42
FCS_IPSEC_EXT.1.8	42
FCS_IPSEC_EXT.1.11	42
FCS_IPSEC_EXT.1.14	42
FIA_PSK_EXT.1	42
FAU_STG_EXT.1	42
FTA_TSE.1	44
FPT_TST_EXT.1 (self-tests)	49
FCS_EAP-TLS_EXT.1	50
Appendix A: FAU_GEN.1 Auditable Events	50
Appendix B	83
IPsec Traffic Selector Rules	83
Encrypt Rules	83
Bypass Rules	83
Drop Rules	83
Final Rule	83
Processing Order	84

CONFIGURATION

Configuration of ClearPass Policy Manager (herein referred to as ClearPass) to conform to Common Criteria evaluated configuration is broken into two primary sections. The first section is for initial configuration and entering into the high-level Common Criteria Mode. This will establish the primary configuration requirements of NDCPP version 2.2e and NDCPP_APP_AUTHSVR_EP version 1.0. The second section will outline any remaining configurations or individual notes from Common Criteria configuration for individual settings, to perform optional configurations.

AGD_OPE.1

ClearPass has been evaluated for compliance with Common Criteria Collaborative Protection Profile for Network Devices (CPP_ND_V2.2e) and Extended Package for Authentication Servers (PP_NDCC_APP_AUTHSVR_EP_V1.0). The limits of this evaluation are documented in the Security Target (ST) as submitted during certification.

Cryptographic limits documented through this document will ensure that the ClearPass appliance is configured to use only approved ciphers and algorithms. Without these configurations, there are additional capabilities that are capable of being used that were not evaluated as part of the Common Criteria process. To ensure that only approved cryptographic functionality is enabled, ClearPass must be configured to use both FIPS140-2 and Common Criteria Mode when operating to limit functionality to evaluated capabilities.

The Aruba ClearPass Access Management System™ includes several components. The Policy Manager component has been evaluated by Common Criteria for all the security functions indicated by the protection profiles. Many of the other components were outside of scope, including features that require additional licenses.

ClearPass includes a reporting system known as Insight. Insight does not perform any security functions that were within scope for Common Criteria evaluation. The interface has been evaluated as part of Common Criteria only due to the same functionality being shared between Insight and Policy Manager.

The Guest functionality provides workflows for allowing guest users to access networks. Guest functionality was not within Common Criteria evaluation scope. The interface has been evaluated as part of Common Criteria only due to the same functionality being shared between it and Policy Manager. Similarly, the RADIUS functionality within Guest has been evaluated as part of Common Criteria only due to the same functionality being shared between Guest and Policy Manager.

The add-on Onboard functionality provides a certificate authority (CA) for use with device authentication. Onboard functionality was not within Common Criteria evaluation scope. The interface has been evaluated as part of Common Criteria only due to the same functionality being shared between it and Policy Manager. No Onboard CA functionality should be considered evaluated by Common Criteria.

The add-on OnGuard functionality provides endpoint posture checking capabilities for use with Policy Manager. OnGuard policy is configured within Policy Manager but has not been evaluated by Common Criteria in any capacity.

ClearPass includes the ability to actively or passively profile endpoints and network devices. This functionality is configured within Policy Manager but has not been evaluated by Common Criteria in any capacity.

ClearPass makes use of a digital signature whenever updates/upgrades are applied to the system, regardless of the package size or intent. All ClearPass systems store a copy of the package-signing public key. When a new package is to be installed, the server will load the package onto the server and then validate the signing key against the stored copy of the public key. If the cryptographic signatures are identical, then the update process is allowed to proceed. If the signatures do not match, then the package update will fail with an error message indicating that the package has failed to validate.

To reduce the potential of errors in systems downloading packages manually from <https://support.arubanetworks.com> or <https://asp.arubanetworks.com>, it is also recommended to validate the package hash and compare against the published

values from the download site prior to loading onto ClearPass. While this process was not evaluated as part of Common Criteria evaluation, it is helpful in updates to systems without direct internet connections.

Applying patches to ClearPass can be performed by direct connection or manual upload of the patch for non-Internet connected systems. Navigate to **Administration > Agents and Software Updates > Software Updates** to install patches. To manually install patches, first the patch must be loaded to the ClearPass server by clicking the button **Import** Updates under **Firmware & Patch Updates**. The interface box will upload the patch to the appropriate directory for installation. Installation will then proceed as the Internet connected systems once the patch has been downloaded to the system.

Internet connected systems may download the patches through **Firmware & Patch Updates** section by clicking the **Download** button to download the patch, then **Install** to install the patch. Most patches will require a reboot once installed. ClearPass has been evaluated for Common Criteria using a single node. Patching of clusters is outside the scope of the evaluation and should follow regular documentation processes for applying patches to clusters.

BASELINE SETUP REQUIREMENTS

Passwords and Accounts

During initial setup, administrators are allowed to specify the initial password for use with the CLI and Web UI accounts. While minimum complexity and length requirements exist, they are not considered strong or secure passwords for ongoing use. It is recommended that the following guidelines be followed for establishing a more secure password to be used:

- Require a minimum password length of at least 15 characters
- Make use of upper case, lower case, numerical values, and allowed special characters in all passwords
- Passwords are not based on dictionary words (unless passphrases longer than 22 characters are used)
- Secure common passwords (such as CLI users) in a secure location with restricted access.

Examples of special characters include: ! @ # \$ % ^ & * ()

Initial setup will create two accounts: appadmin for CLI/SSH access and admin for Web UI access. Both use the same password initially. Aruba recommends securing the appadmin account for emergency access if the core authentication services become unavailable.

After initial setup, the administrator should create individual accounts for all the administrators and no longer use the default Web UI account or password. Directions to perform this can be found in the [Managing Admin Users](#) section of the ClearPass Policy Manager User Guide. Navigate to **Administration > Users and Privileges > Admin Users** to create and modify administrator accounts. Administrator accounts should always have strong passwords set.

Administrator permissions are limited to users with appropriate roles. In compliance with FMT_MTD.1, only administrators should have access to the security management functionality on the system. General users are not required to have local accounts defined.

FCS_CKM.1 - Enable FIPS 140-2 Mode

As noted in AGD_OPE.1, the evaluated configuration requires FIPS 140-2 mode to be enabled. Configurations that do not apply this requirement may use cryptographic capabilities that were not evaluated or tested during the Common Criteria evaluation process.

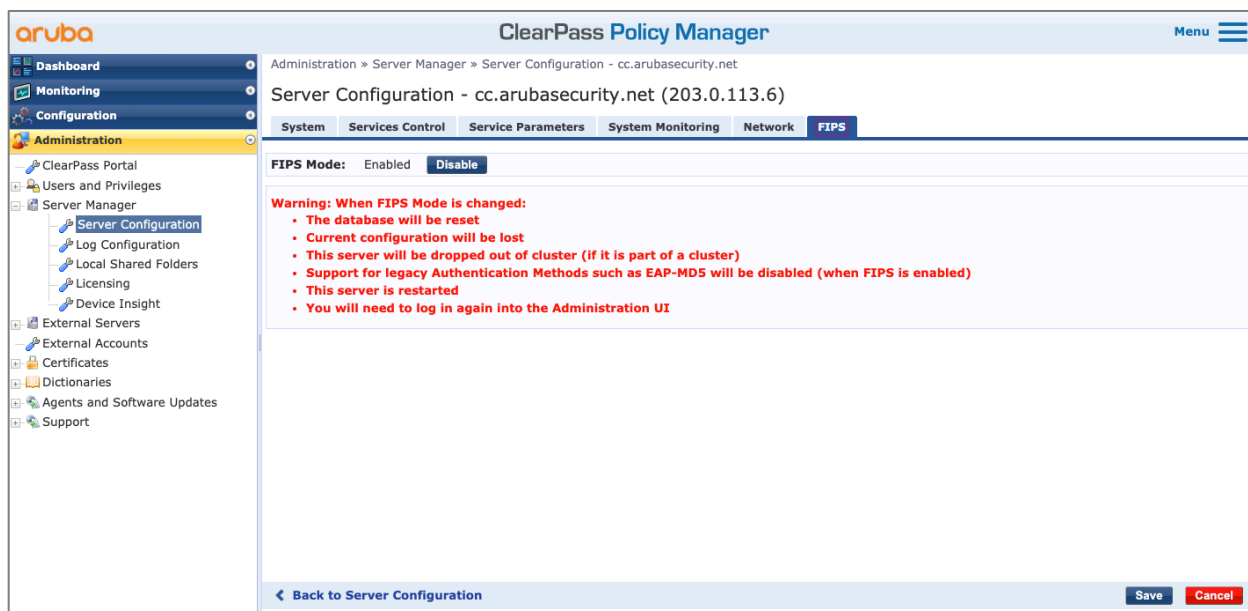
Enabling the FIPS 140-2 mode may be accomplished during installation or after installation. Performing the transition after installation will reset the system configuration, and is not recommended.

During initial setup through the command line interface (CLI), the administrator is prompted with the following option:

```
Do you want to enable FIPS mode? [y|n]: _
```

Answering yes to this question enables the system to operate using FIPS 140-2 algorithms only from initial configuration.

After installation, to enable FIPS mode, open ClearPass Policy Manager. Navigate to **Administration > Server Manager > Server Configuration** and select the server in the list. Select the **FIPS** tab, and then click the **Enable** button in the **FIPS Mode** field, as shown below.



Post-installation conversions require a reboot when enabling FIPS mode before continuing with the configuration process.

FCS_CKM.4 – Cryptographic Key Destruction

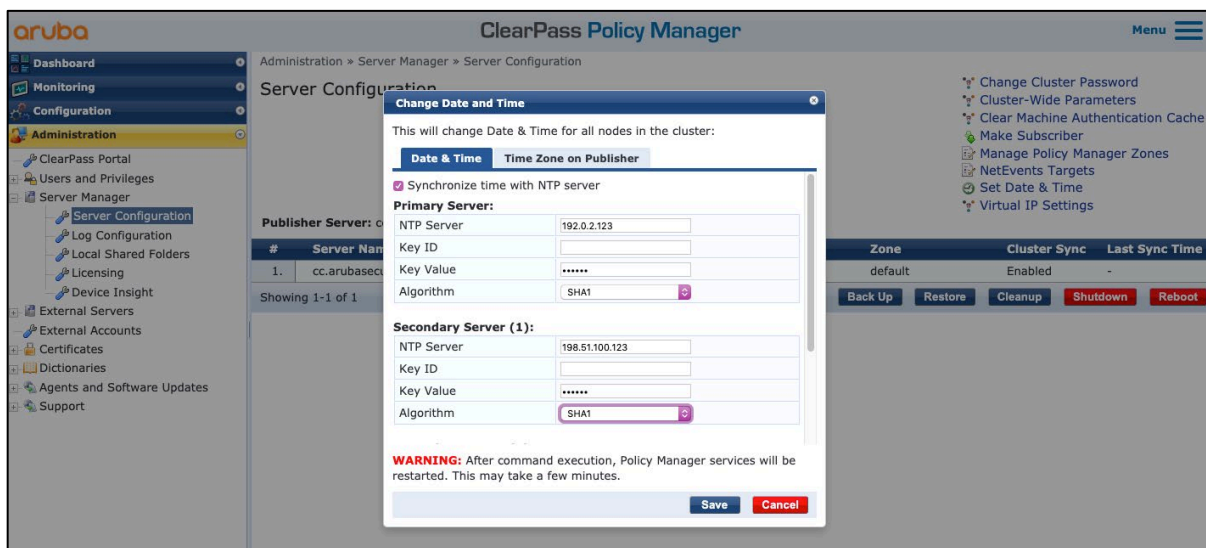
Cryptographic key destruction is performed automatically. There are no administrator prerequisites to meet this requirement. There are no circumstances that do not strictly conform to the key destruction requirement and there are no situations where key destruction may be delayed at the physical layer.

Configure System Time

It is important to set the system date and time prior to continuing. Certificates will be based off validity durations that can be affected by changes in date/time. To manually configure time on ClearPass, navigate to **Administration > Server Manager > Server Configuration**, and select the option **Set Date & Time** in the upper right corner.



Time and date settings can be entered using the **Date & Time** tab. The **Time zone on publisher** tab can be used to set the time zone of the server. Time can be set manually, or using the **Synchronize time with NTP server** option.



NTP use was configured during Common Criteria evaluation in compliance with FCS_NTP_EXT.1 requirements. NTP servers must support NTPv4 to work. The Web UI allows a minimum of one (1) NTP server to be used, but it is recommended to specify at least three (3) NTP servers. The Web UI allows the specification of 1-5 NTP servers. When configuration is performed with NTP the communication between appliance and NTP server should be configured to a secure key and hash algorithm to ensure the communication is not modified. Only SHA-1 is allowed for a CC evaluated configuration. The NTP service does not accept multicast or broadcast NTP information, there are no configuration options to change this behavior.

In cases where NTP servers cannot support secure hash algorithms IPsec encapsulation is recommended.

When the date and/or time are modified, the system will restart services and require a re-login to the UI.

Configure Audit Export

ClearPass has limited storage available to retain logs. Aruba recommends exporting all the audit logs to an external source. The recommended process to accomplish this is via syslog export. Because log information may be sent to multiple syslog receivers, there are two places that syslog export must be configured on ClearPass.

Exporting all ClearPass audit information begins with specifying the configuration at the system level. Navigate to **Administration > Server Manager > Log Configuration**, and select the **System Level** tab. Specify the IP address of the syslog server in the appropriate space.

Administration > Server Manager > Log Configuration

Log Configuration

You can specify the default log level for each service and its modules and the number and size of log files you need to maintain for each service.

Select Server: CPPM-611-130

Service Log Configuration System Level

Number of log files: 12 (default is 12 files)

Limit each log file size to: 50 MB (default is 50 MB)

Syslog Settings:

Syslog Server: []

Syslog Server Port: 514 (default is 514)

Service Name	Enable Syslog	Syslog Filter Level	Default Level
1. Admin server	<input checked="" type="checkbox"/>	WARN	WARN
2. AirGroup notification service	<input type="checkbox"/>	WARN	WARN
3. Apache web server	<input checked="" type="checkbox"/>	All	ALL
4. ClearPass IPsec service	<input type="checkbox"/>	WARN	WARN
5. ClearPass network services	<input checked="" type="checkbox"/>	WARN	WARN
6. Domain service	<input type="checkbox"/>	All	ALL
7. Guest/Onboard	<input checked="" type="checkbox"/>	WARN	WARN
8. Micros Fidello FIAS	<input type="checkbox"/>	WARN	WARN
9. Policy server	<input checked="" type="checkbox"/>	WARN	WARN
10. RadSec service	<input checked="" type="checkbox"/>	WARN	WARN
11. Radius server	<input checked="" type="checkbox"/>	WARN	WARN
12. Syslog client service	<input checked="" type="checkbox"/>	WARN	WARN
13. TACACS+ server	<input type="checkbox"/>	WARN	WARN

Restore Defaults Save

Select the components desired to export by selecting the **Enable Syslog** option for the appropriate services. To ensure maximum audit compliance, it is recommended to enable syslog for all services. To capture all Common Criteria related audit messages, the RADIUS server should be configured to display audits to the DEBUG level.

Note: The ClearPass IPsec service is now included in the list of services whose service logs can be sent to a syslog server, and is available in the Service Name list on the **Administration > Server Manager > Log Configuration > System Level** tab.

At least one syslog receiver must be defined for general use. Navigate to **Administration > External Servers > Syslog Targets** and click **Add** in the upper right corner.

Administration > External Servers > Syslog Targets

Syslog Targets

ClearPass can export session data, audit records, and event records. This information can be sent to one or more syslog target servers.

Filter: Host Address contains Go Clear Filter

Show 20 records

#	Host Address	Description

Add Syslog Target

Host Address: []

Description: []

Protocol: UDP TCP

Server Port: 514

Save Cancel

The syslog target IP address should be specified, along with the protocol and port to send to. The default value for syslog is to use UDP port 514. Further information on Common Criteria recommended deployments of syslog is available in section FTP_ITC.1.1(1).

Once the target is defined, the data to be transmitted needs to be specified. Navigate to **Administration > External Servers > Syslog Export Filters**, and click **Add** in the upper right corner. A total of three (3) filters are required to send the data to the syslog server(s).

aruba ClearPass Policy Manager

Administration » External Servers » Syslog Export Filters » Add

Syslog Export Filters

General Summary

Name: Audit record export

Description: Syslog export of all the Audit Record

Export Template: Audit Records

Include Audit Entity Details: Enable to include EntityData field that provides the audit entity details in XML format

Export Event Format Type: RFC 5424

Local Facility Level: Local Use 1 (local!)

Syslog Servers: 192.0.2.145 Remove View Details Modify Add New Syslog Target

ClearPass Servers: If specified, syslog messages will only be sent from the selected ClearPass servers. Otherwise, it will be sent from all ClearPass servers in the cluster. Remove --Select to Add--

Back to Syslog Filters Next Save Cancel

The first filter will need to use the *Audit Records Export Template*. Specify the syslog target from the available list to note the receiver. The **Export Event Format Type** offers the choice between Standard, LEEF, CEF, and RFC 5424. It is not required to specify the ClearPass Servers that this filter will be applied to unless using a cluster. Clusters were not evaluated by Common Criteria.

The second filter must use the *System Events Export Template*. Specify the syslog target from the available list to note the receiver.

The final filter will need to use the *Session Logs Export Template*. Specify the syslog target from the available list to note the receiver. Unlike the first two filters, session logs require a second set of information to be included.

aruba ClearPass Policy Manager

Administration » External Servers » Syslog Export Filters » Add

Syslog Export Filters

Syslog filter has not been saved

General Filter and Columns Summary

Option 1: For common use-cases, select Data Filter and Columns for export:

Data Filter: [All Requests] Modify Add New Data Filter

Columns Selection:

Predefined Field Groups -

- Logged in users
- Failed Authentications
- RADIUS Accounting
- TACACS+ Administration
- TACACS+ Accounting
- Web Authentication
- Guest Access

Available Columns -

Type: Common

- Common.Request-Timestamp
- Common.Roles
- Common.Service
- Common.Session-Log-Timestamp
- Common.Source
- Common.System-Posture-Token
- Common.Username

Selected Columns -

- Common.Alerts
- Common.Alerts-Present
- Common.Audit-Posture-Token
- Common.Auth-Type
- Common.Connection-Status
- Common.Enforcement-Profiles
- Common.Error-Code
- Common.Host-MAC-Address
- Common.Login-Status
- Common.Monitor-Mode
- Common.NAS-IP-Address
- Common.NAS-Name
- Common.NAS-Port
- Common.Request-Id

Option 2: For advanced use-cases, specify custom SQL query for export:

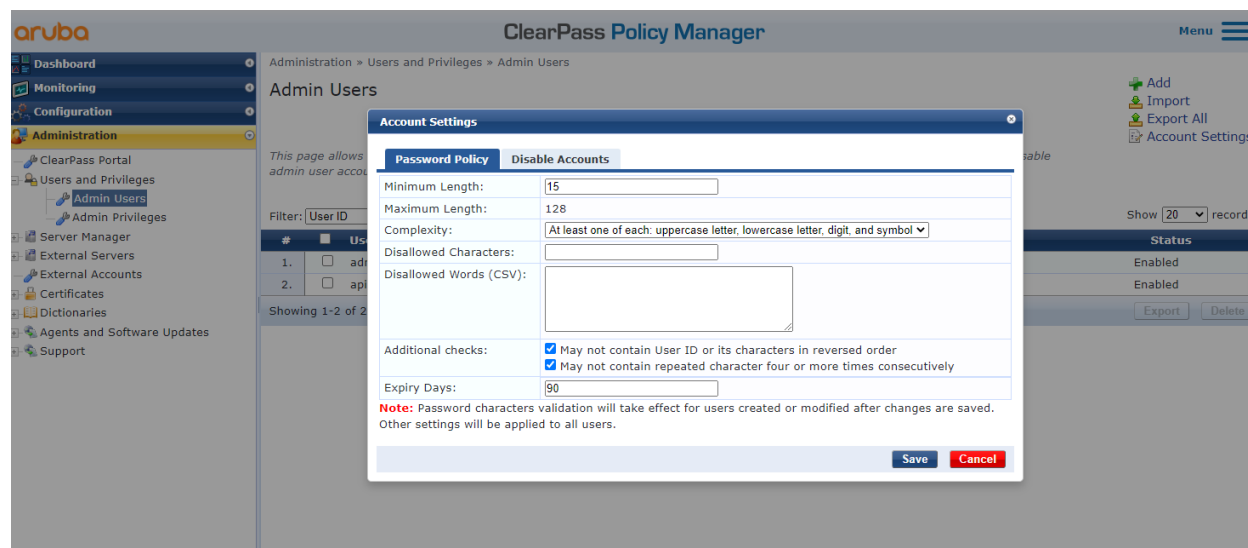
Custom SQL:

Back to Syslog Filters Next Save Cancel

The **Filters and Columns** tab allows the two options to be specified when selecting the information to export. It is recommended to use the first option. Specifying the **Data Filter** of *[All Requests]* will capture all session related information. The recommended deployment is to select all available columns from the Common type selection.

Establish Password Policy Enforcement

ClearPass uses a default password policy that requires only a six (6) character password length with no password complexity requirements. The password policy allows passwords with six (6) to one hundred (100) characters for Web UI accounts and six (6) to one hundred twenty-eight (128) characters for SSH/CLI access. This may create confusion to administrators that may attempt to use different password length maximums, it is recommended that a maximum of 100-character password length be used. A future release will align this maximum to two hundred fifty-six (256) characters as are enforced maximums for all passwords. To ensure compliance with Common Criteria evaluated configuration, the defaults should be changed to have a higher security setting. Navigate to **Administration > Users and Privileges > Admin Users**, and then select the option **Account Settings** in the upper right corner.



The **Minimum Length** value has been modified to fifteen (15) characters. **Complexity** is set to require **At least one of each: uppercase letter, lowercase letter, digit, and symbol**. The **Additional Checks** have both been selected to prevent user ID or reversed user ID, or repeating characters four (4) or more times in the password. The **Expiry Days** have been set to ninety (90) days to force administrative users to change their passwords regularly.

FIA_X509_EXT.1/Rev (Install Certificates)

The use of self-signed certificates is not allowed in Common Criteria configurations. It is recommended to use certificates from trusted issuers in all cases, but rigidly enforced when enabling Common Criteria mode. ClearPass will not allow administrators to enable Common Criteria Mode without externally, certificate authority (CA) signed HTTPS and RADIUS certificates installed.

By default, ClearPass generates self-signed certificates for the RADIUS, HTTPS, and Database servers. All certificates will need to be replaced with certificates that are signed by a trusted certificate authority (CA). Begin the process by navigating to **Administration > Certificates > Trust List**. Ensure that the CA root is listed and enabled in the available list.

Administration > Certificates > Trust List

Certificate Trust List

This page displays a list of trusted Certificate Authorities (CA). You can add, view, or delete a certificate.

Filter: Subject contains [] Go Clear Filter Show 20 records

#	Subject	Usage	Validity	Enabled
1.	<input type="checkbox"/> CN=AddTrust External CA Root,OU=AddTrust External TTP Network,O=AddTrust AB,C=SE	AD/LDAP Servers, Endpoint Context Servers, SAML, SMTP, Others	Valid	Enabled
2.	<input type="checkbox"/> CN=Alcatel Contact Center Solutions,OU=PKI Authority,O=Alcatel,C=FR	Others	Valid	Disabled
3.	<input type="checkbox"/> CN=Alcatel Enterprise Solutions,OU=PKI Authority,O=Alcatel,C=FR	Others	Valid	Disabled
4.	<input type="checkbox"/> CN=Alcatel IP Touch,OU=PKI Authority,O=Alcatel,C=FR	Others	Valid	Disabled
5.	<input type="checkbox"/> CN=Aruba Networks Trusted Computing Root CA 1.0,C=US,O=Aruba Networks,OU=Operations,OU=DeviceTrust	Aruba Infrastructure	Valid	Disabled
6.	<input type="checkbox"/> CN=Certum CA,O=Unizeto Sp. z o.o.,C=PL	Others	Valid	Disabled
7.	<input type="checkbox"/> CN=COMODO High-Assurance Secure Server CA,O=COMODO CA Limited,L=Salford,ST=Greater Manchester,C=GB	Others	Valid	Disabled
8.	<input type="checkbox"/> CN=DigiCert Global Root CA,OU=www.digicert.com,O=DigiCert Inc,C=US	Others	Valid	Disabled
9.	<input type="checkbox"/> CN=DigiCert Global Root G2,OU=www.digicert.com,O=DigiCert Inc,C=US	AD/LDAP Servers, Endpoint Context Servers, SAML, SMTP, Others	Valid	Enabled
10.	<input type="checkbox"/> CN=DigiCert High Assurance EV Root CA,OU=www.digicert.com,O=DigiCert Inc,C=US	Others	Valid	Disabled
11.	<input type="checkbox"/> CN=DoD Root CA 2,OU=PKI,OU=DoD,O=U.S. Government,C=US	Others	Valid	Disabled
12.	<input type="checkbox"/> CN=DST Root CA X3,O=Digital Signature Trust Co.	Others	Valid	Disabled
13.	<input type="checkbox"/> CN=Entrust.net Certification Authority (2048),OU=(c) 1999 Entrust.net Limited,OU=www.entrust.net/CPS_2048_incorp. by ref. (limits liab.),O=Entrust.net	Others	Valid	Disabled
14.	<input type="checkbox"/> CN=Entrust Root Certification Authority,OU=(c) 2006 Entrust, Inc.,OU=www.entrust.net/CPS is incorporated by reference,O=Entrust, Inc.,C=US	Others	Valid	Disabled

To enable a CA, click its row in the list to open the **View Certificate Details** window. Select the **Enable** button to enable a trusted CA. If the required CA certificate is not loaded in ClearPass, it can be manually imported by selecting the **Add** button in the top right of the **Certificate Trust List** screen.

Certificate usage must be enabled for the CA certificate to be used. If the certificate is enabled, but not allowed for use with the specific system it will not be considered valid for those services. Common Criteria evaluated services were limited to functions required for validation: EAP (for RADIUS communication), HTTPS (for Web UI administration), Database (required to enable CC mode), RadSec (TLS encrypted RADIUS communication), SAML (for testing with FCS_TLSS_EXT.2 / FCS_TLSS_EXT.2.5 only), and other (for IPsec).

When using a CA that is not listed in the available trust list, the CA's public certificate must be imported. Imported CAs will automatically be enabled during the import process. Imported CA certificates cannot be self-signed when using Common Criteria mode.

Then, to update a ClearPass certificate, navigate to **Administration > Certificates > Server Certificate** and select the desired server certificate from the **Select Type** drop down list. The new certificate can then be imported by using the **Import Server Certificate** link, or a new Certificate Signing Request (CSR) can be made by using the **Create Certificate Signing Request** link.

When this process is completed for one certificate, the other can be completed. After the **RADIUS/EAP Server Certificate**, **HTTPS Server Certificate**, and **Database Server Certificate** are not self-signed, the process can continue.

Please note that the type of certificate used will influence which ciphers are available later. For example, RSA certificates will not be able to perform ECDSA based ciphers, so those encryption options will automatically be disabled.

The following list is all the allowed hash and encryption types that may be used for either HTTPS or RADIUS server certificates when operating in CC Mode:

Encryption: RSA

Size: 2048-bit, 3072-bit, or 4096-bit

Hash: SHA256, SHA384, or SHA512

Encryption: ECDSA

Size: NIST/SECG curve over 384-bit prime field

Size: NIST/SECG curve over 521-bit prime field

Size: X9.62/SECG curve over 256-bit prime field

Hash: SHA256, SHA384, or SHA512

Note: While listed as possible, the X9.62/SECG curve over 256-bit prime field is not a CC approved encryption type and should not be used. The NIST/SECG curve over 521-bit prime field was not evaluated.

The type of key will be used to automatically determine the available cipher suites. Cipher suites cannot be manually modified for use from those listed in FCS_TLSS_EXT.2.1 later in this document.

Attempts to generate a CSR or load a certificate with sizes below the specified thresholds will fail. The UI will fail to complete the CSR generation, it will continue to spin in the waiting state.

The ClearPass system must be restart after configuring the Database Server Certificate. Navigate to **Administration > Server Manager > Server Configuration** and select the option **Reboot** in the lower right area.

Enable Ingress Events Processing

To properly track events related to IPsec processing or HTTP daemon logging, ClearPass must be configured to process these events. Each node within a cluster (if applicable) must repeat the following process.

Navigate to **Administration > Server Manager > Server Configuration** and select the server/node from the list. From the **System** tab, enable the **Enable Ingress Events Processing on this server** option.

The screenshot shows the 'Server Configuration' page for a server named 'cppm226'. The 'System' tab is selected, and the 'Enable Ingress Events Processing' checkbox is checked. The page also shows configuration options for IP addresses and subnets for Management and Data/External ports.

	IPv4	IPv6	Action
Management Port	IP Address	10.2.55.226	Configure
	Subnet Mask	255.255.255.0	
	Default Gateway	10.2.55.1	
Data/External Port	IP Address		Configure
	Subnet Mask		
	Default Gateway		

A warning message appears when enabling this option indicating the process is a CPU-intensive- operation. The impact of this engine for these events is within acceptable limits; click **Yes** to continue. Without this, several later components will be impacted. This includes FCS_IPSEC_EXT.1, FCS_SSHC_EXT., and FCS_SSHS_EXT.1.

After enabling ingress events processing on the server/node, open the **Services Control** tab and validate the **Ingress logger service** and **Ingress logrepo service** (position 11) services are both running. If they have not automatically started, click the **Start** button to complete the process.

Verify Local User Repository is available

At **Configuration > Services**, the service **[Policy Manager Admin Network Login Service]** is enabled by default in position one (1). Ensure the Local User Repository is available when performing initial deployment until all remote authentication sources are validated.

Configuration » Services

Services

This page shows the current list and order of services that ClearPass follows during authentication and authorization.

Filter: [Name] contains [] Go Clear Filter Show 20 records

#	Order	Name	Type	Template	Hit Count	Status
1.	1	[Policy Manager Admin Network Login Service]	TACACS+	TACACS+ Enforcement	-	✖
2.	2	[AirGroup Authorization Service]	RADIUS	RADIUS Enforcement (Generic)	-	✔
3.	3	[Aruba Device Access Service]	TACACS+	TACACS+ Enforcement	-	✔
4.	4	[Guest Operator Logins]	Application	Aruba Application Authentication	-	✔
5.	5	[Insight Operator Logins]	Application	Aruba Application Authentication	-	✔
6.	6	[Device Registration Disconnect]	WEBAUTH	Web-based Authentication	-	✔

Showing 1-6 of 6 Reorder Copy Export Delete

Ensure the rule **[Policy Manager Admin Network Login Service]** is listed at the top. Select the rule's row in the list to view its details.

Configuration » Services » Edit - [Policy Manager Admin Network Login Service]

Services - [Policy Manager Admin Network Login Service]

Summary Service Authentication Roles Enforcement

Service:

Name: [Policy Manager Admin Network Login Service]
 Description: Service for access to Policy Manager Admin for network users
 Type: TACACS+ Enforcement
 Status: Enabled
 Monitor Mode: Disabled
 More Options: -

Service Rule

Match ANY of the following conditions:

Type	Name	Operator	Value
1.	Connection	NAD-IP-Address	EQUALS 127.0.0.1

Authentication:

Authentication Sources: 1. [Local User Repository] [Local SQL DB]
 2. [Admin User Repository] [Local SQL DB]
 Strip Username Rules: -

Roles:

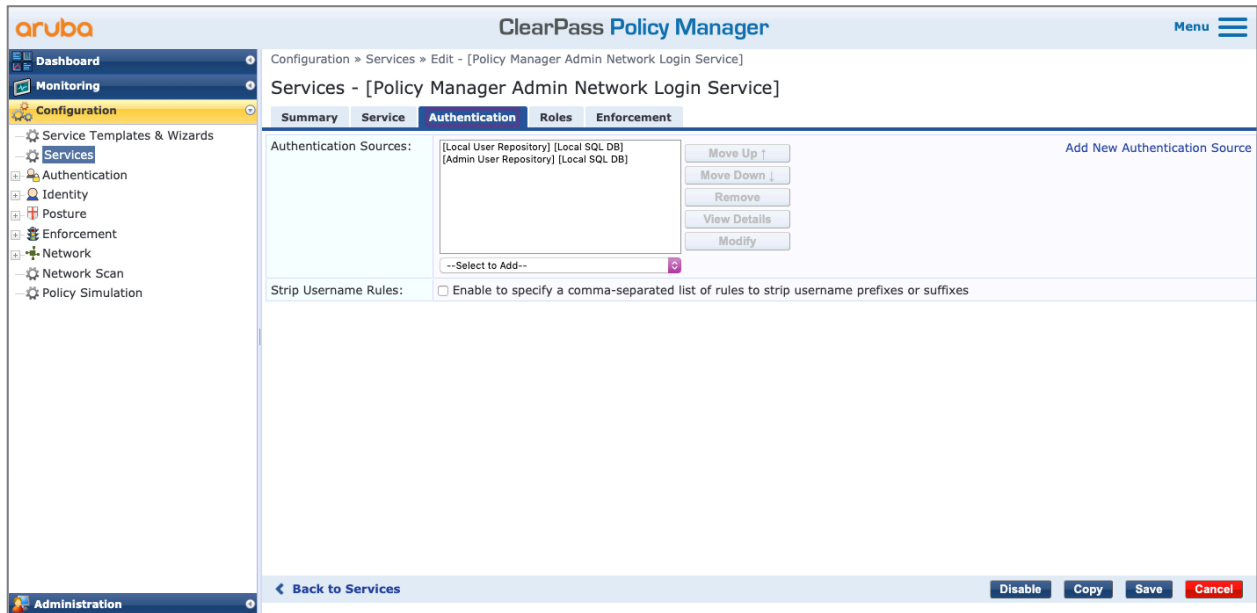
Role Mapping Policy: -

Enforcement:

Use Cached Results: Disabled
 Enforcement Policy: [Admin Network Login Policy]

◀ Back to Services Disable Copy Save Cancel

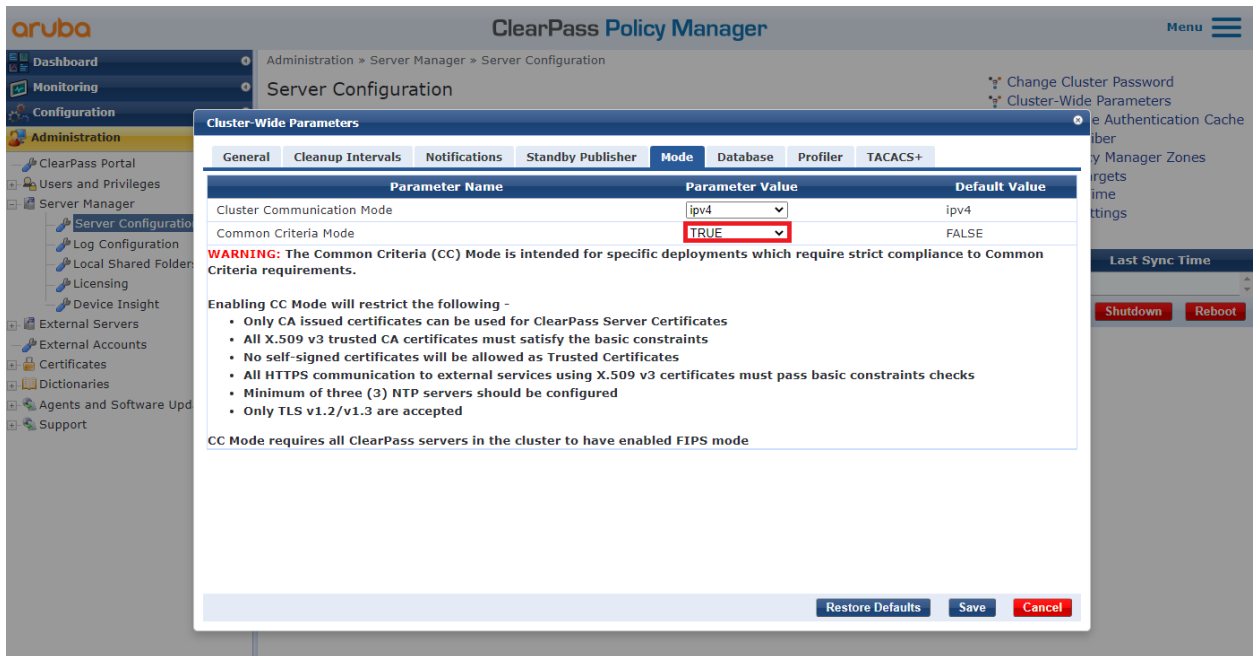
On the **Summary** tab, the **Authentication Sources** field must include **[Local User Repository]** prior to enabling Common Criteria mode or an administrator may be locked out.



From the **Authentication** tab, if the default service is not used, ensure the **[Local User Repository]** value has been added to the service. In the **Authentication Sources** field, use the drop-down menu and buttons to add to or reorder the list of available authentication sources.

Enable Common Criteria Mode

To enable Common Criteria mode through the Web UI, navigate to **Administration > Server Manager > Server Configuration**, select the **Cluster-Wide Parameters** link, and then select the **Mode** tab, as shown below.



While Common Criteria mode is supported by ClearPass clusters, it has been evaluated as a single, non-clustered server for certification.

FMT_SMR.2.3

Once Common Criteria mode is enabled, the list of ciphers available for use is limited to those specified within the Security Target (ST). ClearPass console access does not require further changes to access it in this mode. Most modern Web browsers support the available ciphers without further configuration. SSH clients that are not configured to support only FIPS 140-2 approved cryptographic ciphers will need to have ciphers re-prioritized to use the ones allowed by ClearPass or connections will not establish.

FIA_AFL.1.2

SSH access can be locked after a specified number of failed attempts for a configurable length of time. By default, SSH lockout is not enabled. To enable SSH lockout, one of the following commands should be executed:

```
ssh lockout count <N>
ssh lockout duration <N minutes>
```

Where the value of *<N>* is the number of failed login attempts, or the value of *<N minutes>* is the length of time the lockout will be enabled for. Example: To trigger a lockout after 3 failed attempts for a 30-minute window, the following commands would be executed:

```
ssh lockout count 3
ssh lockout duration 30
```

Unlocking the SSH account can be accomplished only from the console, or from another SSH session that is authorized using public key authentication. To reset the SSH lockout, the following command must be executed:

```
ssh unlock
```

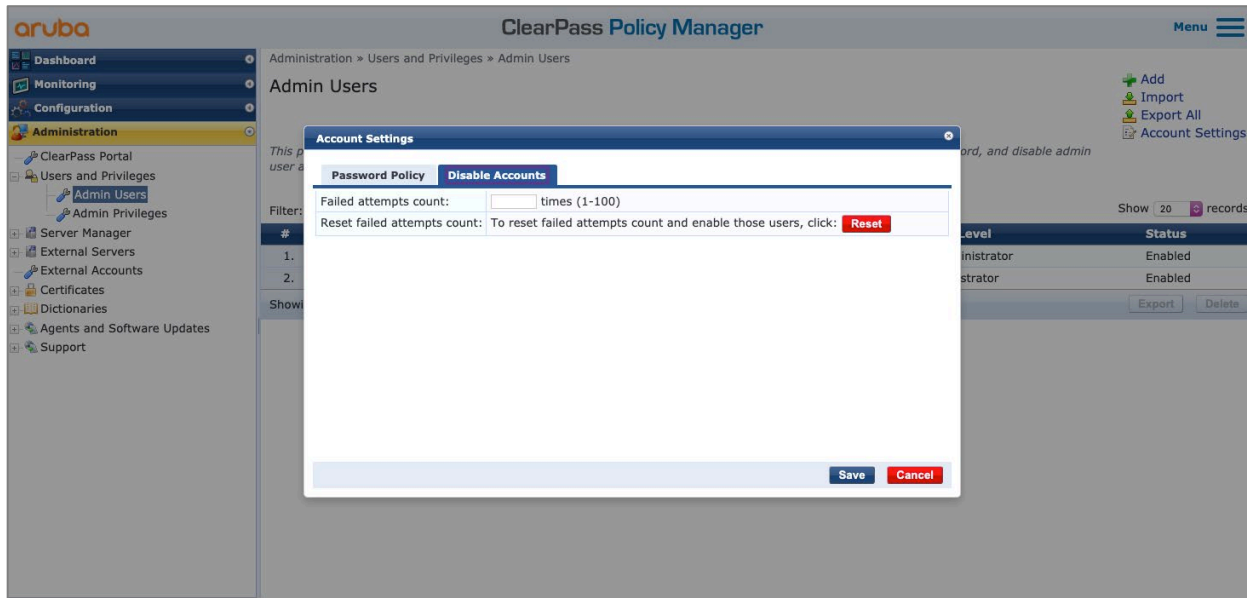
By default, when the account is locked, you can perform this operation by logging in to the system via the console or from a host that is enabled for SSH public key authentication with ClearPass. The lockout capability can be extended to include SSH public key authentication by executing the following command:

```
ssh lockout mode advanced
```

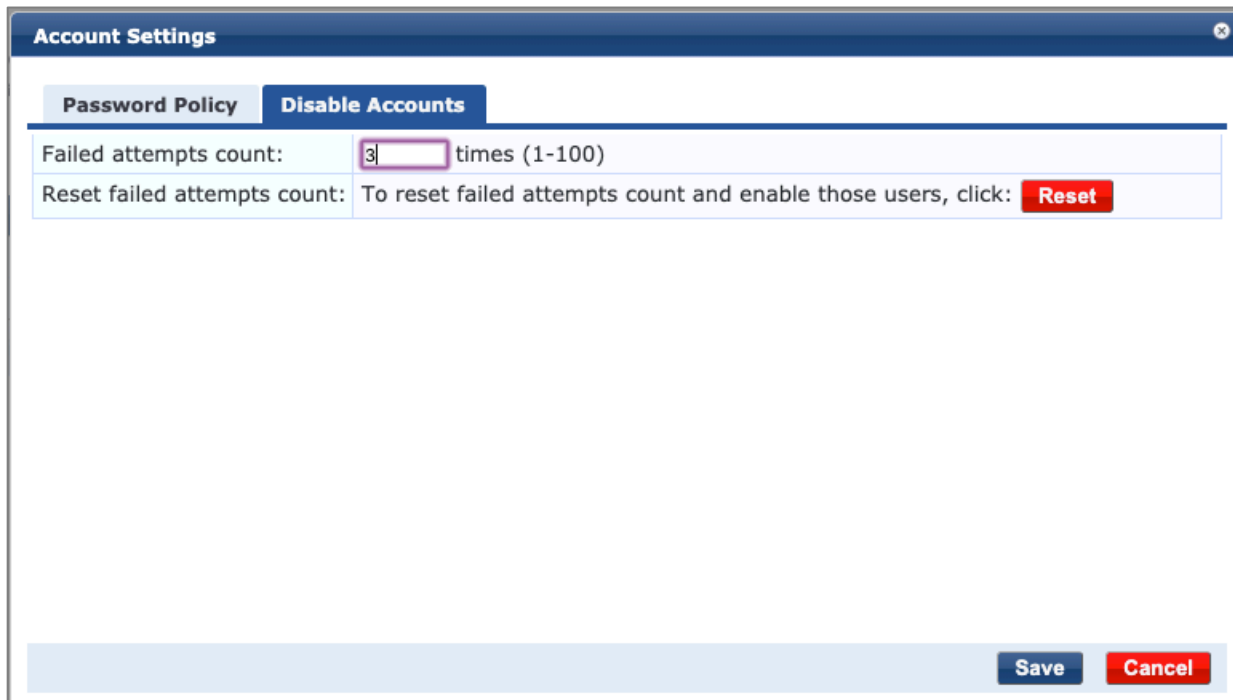
Advanced mode will apply the same conditions to both username/password authentication and SSH public key authentication. When Advanced mode is enabled, the only way to unlock the account is by waiting for the duration to expire or to execute the unlock command from the console or previously established SSH session.

Disable Admin User and Local User Account

Web UI access can be locked after a specified number of failed attempts. The time duration for these events is permanent until unlocked by another administrator. The number of failed attempts can be configured through the Web UI. Navigate to **Administration > Users and Privileges > Admin Users**, select the **Account Settings** link, and then select the **Disable Accounts** tab. The **Failed attempts count** field can be populated with the desired number of failed login attempts.



Re-enable the account by clicking the **Reset** button.



If the **Reset** button is clicked, a message displays notifying you of the number of accounts being unlocked. Accounts may also be individually unlocked directly from the **Admin Users** screen by selecting individual administrators and re-enabling their account.

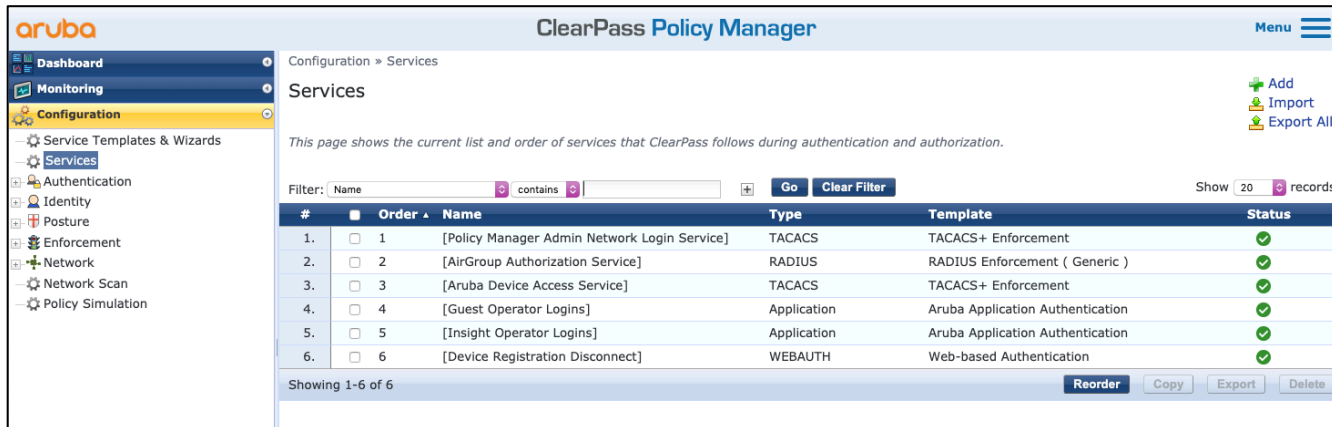
If the Web UI access is lost, the following steps can help resolve the issue:

Issue	Likely Problem and Resolution
Login fails	<p>Incorrect username and credentials</p> <p>Attempt with another user</p>
Web UI service is not responding	<p>The 'cpass-admin-server' service has stopped</p> <p>Execute the CLI command:</p> <pre>service start cpass-admin-server</pre> <p>Verify the server is restart with the CLI command:</p> <pre>service status cpass-admin-server</pre> <p>Admin server [cpass-admin-server] is running</p>
Web UI blocked by browser due to HTTPS certificate expired	<p>View audit on syslog server, look for "SSL_ERROR_EXPIRED CERT_ALERT" with "error:140800FF:SSL routines:ssl3_accept:unknown state Client IP Address" (including client IP address)</p> <p>Temporarily regenerate a self-signed certificate to return to access on the system with the following CLI commands:</p> <pre>Cluster reset-database</pre> <pre>system reset-server-certificate.</pre> <p>Select option 2 (Reset HTTP Server Certificate)</p> <p>This will reset the system to initial configuration. Log in through the UI, restore the last known configuration backup, import valid certificate(s) and re-enable CC Mode.</p>

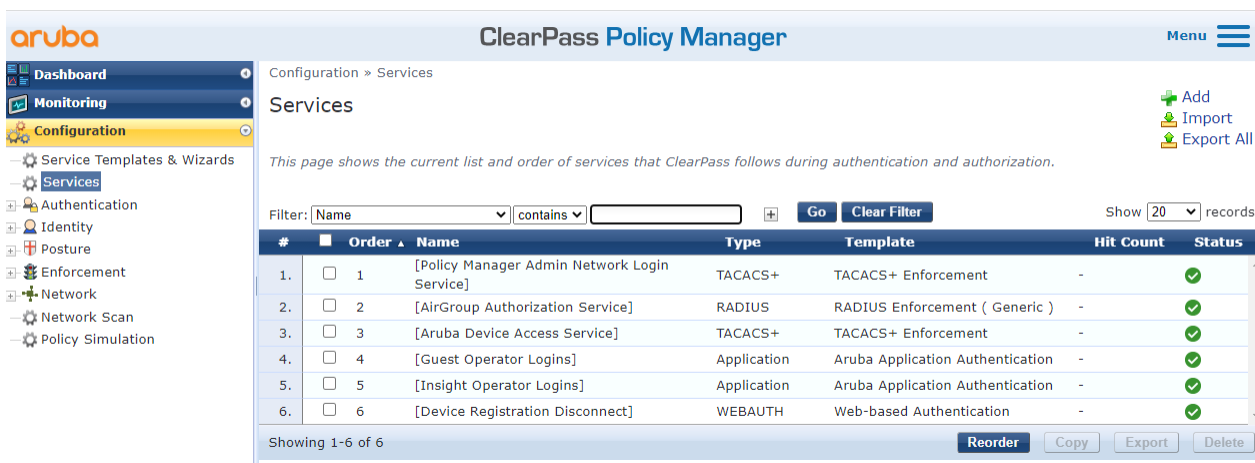
FTP_ITC.1(1)

It is important to configure the ClearPass RADIUS service. It is recommended to consult the User Guide for information related to configuring ClearPass. Configuration will automatically occur if the NAD was created using the service template available at **Configuration > Service Templates & Wizards**. The service template will create the required enforcement profile(s), enforcement policy(s), and service(s) specified.

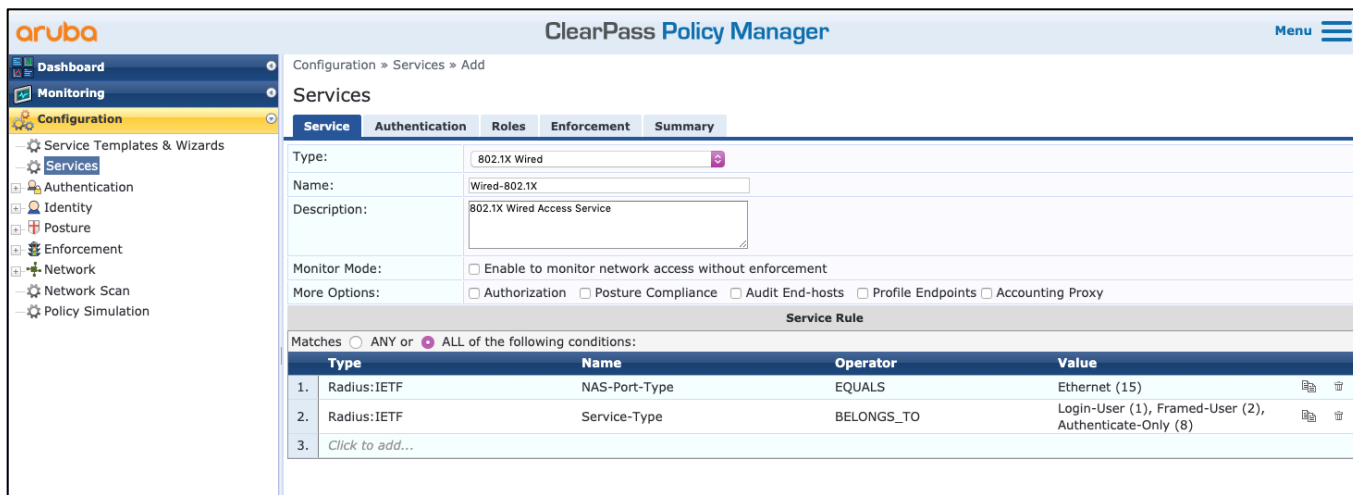
RADIUS can also be configured directly by navigating to **Configuration > Services**. Template-created policies will be named starting with the provided prefix.



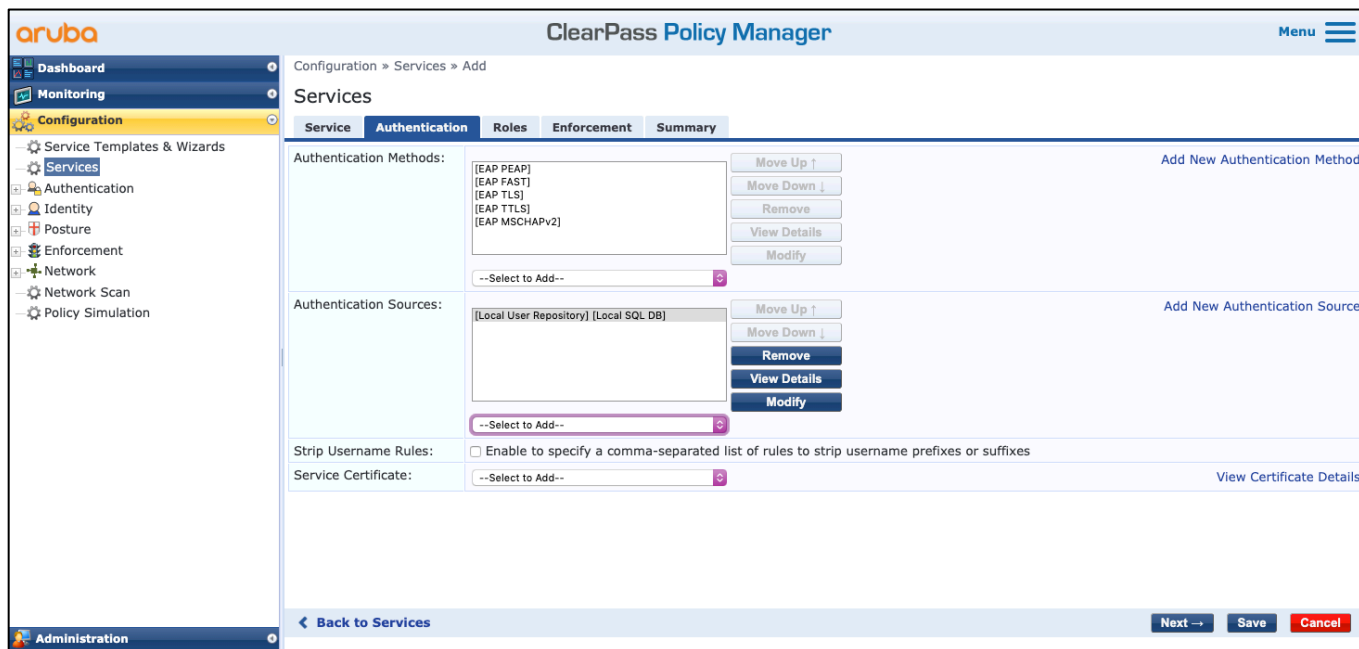
New services may be added by clicking the **Add** button on the top right. Services may also be enabled or disabled by clicking the status icon. Enabled services display a green circle with a check, disabled or stopped services display a red circle with a square. Services enabled but operating in monitor mode display with an orange circle and bi-directional arrows.



When adding new services, the type of service will determine the options that are available and displayed here. The below example is built using the type “802.1X Wired” service and will pre-define the IETF attributes that should be matched to apply for this rule.



Available authentication methods must be configured on the **Authentication** tab. To conform with Common Criteria evaluated configuration, only the EAP-TLS authentication method may be used. When creating a new service through service templates, or manually, the default will include several available authentication methods. Other EAP methods are not evaluated by Common Criteria evaluation.



Additional configuration options such as **Roles** and **Enforcement** may be configured on their appropriate tabs. The RADIUS service can be used immediately.

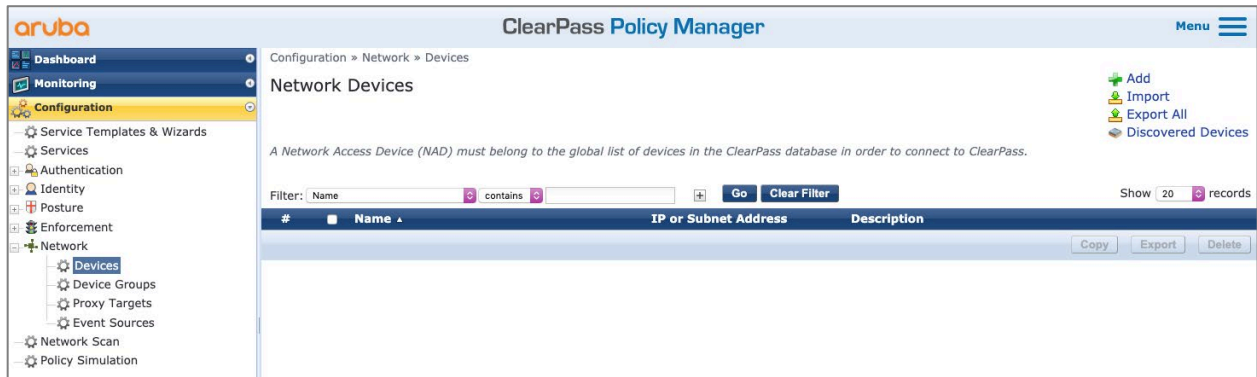
When RADIUS communication is not functioning correctly, it is typically due to either an incorrect address specified, or the shared secret is not correctly entered between the devices. When RADIUS has been communicating correctly between two hosts and unexpectedly stops, the service should be re-validated on both systems. Ensure the IP address(es) of each device is correctly specified. Re-enter the shared secret passwords on both devices. Also validate that no network control device, such as a firewall or IPsec VPN tunnel, is preventing the network traffic from reaching both devices correctly.

When RADIUS is tunneled over IPsec VPNs, ensure the IPsec traffic is not blocked between the endpoint and ClearPass. It is recommended to enable IPsec VPN use only after RADIUS is established to ensure that the communication parameters are configured correctly as it may be difficult to determine the issue when IPsec point-to-point tunnels are used.

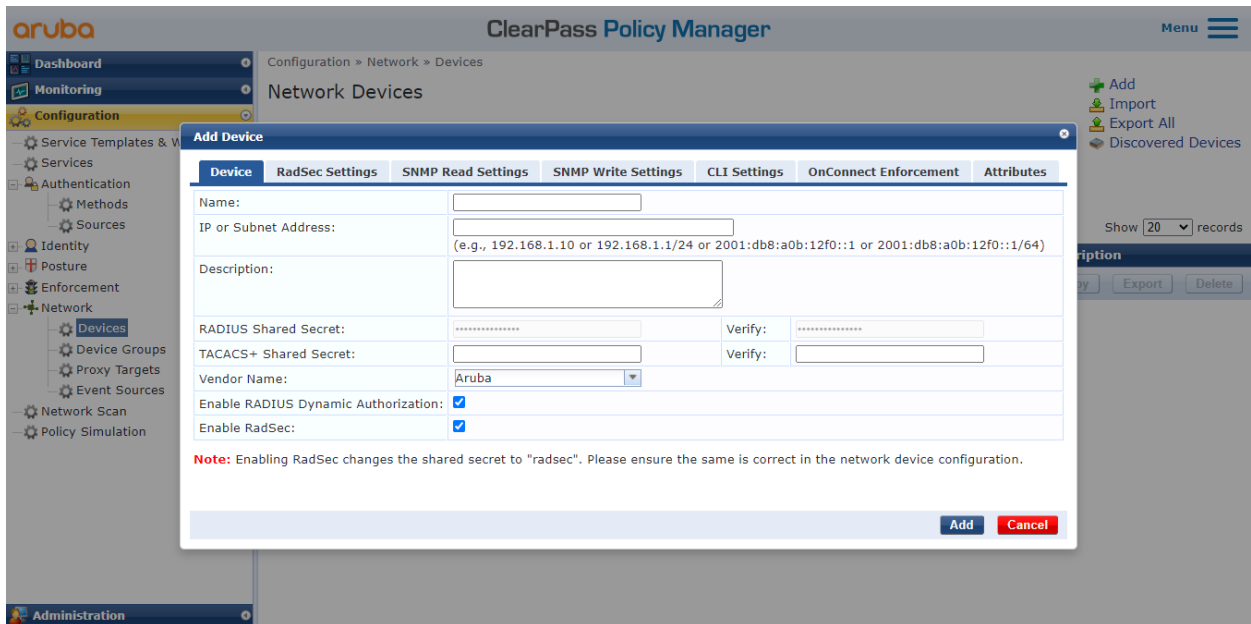
Add Network Access Devices

After Common Criteria configurations are completed, Aruba recommends network access devices (NAD) be added to the system prior to conduction RADIUS and/or TACACS+ authentication events.

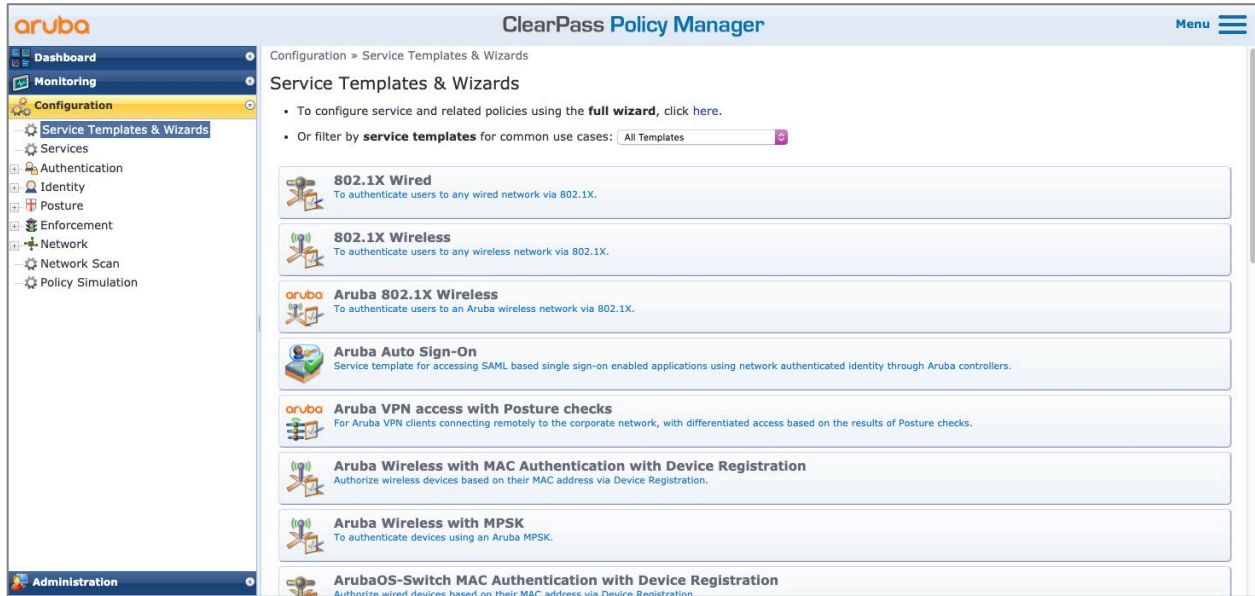
To configure this through the Web UI, navigate to **Configuration > Network > Devices** and select the **Add** link.



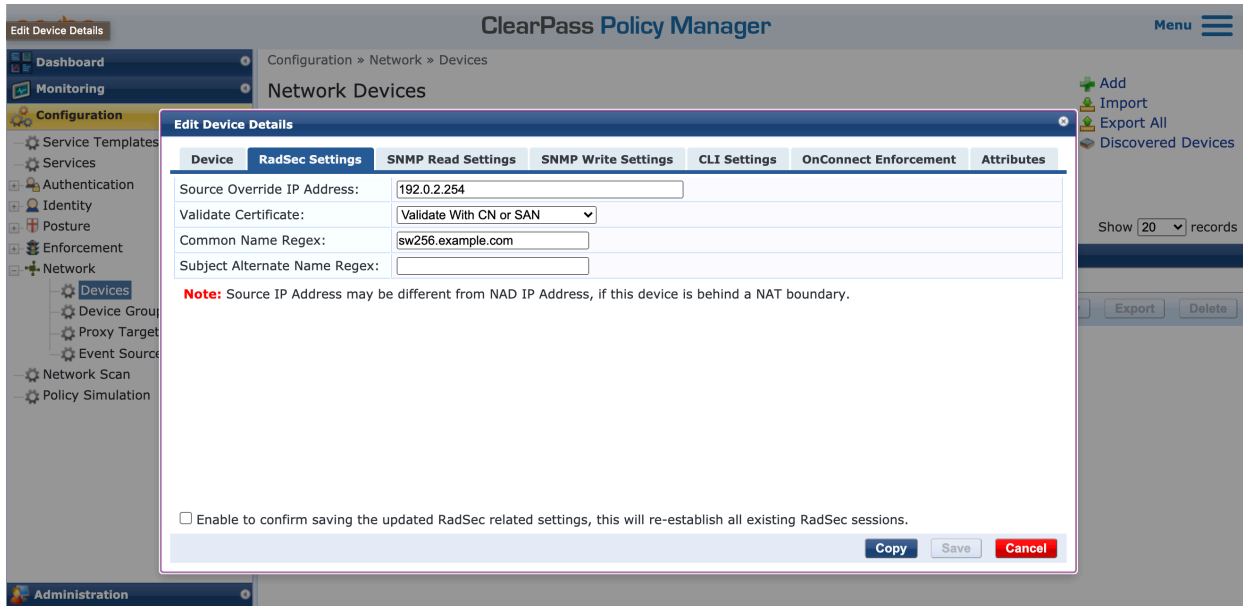
From the **Add Device** form, use the available list of options to complete the information required to add the network device.



The above image indicates RadSec was used. The use of RADIUS would require an IPsec VPN to protect the communications. An alternative method is to use a service template, available at **Configuration > Service Templates & Wizards**. This method will also request all additional information related to the selected template.



Each NAD should use an agreed upon RADIUS shared secret key/password that is secured using established password security requirements. It is recommended that all shared secrets be at least 22 characters, and each NAD uses a unique shared secret. When communication between NAD and Policy Manager over RadSec, the shared secret key/password is automatically set to “radsec” in compliance with RFC behavior. RadSec sessions use certificate validation to establish communication. These may be selected from the **RadSec Settings** tab.



The Source Override IP Address field allows the connection to be processed through a NAT boundary where the actual address of the device and the received address may be different.

The default Validate Certificate option is *No Authorization Checks*. The *No Authorization Checks* option is not recommended for production use and is not allowed for use in CC configurations. It is available only to aid in ensuring connectivity problems are not network specific. The CC evaluated Validate Certificate option is **Validate with CN or SAN** although the option *RFC Compliant (Serial + Issuer)* is also available. When specifying the Common Name Regex, the distinguished name (DN) field is matched. The use of regular expressions (Regex) is allowed when required. When specifying the Subject Alternative Name

Regex, the SAN fields are matched. These may be DNS domain name, IP address, username, or Email address to match against.

Configuring RadSec

A Network Access Devices (NAD) can be configured to use either RADIUS or RadSec. When the option to Enable RadSec is selected on the NAD Policy Manager will not accept communication from that device using RADIUS, RADIUS Accounting, or RADIUS Dynamic Authorization ports.

To comply with Common Criteria evaluated status, all RADIUS communications should be encrypted between ClearPass and the NAD(s). Section FCS_IPSEC_EXT.1 details the basic information to establish IPsec tunnels. If ports are restricted to RADIUS, ensure that RADIUS Accounting and RADIUS Dynamic Authorization are also allowed to pass through the IPsec tunnel to comply with CC evaluation configuration. The use of RadSec communication in place of IPsec encoding was also evaluated. When using RadSec, only TCP port 2083 is used for all communication between NAD and ClearPass.

Configure Notifications

ClearPass notifies administrators when specific alerts and alarms occur. These alerts are triggered by email, SNMP, or SMS notifications, depending on configuration. SNMP and SMS notifications were not validated during Common Criteria validation.

To configure email notification events, navigate to **Administration > External Servers > Messaging Setup**.

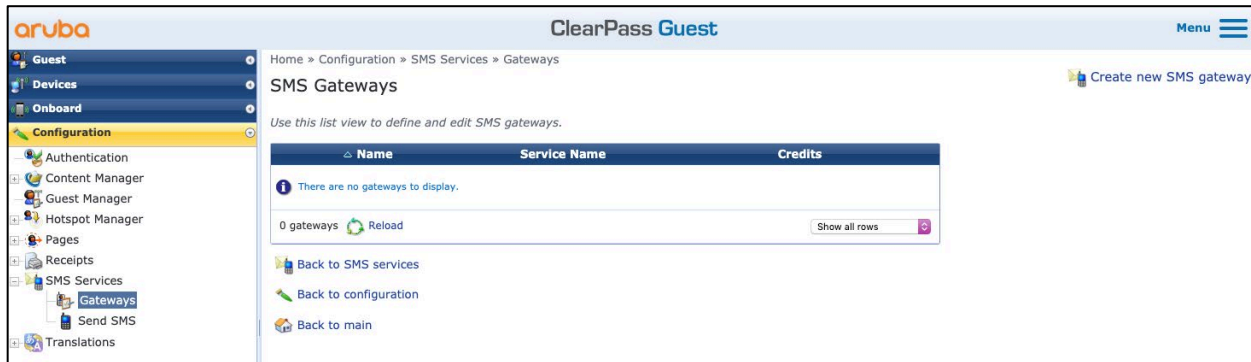
The screenshot shows the ClearPass Policy Manager web interface. The breadcrumb navigation is Administration > External Servers > Messaging Setup. The main heading is 'Messaging' with a 'Configure SMS Gateway' link. Below this is the 'SMTP Server' configuration section. The 'SMTP Settings' table includes the following fields:

SMTP Settings	
Server Name:	<input type="text"/>
Username:	<input type="text"/>
Password:	<input type="password"/>
Verify Password:	<input type="password"/>
Default From Address:	<input type="text"/>
Connection Security:	None
Port:	25
Connection Timeout:	30 seconds

At the bottom of the form are buttons for 'Send Test Email', 'Send Test SMS', 'Reset', and 'Save'.

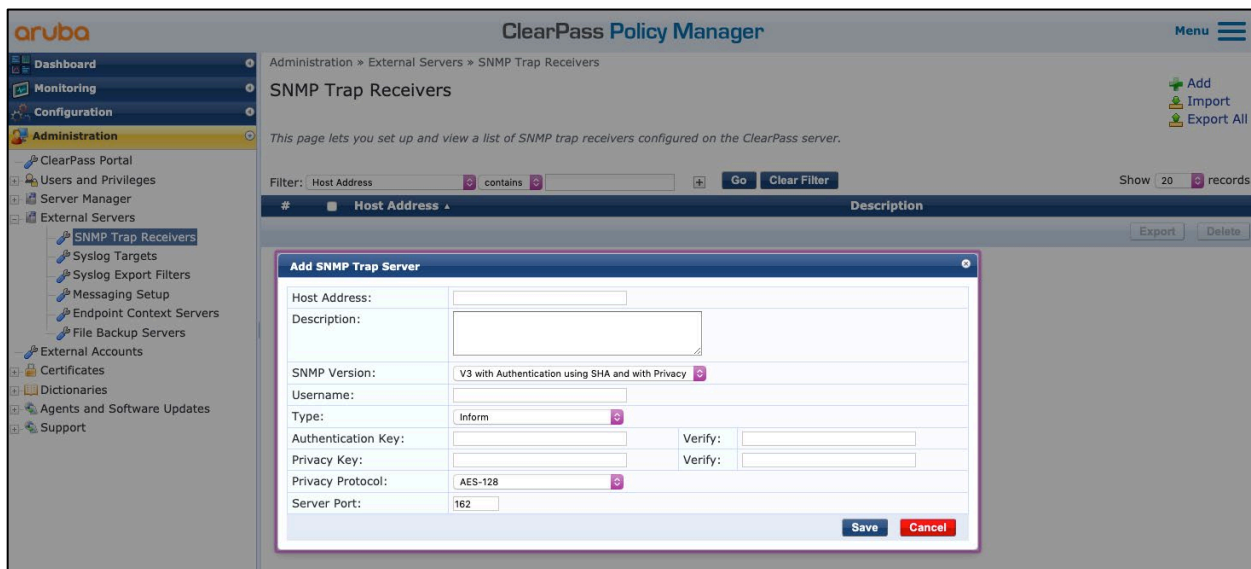
Specify the appropriate information to transmit SMTP messages to your server. When completed, it is recommended to click the button **Send Test Email** to validate that the configuration works. ClearPass does support TLS encoded SMTP delivery or message delivery may be secured over IPsec to ensure security. Common Criteria evaluation was performed using the IPsec security.

To configure SMS notification events, navigate to **Administration > External Servers > Messaging Setup**. Select the option **Configure SMS Gateway**. This will open a new browser tab in the Guest Web UI, as if you navigated to **Guest > Configuration > SMS Services > Gateways**.



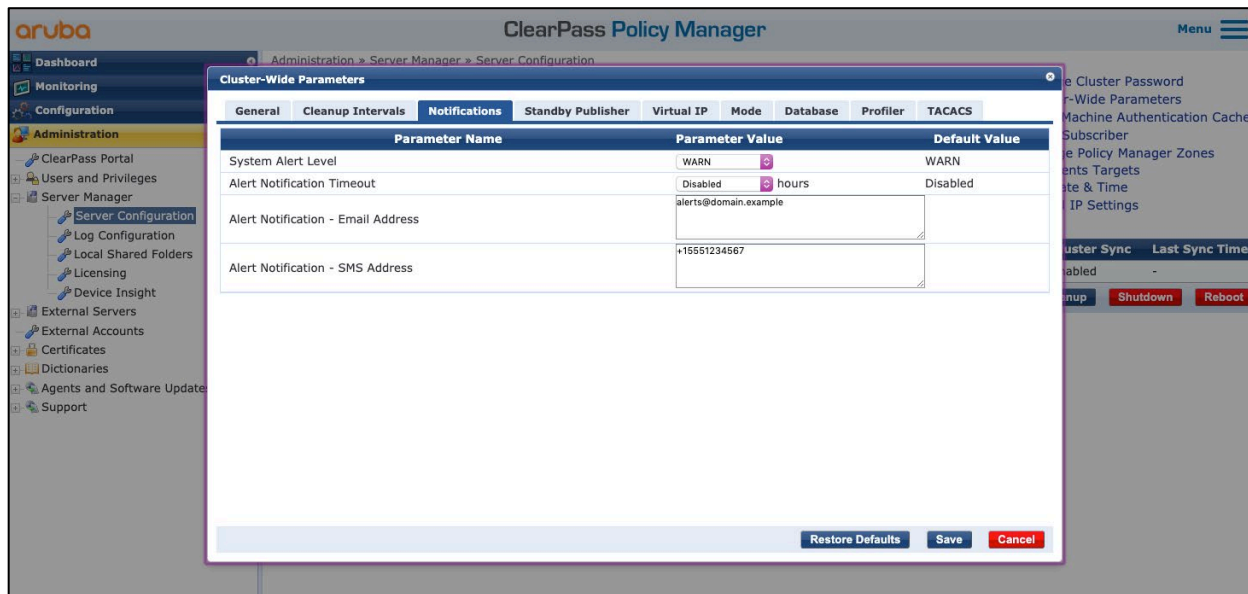
If using a new SMS provider, click the option **Create new SMS gateway** and specify the appropriate information. Once the SMS gateways are specified correctly, return to the Policy Manager **Messaging Setup** screen and test the configuration using the **Send Test SMS** button.

To configure SNMP notification events, navigate to **Administration > External Servers > SNMP Trap Receivers**. Select the **Add** option to input a new SNMP destination.



Enter the appropriate information for the required SNMP version. Monitoring the SNMP receiver will indicate that info is being received after a ten (10) minute window. Aruba recommends importing the ClearPass SNMP MIBs to the SNMP receiver to ensure accurate data is displayed.

When notifying via email and/or SMS alerts, the recipients must be specified. This can be accomplished by navigating to **Administration > Server Manager > Server Configuration** and selecting the **Cluster-Wide Parameters** link.



Email and/or SMS recipients may be specified in the provided fields of the **Notifications** tab.

CONTINUED GUIDANCE CONFIGURATION

FIA_UIA_EXT.1

ClearPass includes support for clustering multiple systems together. If ClearPass is being deployed in a stand-alone environment, one (1) additional port must be blocked to prevent inbound connections. This is accomplished by administrators logging in to the console directly and entering the following command:

```
configure port input tcp 5432 reject
configure port input tcp 5433 reject
```

FIA_X509_EXT.1/Rev

Valid certificates (including intermediate Certificate Authorities) must be installed prior to enabling Common Criteria mode, as previously noted.

FIA_X509_EXT.2.2

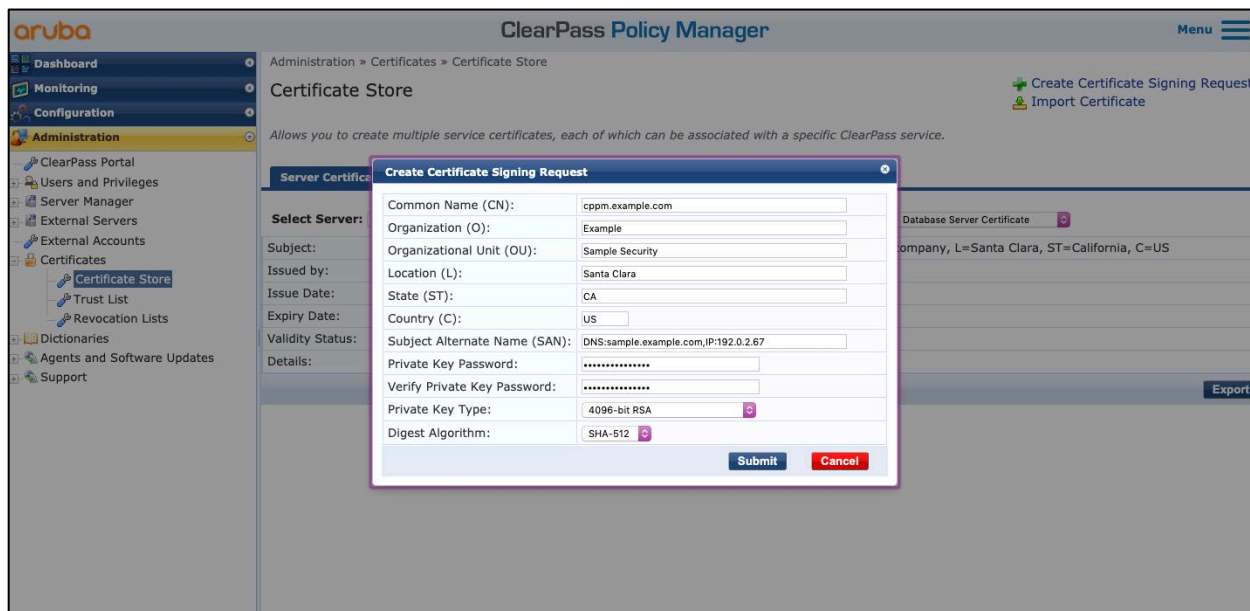
If the validity of the certificate cannot be established, the default configuration is to not accept the certificate.

FIA_X509_EXT.3.1

The minimum required selection of a Certificate Request Message is the Common Name. It is recommended to include all relevant information (Common Name, Organization, Organizational Unit, and Country) when generating certificates or certificate signing requests (CSR) for ClearPass.

Generating a CSR on ClearPass can be found by navigating to **Administration > Certificates > Certificate Store**. Select the desired certificate type from the drop-down list **Select Usage** and selecting the **Create Certificate Signing Request** link. This will generate a new CSR of the selected type. The default will be *RADIUS/EAP Server Certificate*. Other valid selections include HTTPS Server Certificate, RadSec Server Certificate, and Database Server Certificate use. Individual **Service and Client**

Certificates may also be generated from the specified tab but were not part of the evaluated configuration.



Specify the Common Name that the certificate will use, the Organization name, Organizational Unit, and two (2) letter Country code for all certificates to be used in Common Criteria evaluated configurations. The use of the Locality and Subject Alternative Name (SAN) are optional and were not evaluated as part of Common Criteria evaluation. Though not required, when specifying SAN, the values must be indicated with the appropriate type (DNS or IP) and a colon (:) to indicate the desired values.

Specify the Private Key Type as an approved CC evaluated type (2048-bit RSA, 3072-bit RSA, 4096-bit RSA, NIST/SECG curve over 384-bit prime field, or NIST/SECG curve over 521-bit prime field, X9.62/SECG curve over a 256-bit field). While listed as possible, the X9.62/SECG curve over 256-bit prime field is not a CC approved encryption type and should not be used. The NIST/SECG curve over 521-bit prime field was not evaluated. Specify the Digest Algorithm as an approved CC evaluated type (SHA-1, SHA-256, SHA-384, or SHA-512). The use of SHA-224 is not approved for use in CC evaluations. Specify the Private Key Password and verify.

FPT_TUD_EXT.1.3

ClearPass makes use of a digital signature whenever updates/upgrades are applied to the system, regardless of the package size or intent. When a new package is to be installed on ClearPass, it will initially be loaded to the server. Package signatures are verified after the package is loaded, but prior to the installation process. The signature is verified using a locally stored copy of the public key. If the cryptographic signatures are identical, then the update process is allowed to proceed. If the signatures do not match, the package update will fail with an error message indicating that the package has failed validation prior to installation.

To reduce error potentials when manually downloading packages, such as for a non-internet connected system, it is also recommended to validate the package hash and compare it against the published values from the ClearPass download site prior to loading onto ClearPass. While this process was not evaluated as part of Common Criteria evaluation, it is helpful in pre-validating that downloads have not been tampered with when updating systems without direct internet connections.

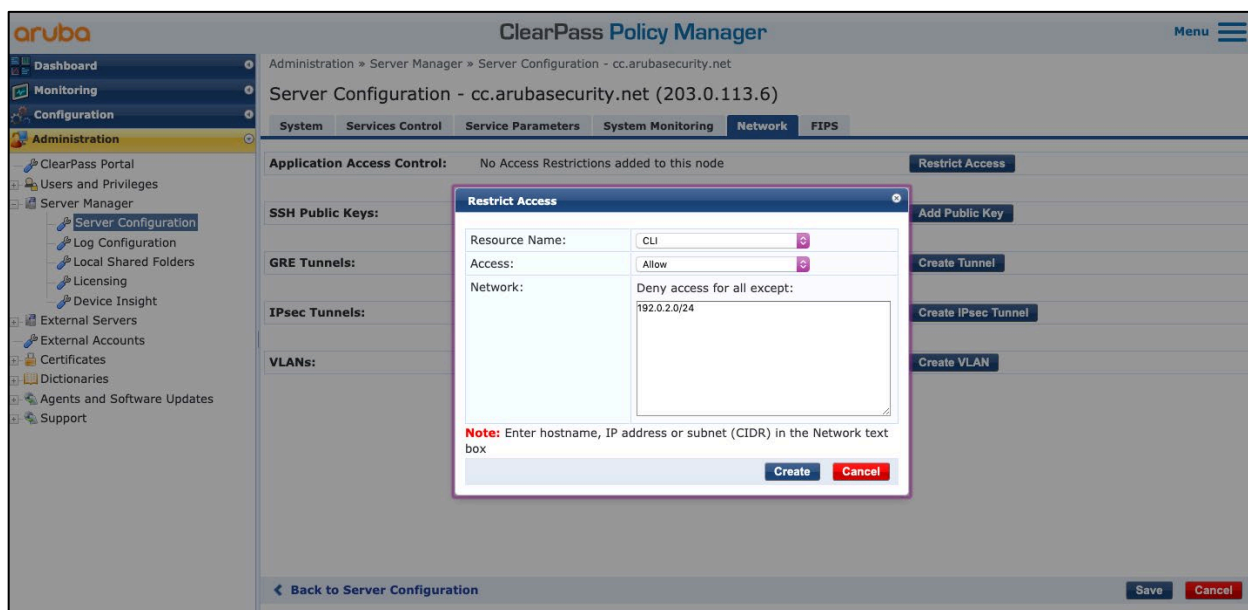
FMT_SMF.1.1

Network Time Protocol (NTP) is recommended to maintain reliable time stamps . Common Criteria evaluation was performed with NTP enabled.

Local administration is available on appliances using the following interfaces:

- Peripherals (monitor and keyboard directly attached)
- RS-232 terminal (serial console)
- Management Ethernet port

Because the Ethernet port may also be used for other communications, it is recommended to restrict the access for both CLI (secure shell) and Administrative Web UI. This is accomplished by navigating to **Administration > Server Manager > Server Configuration**. Select the server and then select the **Network** tab. Click the **Restrict Access** button near **Application Access Control** to create the desired controls.

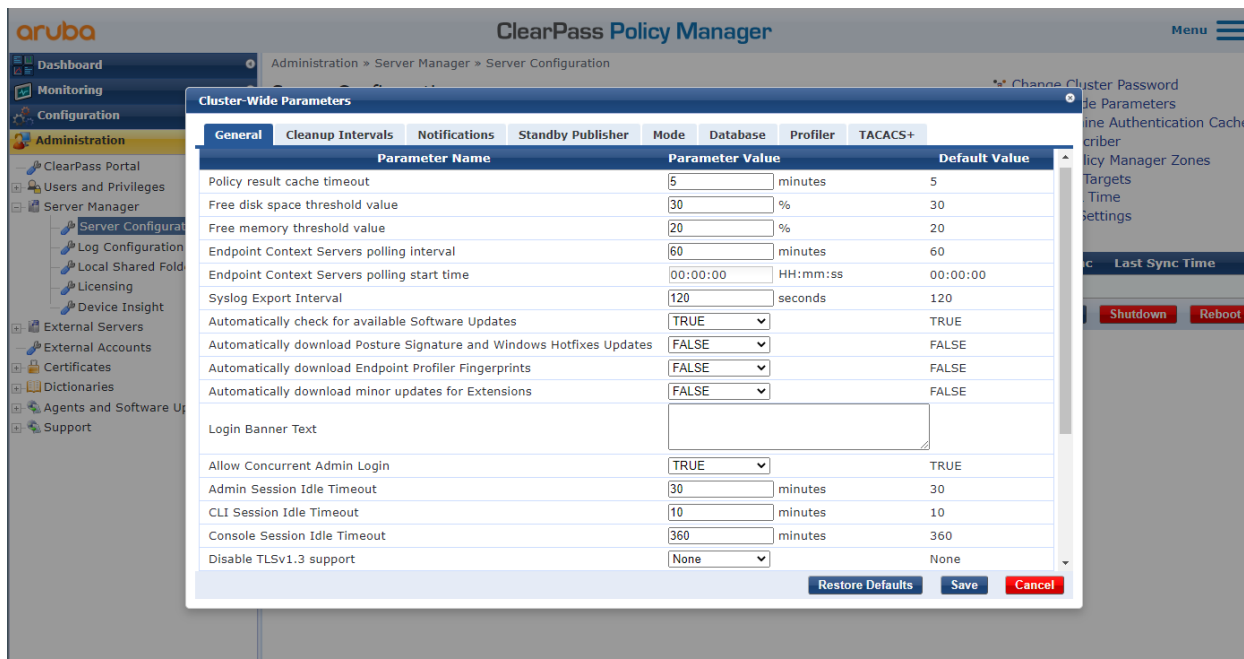


Definitions of the Resource Names may be found in the [ClearPass Policy Manager User Guide](#). Note that restricting the CLI will only apply to SSH connections. Console connections (including serial connections) are not impacted by these network restrictions.

Multiple application access controls may be specified to restrict the service availability. When selecting Policy Manager as the Resource Name, similar restrictions should be applied to the Insight and Guest Operator nodes to ensure all interfaces are restricted equally.

FTA_SSL.3 / FTA_SSL.4 / FTA_SSL_EXT.1.1

Both CLI (console and SSH) and Web UI sessions can be configured to timeout sessions after inactivity. This setting is available through the Web UI by navigating to **Administration > Server Manager > Server Configuration**. Select the option for **Cluster-Wide Parameters**, as shown below.



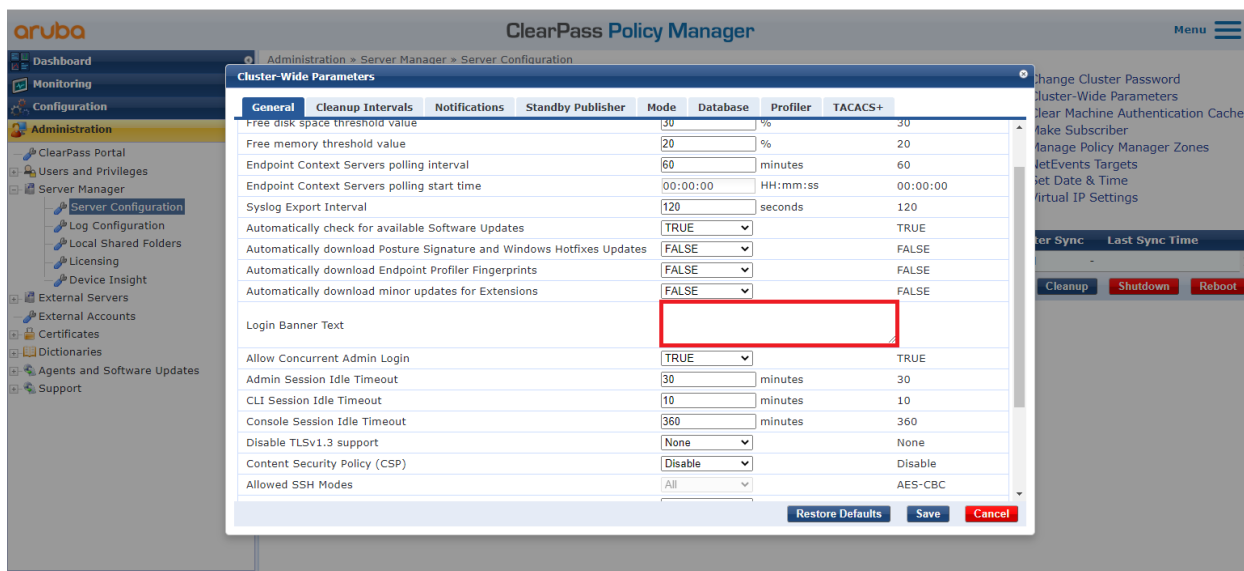
Modify the **Admin Session Idle Timeout** (default value **30**) to the desired time in minutes to change the Web UI settings. SSH sessions will timeout based on the **CLI Session Idle Timeout** (default value **15**) time in minutes. Console sessions will timeout based on the **Console Session Idle Timeout** (default value **360**) time in minutes.

The Web UI screens available under **Monitoring > Live Monitoring** will automatically refresh by default.

Termination of local console or CLI (SSH) sessions by the administrator is accomplished by entering the “exit” command to log out before idle session timeout. Web UI screens may be triggered from the Menu list in the upper right corner and selecting “Logout”.

FTA_TAB.1

Configure an access banner with appropriate text by navigating to **Administration > Server Manager > Server Configuration**. Select the option for **Cluster-Wide Parameters**, as shown below.



Modify the **Login Banner Text** field to include the information desired. This text will be applied to both the local console, Web UI, and SSH login events prior to the user logging in.

FTP_ITC.1

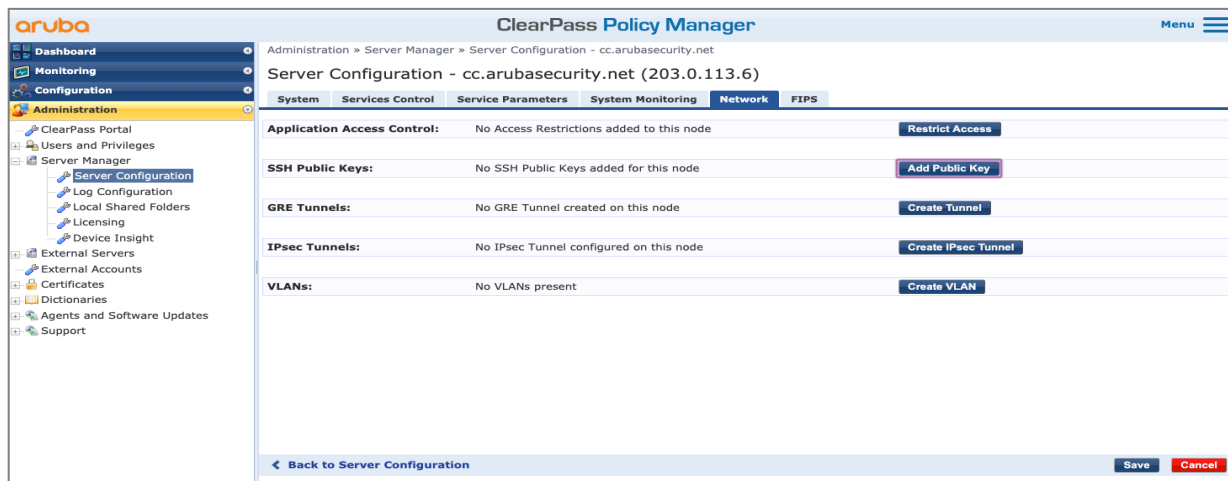
Most communication is already performed over encrypted channels, but some protocols do not support TLS encryption to ensure confidentiality and integrity. An example of this could be Syslog. In use cases where trusted communications are required to interact with these external devices, the use of IPsec is recommended.

To comply with Common Criteria evaluated status, all syslog communications should be encrypted between ClearPass and the remote syslog system(s). Section FCS_IPSEC_EXT.1 details the basic information to establish IPsec tunnels. It is recommended to restrict the traffic to only the syslog traffic (default UDP port 514) unless additional services are required on the same remote server.

FCS_SSHS_EXT.1.2

Configure SSH public key authentication by navigating to **Administration > Server Manager > Server Configuration**. Each node within a cluster (if applicable) must repeat the following process. Select the server/node to enable SSH public keys. Navigate to the **Network** tab. Click the button to **Add Public Key** and paste the desired key information in the **SSH Public Key** text field.

ClearPass supports SSH Public Key Authentication when using SSH-RSA and ecdsa-sha2-nistp256 key types only, regardless of operating modes. Attempting to import an unsupported SSH key type will result in the UI error indicating 'SSH Public key is invalid'.



Additional keys for different users can be added as needed.

FCS_SSHS_EXT.1.4

The modification of the Allowed SSH Modes option is not permitted when FIPS/CC mode is enabled. When FIPS/CC mode is enabled, aes256-gcm@openssh.com, aes256-ctr, aes256-cbc, aes128-gcm@openssh.com, aes128-ctr and aes128-cbc ciphers are supported.

FCS_SSHS_EXT.1.5

The Public Key(s) specified in the SSH Public Keys section (as outlined in FCS_SSHS_EXT.1.2) determine the available key algorithms available from the available `ecdsa-sha2-nistp256`, `rsa-sha2-256`, `rsa-sha2-512` and `ssh-rsa`. No administrator settings are configurable.

FCS_SSHS_EXT.1.6

The SSH transport uses `hmac-sha1`, `hmac-sha2-256`, or `hmac-sha2-512` MAC algorithms. No administrator settings are configurable.

FCS_SSHS_EXT.1.7

The SSH key exchange methods available are `ecdh-sha2-nistp256`, `ecdh-sha2-nistp384` and `ecdh-sha2-nistp521`. No administrator settings are configurable.

FCS_SSHS_EXT.1.8

SSH rekey events are initiated for every 128 MB of data sent over the connection, or every sixty (60) minutes (1 hour). These events can be monitored in the Web UI by navigating to **Monitoring > Event Viewer**. Applying the filter **Category contains SSH Rekeying** will show all rekey events. Below is an example event.

#	Source	Level	Category	Action	Timestamp
1.	Command Line	INFO	Logged out	None	Mar 10, 2020 21:56:29 UTC
2.	Command Line	INFO	SSH Rekeying	None	Mar 10, 2020 21:51:08 UTC
3.	Command Line	INFO	SSH Rekeying	None	Mar 10, 2020 21:51:08 UTC

Two (2) events will occur for rekey events. The first is ClearPass sending clients updated keys. The second is ClearPass receiving updated client keys. SSH rekey events will occur for either one (1) hour or 128 megabyte (MB) of data transferred, whichever event occurs first.

FCS_TLSS_EXT.2.1

The following is the complete list of evaluated cipher suites available on ClearPass in configured Common Criteria mode (includes functional limits of FIPS mode when enabled). When Common Criteria mode is enabled, these suites are automatically enabled without further administrator action:

```

TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA

```

```

TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA256
TLS_RSA_WITH_AES_128_CBC_SHA256
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_GCM_SHA384
TLS_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384

```

The following cipher suites are available only when an ECDSA certificate is installed on ClearPass:

```

TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA

```

The following cipher suites are available for the RadSec sessions:

```

TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA256
TLS_RSA_WITH_AES_256_CBC_SHA256
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384

```

The following cipher suites are available for the EAP-TLS use:

```

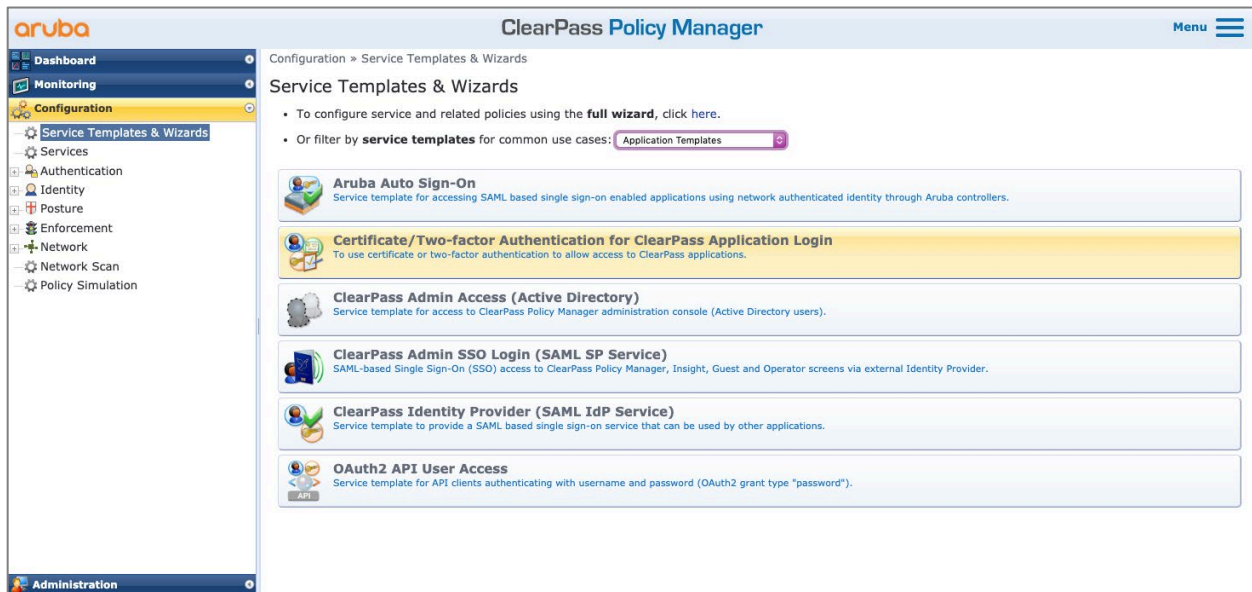
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA256
TLS_RSA_WITH_AES_256_CBC_SHA256
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

```

FCS_TLSS_EXT.2.2

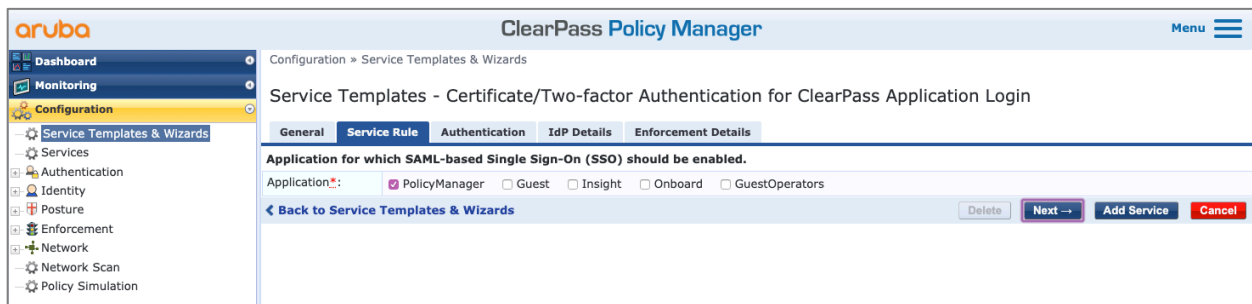
Web UI sessions may use certificate identification through mutual TLS authentication. This process requires that all DNS entries be configured correctly prior to establishment. It is critical to ensure that fully qualified domain names (FQDN) are resolvable from the client. Additionally, client systems will need to have the ClearPass Web UI public certificate available locally, along with any required CA intermediate certificates. That process is outside the scope of this document.

To aid in this process, a setup wizard is available to administrators in the Web UI. Begin by navigating to **Configuration > Service Templates & Wizards**. Select the **Certificate/Two-factor Authentication for ClearPass Application Login** service template.



On the **General** tab, the **Name Prefix** specifies is used to identify all components the wizard generates when used. For reference, the name “TLS-SSO” is used in later screen examples. Select the **Next** button to advance through the wizard.

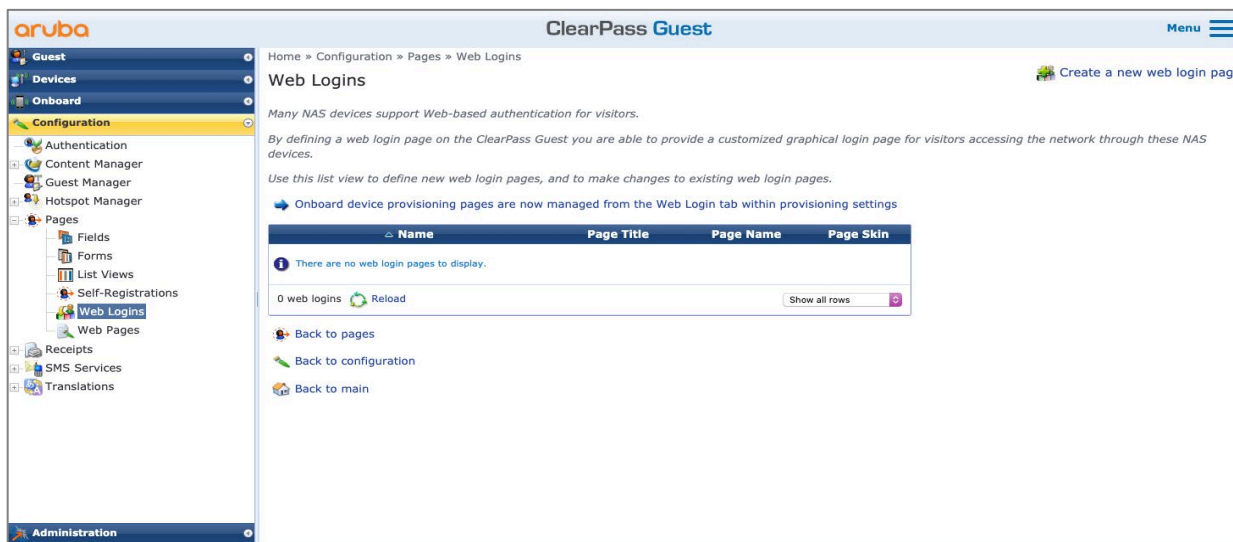
The **Service Role** tab allows the selection of Web UI components that will be configured to use TLS mutual authentication. The default includes the **PolicyManager** component, which controls the policy pieces of the system. Additional components may be selected as desired.



By default, the **Authentication** tab includes all the authentication sources that are already defined. If one has not been created, a new one may be created. This will default to an Active Directory (AD). Select or create the appropriate source and click **Next**.



The **IdP Details** tab allows selection of the appropriate Web login page. By default, only the device provisioning page is available. A new page must be created. Select the **Add New Guest Web Login page** link. A new browser tab will open to continue.



On the **Guest > Configuration > Pages > Web Logins** page, select the **Create a new web login page** link. The Web Login (new) page opens. In the Vendor Settings drop-down list, select **Single Sign-On – SAML Identify Provider**. In the Client Certificate drop-down list, select **Required – Require a client certificate from the user**. To allow certificate-only authentication, the default value may be used in the Authentication field (**Certificate only – No username or password required**).

The screenshot shows the 'Web Login Editor' interface in the Aruba ClearPass Guest management console. The left sidebar contains navigation options like Guest, Devices, Onboard, Configuration, and Administration. The main content area is titled 'Web Login (new)' and includes a breadcrumb trail: Home » Configuration » Pages » Web Logins. Below the title is a 'Web Login Editor' form with the following fields:

- * Name:** TLS-SSO (with a sub-note: 'Enter a name for this web login page.')
- Page Name:** tls_sso (with a sub-note: 'Enter a page name for this web login. The web login will be accessible from "/>

Additional edits may be made to the page as desired. When completed, select the **Save Changes** button at the bottom of the **Web Login (new)** page. Return to the other browser tab where the **Policy Manager > Configuration > Service Template** wizard is displayed. On the **IdP Details** tab, click the blue arrow. This refreshes the **Page Name** drop-down list to include the newly generated page name. Select the new page name in the list and then click **Next**.

The **Enforcement Details** tab lets you select attributes from the certificate to match against enforcements. A wide variety of components may be selected based on the certificate attribute or attributes.

The screenshot shows the 'Service Templates - Certificate/Two-factor Authentication for ClearPass Application Login' page in the Aruba ClearPass Policy Manager. The left sidebar shows navigation options like Dashboard, Monitoring, Configuration, and Service Templates & Wizards. The main content area is titled 'Service Templates - Certificate/Two-factor Authentication for ClearPass Application Login' and includes a breadcrumb trail: Configuration » Service Templates & Wizards. Below the title are tabs for General, Service Rule, Authentication, IdP Details, and Enforcement Details. The 'Enforcement Details' tab is active, showing a table with the following columns: Certificate Attribute, Super Admin Condition, Read Only Admin Condition, and Help Desk Condition.

Specify values that must be part of the selected Certificate attributes, to assign admin privileges to users.			
Certificate Attribute:	Subject-CN	Super Admin Condition:	A10X1213 (e.g., Enter attribute value for super admin users)
Certificate Attribute:	Issuer-OU	Read Only Admin Condition:	READONLY (e.g., Enter attribute value for read only users)
Certificate Attribute:	Extended-Key-Usage	Help Desk Condition:	(e.g., Enter attribute value for help desk users)

At the bottom of the page, there are buttons for 'Back to Service Templates & Wizards', 'Delete', 'Next -->', 'Add Service', and 'Cancel'.

When the **Add Service** button is selected, the appropriate services will be created within the system. By default, two services will be created that have the prefix provided in the **Name Prefix** step.

ClearPass Policy Manager

Configuration » Services

Services

Added 3 Enforcement Profile(s)
Added 2 Enforcement Policies
Added 2 service(s)

This page shows the current list and order of services that ClearPass follows during authentication and authorization.

Filter: Name contains Go Clear Filter Show 20 records

#	Order	Name	Type	Template	Status
1.	1	[Policy Manager Admin Network Login Service]	TACACS	TACACS+ Enforcement	✓
2.	2	[AirGroup Authorization Service]	RADIUS	RADIUS Enforcement (Generic)	✓
3.	3	[Aruba Device Access Service]	TACACS	TACACS+ Enforcement	✓
4.	4	[Guest Operator Logins]	Application	Aruba Application Authentication	✓
5.	5	[Insight Operator Logins]	Application	Aruba Application Authentication	✓
6.	6	[Device Registration Disconnect]	WEBAUTH	Web-based Authentication	✓
7.	7	mTLS-login ClearPass Certificate SSO Login	Application	Aruba Application Authentication	✓
8.	8	mTLS-login ClearPass Identity Provider	Application	Aruba Application Authentication	✓

Showing 1-8 of 8

Reorder Copy Export Delete

After completion of the Service Template & Wizard, select **Configuration > Identity > Single Sign-On (SSO)** and select the **SAML IdP Configuration** tab. The Web Login Configuration & Metadata section must be configured to indicate the previously created page and specify the Identity Provider (IdP) Signing Certificate. The Identity Provider (IdP) Encryption Certificate is not required.

ClearPass Policy Manager

Configuration » Identity » Single Sign-On (SSO)

Single Sign-On (SSO)

This page allows users to access the Policy Manager, Guest Onboard, Insight applications, and administration settings without reauthenticating.

Add Web Login Configuration

Page Name: Add New Guest Web Login Page

Identity Provider (IdP) Signing Certificate

Signing Certificate:

Note: This Certificate is used to sign the SAML response from the IdP. Add the certificate under Service & Client Certificates, if not listed above.

Identity Provider (IdP) Encryption Certificate

Encryption Certificate: None - No Encryption

Note: This Certificate is used to encrypt the SAML response from the IdP. Add and enable the certificate under Certificate Trust List, if not listed above.

ClearPass Service Provider (SP) Signing Certificate

Signing Certificate:

Note: This Certificate will be used to verify the signed SAML request from the SP if the KeyInfo is removed from the request. Add and enable the certificate under Certificate Trust List, if not listed above.

Save Cancel

Certificates are not available for the IdP Signing Certificate if the certificate under Service & Client Certificates is not created. Root and Intermediate CA certificates used to sign the user certificate must be configured with “Others” in the certificate trust list for the certificate authentication to work.

Additional information on modifications and on troubleshooting this process can be obtained by contacting technical support.

FCS_TLSS_EXT.1.2

ClearPass supports a flexible TLS model for backwards compatibility with older devices. Support for older SSL-based protocols (SSL 1.0, SSL 2.0, or SSL 3.0) is no longer available in any ClearPass configuration. In Common Criteria deployments TLS v1.0 and TLS v1.1 are disabled and hidden in the UI by default. Navigate to **Administration > Server Manager > Server**

Configuration and select the **Cluster-Wide Parameters** link.

The screenshot shows the Aruba ClearPass Policy Manager web interface. The 'Cluster-Wide Parameters' window is open, displaying the 'General' tab. The 'Disable TLSv1.3 support' dropdown menu is highlighted with a red box and set to 'Admin'. Other settings include 'Automatically download Posture Signature and Windows Hotfixes Updates' (FALSE), 'Automatically download Endpoint Profiler Fingerprints' (FALSE), 'Automatically download minor updates for Extensions' (FALSE), 'Login Banner Text' (empty text area), 'Allow Concurrent Admin Login' (TRUE), 'Admin Session Idle Timeout' (30 minutes), 'CLI Session Idle Timeout' (10 minutes), 'Console Session Idle Timeout' (360 minutes), 'Content Security Policy (CSP)' (Disable), 'Allowed SSH Modes' (All), 'ICMPv6 Filters' (Disable), 'ClearPass Zone Cache Durability' (OFF), 'Post-Authentication v2' (Enable), 'Post-Authentication unsubscribes from the endpoint updates on Acct Stop' (Disable), 'Post-Authentication v2 HTTP enforcement' (Enable), and 'EAP TLS Session Cache Policy' (Internal). Buttons for 'Restore Defaults', 'Save', and 'Cancel' are visible at the bottom.

Parameter	Value	Unit	Value
Automatically download Posture Signature and Windows Hotfixes Updates	FALSE		FALSE
Automatically download Endpoint Profiler Fingerprints	FALSE		FALSE
Automatically download minor updates for Extensions	FALSE		FALSE
Login Banner Text	<input type="text"/>		
Allow Concurrent Admin Login	TRUE		TRUE
Admin Session Idle Timeout	30	minutes	30
CLI Session Idle Timeout	10	minutes	10
Console Session Idle Timeout	360	minutes	360
Disable TLSv1.3 support	Admin		None
Content Security Policy (CSP)	Disable		Disable
Allowed SSH Modes	All		AES-CBC
ICMPv6 Filters	Disable		Disable
ClearPass Zone Cache Durability	OFF		OFF
Post-Authentication v2	Enable		Enable
Post-Authentication unsubscribes from the endpoint updates on Acct Stop	Disable		Disable
Post-Authentication v2 HTTP enforcement	Enable		Enable
EAP TLS Session Cache Policy	Internal		Internal

Within the **General** tab, **Disable TLSv1.3 support** is set to **None** by default. This prevents legacy TLS versions prior to v1.3 from using components such as RADIUS, RadSec, or Web UI. This setting cannot be modified in CC operating mode.

FCS_IPSEC_EXT.1

When situations require additional encryption and integrity, an IPsec VPN tunnel may be established between ClearPass and a remote device. The IPsec tunnel cannot be used as a gateway to or from ClearPass. Remote endpoints should be configured to accept the ClearPass appliance's address exclusively.

While using Online Certificate Status Protocol (OCSP), the Uniform Resource Indicator (URI) should be specified in the **OCSP URI** field, beginning with HTTPS or HTTP. This is only required if connection to a remote VPN device does not transfer a certificate with the OCSP URI encoded. To configure this OCSP URI value, navigate to **Administration > Server Manager > Server Configuration**, select the server in the list, and then select the **Service Parameters** tab. In the **Select Service** dropdown list, select **ClearPass IPsec service**.

The screenshot shows the Aruba ClearPass Policy Manager web interface. The left sidebar contains a navigation menu with categories like Dashboard, Monitoring, Configuration, and Administration. The main content area is titled "Server Configuration - cppm197" and "Server Configuration - cppm197 (10.2.54.197)". The "Service Parameters" tab is active, showing a table of parameters for the "ClearPass IPsec service".

Parameter Name	Parameter Value	Default Value	Allowed Values
OCSF URI	<input type="text"/>		
Strict CRL Policy	no	no	

At the bottom of the page, there are "Save" and "Cancel" buttons, and a "Back to Server Configuration" link.

After clicking **Save**, select the **Network** tab. The **Create IPsec Tunnel** button may be used to generate a new IPsec tunnel. Existing entries may also be directly deleted or modified from this location.

Adding a new IPsec tunnel allows the specification of either Pre-Shared Key (PSK) or certificate-based systems. Select the values required for connection with the remote IPsec device.

To reduce the likelihood of configuration errors where weaker algorithms are used in Phase 2 rather than in Phase 1 negotiations, the encryption algorithm and hash algorithms are selected only one time and applied across the Security Association (SA). These values will also apply to child SAs. Remote peers should be configured to accept the same settings.

Create IPsec Tunnel
✕

General

Traffic Selectors

Local Interface:	203.0.113.6 [MGMT] ⌵
Remote IP Address:	<input style="width: 90%;" type="text"/>
IPsec Mode:	Tunnel ⌵
IKE Version:	2 ⌵
Encryption Algorithm:	RFC6379 ⌵
PRF:	PRF-HMAC-SHA384 ⌵
Hash Algorithm:	HMAC SHA384 ⌵
Diffie Hellman Group:	Group 20 ⌵
Authentication Type:	Certificate ⌵
Peer Certificate Subject DN:	<input style="width: 90%;" type="text"/>
IKE Lifetime:	<input style="width: 80%;" type="text" value="180"/> minutes
Lifetime:	<input style="width: 80%;" type="text" value="60"/> minutes
Enabled:	<input checked="" type="checkbox"/>
ESP (Phase2):	Encryption AES with 256-bit keys in GCM mode Integrity NULL.
IKEv2 (Phase1):	Encryption AES with 256-bit keys in CBC mode.

Create
Cancel

If **Certificate** is selected as the **Authentication Type**, then when specifying the value of the **Peer Certificate Subject DN**, the specified distinguished name must be an exact match to the certificate that the remote device is using. If this is not exactly matched, the tunnel will fail to negotiate. ClearPass will use its HTTPS certificate for IPsec identity, but the CA from the remote peer must also be included in the ClearPass trust list or validation will not occur.

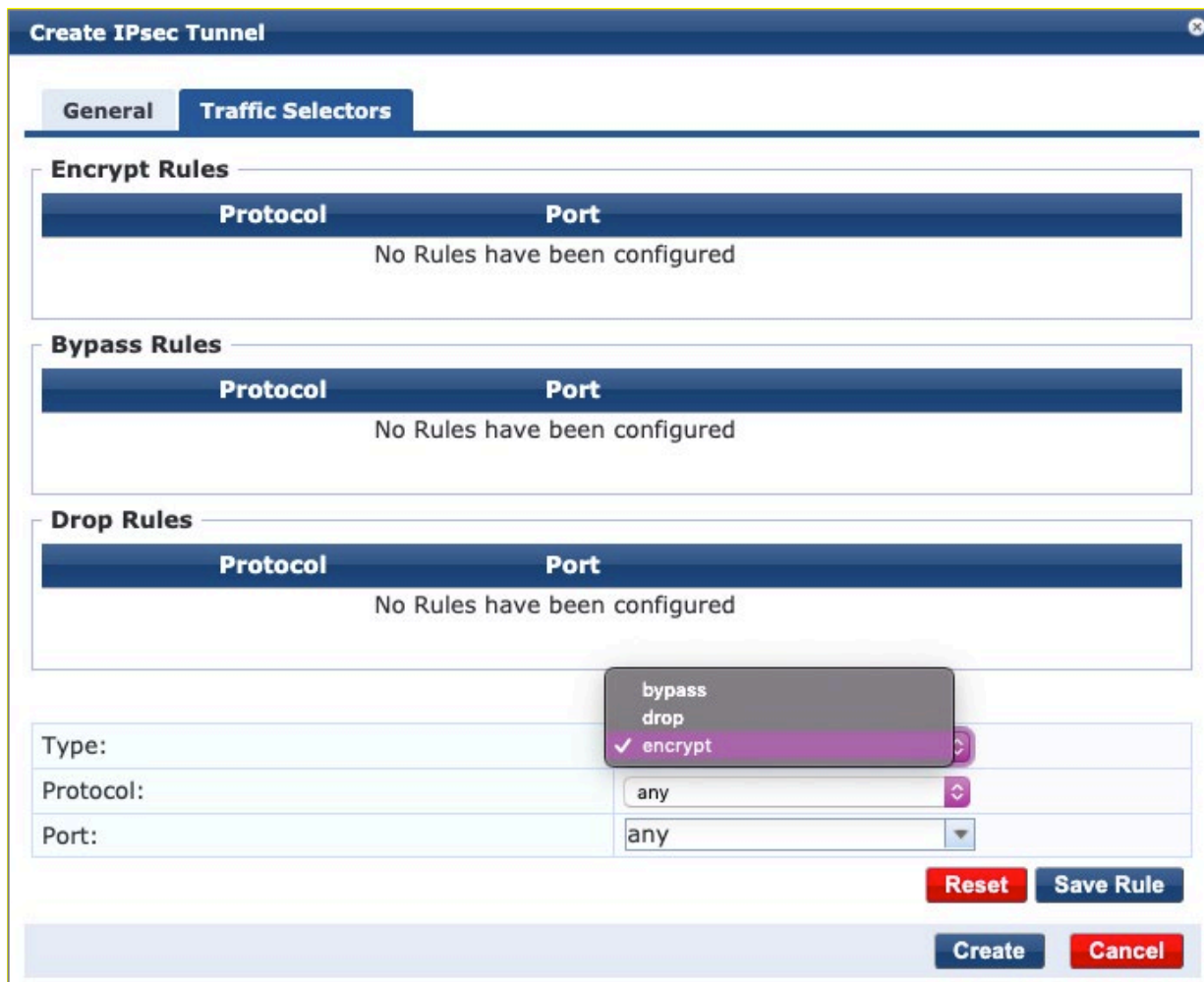
Create IPsec Tunnel ✕

General
Traffic Selectors

Local Interface:	203.0.113.6 [MGMT] ⌵	
Remote IP Address:	198.51.100.12	
IPsec Mode:	Tunnel ⌵	
IKE Version:	2 ⌵	
Encryption Algorithm:	RFC6379 ⌵	
PRF:	PRF-HMAC-SHA384 ⌵	
Hash Algorithm:	HMAC SHA384 ⌵	
Diffie Hellman Group:	Group 20 ⌵	
Authentication Type:	Certificate ⌵	
Peer Certificate Subject DN:	<input style="width: 100%;" type="text"/>	
IKE Lifetime:	<input style="width: 80%;" type="text" value="180"/>	minutes
Lifetime:	<input style="width: 80%;" type="text" value="60"/>	minutes
Enabled:	<input checked="" type="checkbox"/>	
ESP (Phase2):	Encryption AES with 256-bit keys in GCM mode Integrity NULL.	
IKEv2 (Phase1):	Encryption AES with 256-bit keys in CBC mode.	

Create
Cancel

If only specific traffic is sent to the remote host over a VPN, the **Traffic Selectors** tab can also be configured. This will default to encryption of all traffic (protocol and port) between the two hosts. Additional traffic rules can be applied to bypass the traffic, as noted in Appendix B.



Create IPsec Tunnel

General | **Traffic Selectors**

Encrypt Rules

Protocol	Port
No Rules have been configured	

Bypass Rules

Protocol	Port
No Rules have been configured	

Drop Rules

Protocol	Port
No Rules have been configured	

Type: by drop ✓ encrypt

Protocol: any

Port: any

Reset **Save Rule**

Create **Cancel**

In the event IPsec VPNs unexpectedly drop the following steps may be taken to resolve the issue. Note that IPsec tunnels may be alerted on when they change status to down. This will aid in identifying that the IPsec session has failed.

Issue	Likely Problem and Resolution
Certificate failure (expired)	Replace the HTTPS Server certificate on ClearPass or the remote peer certificate device.
Tunnel will not establish	Ensure parameters have not been changed by the remote peer
IPsec indicates it is active (up), but traffic is not passing	Ensure the tunnel status is up Validate the traffic selectors are not restricting access as expected Validate intermediate devices such as firewalls are not preventing traffic from passing

When configuring IPsec tunnels with remote peers that change the peer certificate, the IPsec service on ClearPass should be restarted to clear the previous certificate from the cache. This is accomplished by administrators logging in to the console directly and entering the following command:

```
service restart cpass-ipsec
```

IPsec VPNs may be configured to use various settings. The settings selected will determine the options available. When using IKEv1 in either Tunnel or Transport mode, the following settings may be selected.

IKE Phase 1 Mode: Main

Encryption Algorithm: AES128, AES256

Hash Algorithm: HMAC SHA, HMAC SHA256, HMAC SHA384

Diffie Hellman Group: Group 14, Group 19, Group 20

When using IKEv2 in either Tunnel or Transport mode, the following settings may be selected.

Encryption Algorithm: AES128, AES256, AES128GCM16, AES256GCM16, RFC6379

PRF: PRF-HMAC-SHA1, PRF-HMAC-SHA256, PRF-HMAC-SHA384

Hash Algorithm: HMAC SHA, HMAC SHA256, HMAC SHA384

Diffie Hellman Group: Group 14, Group 19, Group 20

The Encryption Algorithm "RFC6379" is available for use exclusively under IKEv2. This will utilize AES256 in CBC mode for Phase 1 and AES256 in GCM with Integrity NULL for Phase 2. This is the only condition where Encryption Algorithms are not the same for both phases. Selection will also set PRF to PRF-HMAC-SHA384, the Hash Algorithm to HMAC SHA384, and Diffie Hellman Group to be Group 20.

As noted in FCS_IPSEC_EXT.1.4 and FCS_IPSEC_EXT.1.11, the UI will offer options that are not allowed under CC evaluated criteria

[FCS_IPSEC_EXT.1.3](#)

IPsec VPNs may be configured to use either Transport or Tunnel by selecting the IPsec Mode. Tunnel mode is the default IPsec Mode.

[FCS_IPSEC_EXT.1.4](#)

Hash Algorithms are limited to HMAC SHA1, HMAC SHA256 and HMAC SHA384. HMAC SHA should not be selected. The selected hash algorithms are applied to both Phase 1 and Phase 2 for all configurations.

[FCS_IPSEC_EXT.1.5](#)

Support for NAT traversal is included in IPsec.

FCS_IPSEC_EXT.1.6

Encrypted payloads will be encrypted using the selected IKE version and cryptographic algorithms selected. The selected cryptographic algorithms are applied to both Phase 1 and Phase 2 for all configurations except RFC6379.

FCS_IPSEC_EXT.1.7

SA lifetimes are specified in minutes for both IKEv1 and IKEv2. To specify the Phase 1 lifetime, the value "IKE Lifetime" should be set, the default value is 180 minutes. Valid times are 5-1440 minutes for Phase 1 lifetimes.

FCS_IPSEC_EXT.1.8

SA lifetimes are specified in minutes for both IKEv1 and IKEv2. To specify the Phase 2 lifetime, the value "Lifetime" should be set, the default value is 60 minutes. Valid times are 5-1440 minutes for Phase 2 lifetimes.

FCS_IPSEC_EXT.1.11

Diffie Hellman (DH) Groups are limited to group 14, group 19, and group 20. Group 24 is not available. Group 5 should not be selected.

FCS_IPSEC_EXT.1.14

If **Certificate** is selected as the **Authentication Type**, then when specifying the value of the **Peer Certificate Subject DN**, the specified distinguished name must be an exact match to the certificate the remote device is using. If not exactly matched, the tunnel will fail to negotiate. The peer certificate should be specified as stated in the client certificate beginning with the CN= field until the end of the DN is met. When applied to IPsec VPN configurations, the SAN extension in the certificate is not used to match against.

FIA_PSK_EXT.1

When IPsec VPNs are established using a pre-shared key (PSK), it is recommended to use a key of at least 22 characters. ClearPass supports PSK values of up to 128-character length. As with any other human derived password, it is recommended that PSK values make use of a mixture of password character types to maximize the entropy and minimize attack capabilities. Uppercase, lowercase, numerical, and special characters that are supported by both VPN peers are recommended to be used in any PSK.

FAU_STG_EXT.1

Audit integrity is crucial to ClearPass. As such, any modifications to the audit records themselves by anyone is not possible. The only action that an administrator may take involving modification of the logs is to configure the log file size limit and retention numbers in the FAU_STG_EXT.1 section. These settings will affect the on-box log retention settings. The ability to modify or delete records is not a function supported by ClearPass.

ClearPass is not intended to be a long-term audit storage system. The use of syslog to export data is recommended to transfer data to another system that has been built for the purpose of long-term audit record storage. Local audit records are stored for seven (7) days prior to automatic cleanup (deletion). To extend the local audit record storage, navigate to

Administration > Server Manager > Server Configuration and select the **Cluster-Wide Parameters**. The settings can be adjusted by modifying the value on the **Cleanup Intervals** tab. The Access Tracker events can be modified by adjusting the **Cleanup interval for Session log details in the database** parameter (default value is 7 days). The general audit (such as the Accounting) events can be modified by adjusting the **Old Audit Records cleanup interval** parameter (default value is 7 days). Event Viewer records are stored for seven (7) days prior to automatic cleanup. There is no user configurable setting to modify the Event Viewer log storage. Audit records that exceed cleanup intervals will be deleted from the file system and the space reclaimed to write new audit events.

ClearPass log file storage is limited by drive space. The typical storage duration for on-system log storage is seven (7) days. Navigate to **Administration > Server Manager > Log Configuration** and select the **System Level** tab.

The screenshot displays the 'Log Configuration' page in the Aruba ClearPass Policy Manager. The 'System Level' tab is active, showing configuration options for log files and syslog settings. A table lists 13 services with checkboxes for enabling syslog and dropdown menus for selecting filter levels and default levels.

Service Name	Enable Syslog	Syslog Filter Level	Default Level
1. Admin server	<input checked="" type="checkbox"/>	WARN	WARN
2. AirGroup notification service	<input type="checkbox"/>	WARN	WARN
3. Apache web server	<input checked="" type="checkbox"/>	All	ALL
4. ClearPass IPsec service	<input type="checkbox"/>	WARN	WARN
5. ClearPass network services	<input checked="" type="checkbox"/>	WARN	WARN
6. Domain service	<input type="checkbox"/>	All	ALL
7. Guest/Onboard	<input checked="" type="checkbox"/>	WARN	WARN
8. Micros Fidelio FIAS	<input type="checkbox"/>	WARN	WARN
9. Policy server	<input checked="" type="checkbox"/>	WARN	WARN
10. RadSec service	<input checked="" type="checkbox"/>	WARN	WARN
11. Radius server	<input checked="" type="checkbox"/>	WARN	WARN
12. Syslog client service	<input checked="" type="checkbox"/>	WARN	WARN
13. TACACS+ server	<input type="checkbox"/>	WARN	WARN

The number and size of log files may be specified based on observed logging levels. The number and size limits apply to all log file settings. Modifying these values will affect the log files that contain information created by RADIUS, Policy, and other services. Reducing the capacity may decrease the information available to less than seven (7) days. Increasing may cause issues with system free disk space thresholds.

The IP address of the external syslog server that will receive audit messages from ClearPass should be specified, along with all the appropriate audit events to be sent. The default setting does not select any services to enable syslog. It is recommended at least one service be selected. All audit messages equal or higher in priority to the **Syslog Filter Level** setting will be sent to the specified syslog server.

ClearPass does not transfer syslog messages in real time. Messages are queued to a syslog buffer that then transfers all messages to the syslog server every 120 seconds. This value may be reduced to a minimum of every 30 seconds, but will default to every 120 seconds. The potential delay in message queue and receipt by the remote server should be noted to comply with Common Criteria evaluated settings.

Note: The ClearPass IPsec service is now included in the list of services whose service logs can be sent to a syslog server, and is available in the Service Name list on the **Administration > Server Manager > Log Configuration > System Level** tab.

FTA_TSE.1

The User Guide documentation section titled “Configuring Enforcement Policies” should be consulted prior to specifying policies. ClearPass allows for policies to be established using multiple criteria. The security target notes that session establishment may be denied using criteria incorporating time of day, account status, role mapping, or location.

Navigate to **Configuration > Enforcement > Policies** to view the **Enforcement Policies** screen. The default policies cannot be modified, but they may be copied to a new profile. New policies can be directly created by clicking the **Add** button in the top right corner.

ClearPass Policy Manager

Configuration » Enforcement » Policies

Enforcement Policies

ClearPass controls network access by evaluating an enforcement policy associated with the service.

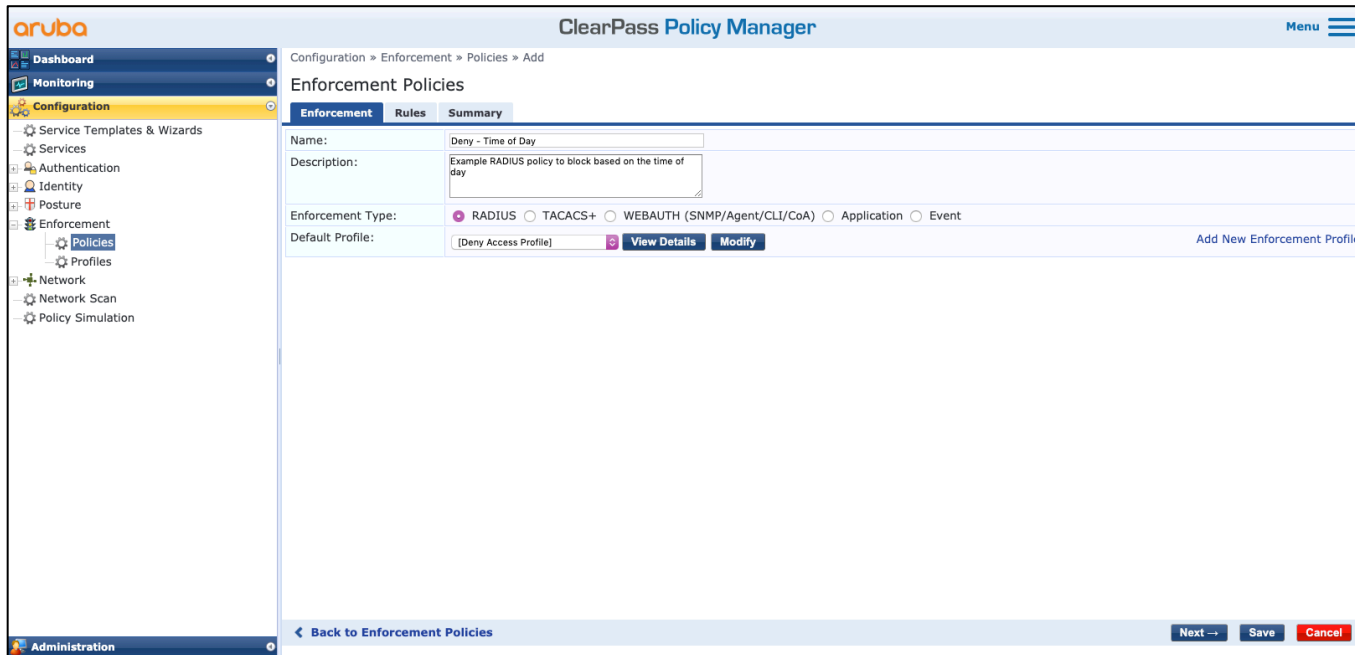
Filter: Name contains Show 50 records

#	Name	Type	Description
1.	[Admin Network Login Policy]	TACACS	Enforcement policy controlling access to Policy Manager Admin
2.	[AirGroup Enforcement Policy]	RADIUS	Enforcement policy controlling access for AirGroup devices
3.	[Aruba Device Access Policy]	TACACS	Enforcement policy controlling access to Aruba device
4.	[Device Registration Disconnect]	WEBAUTH	Enforcement policy to disconnect devices from network
5.	[Guest Operator Logins]	Application	Enforcement policy controlling access to Guest application
6.	[Insight Operator Logins]	Application	Enforcement policy controlling access to Insight application
7.	mTLS-login ClearPass Certificate SSO Login Enforcement Policy	Application	
8.	mTLS-login ClearPass Identity Provider Enforcement Policy	Application	
9.	[Sample Allow Access Policy]	RADIUS	Sample policy to allow network access
10.	[Sample Deny Access Policy]	RADIUS	Sample policy to deny network access

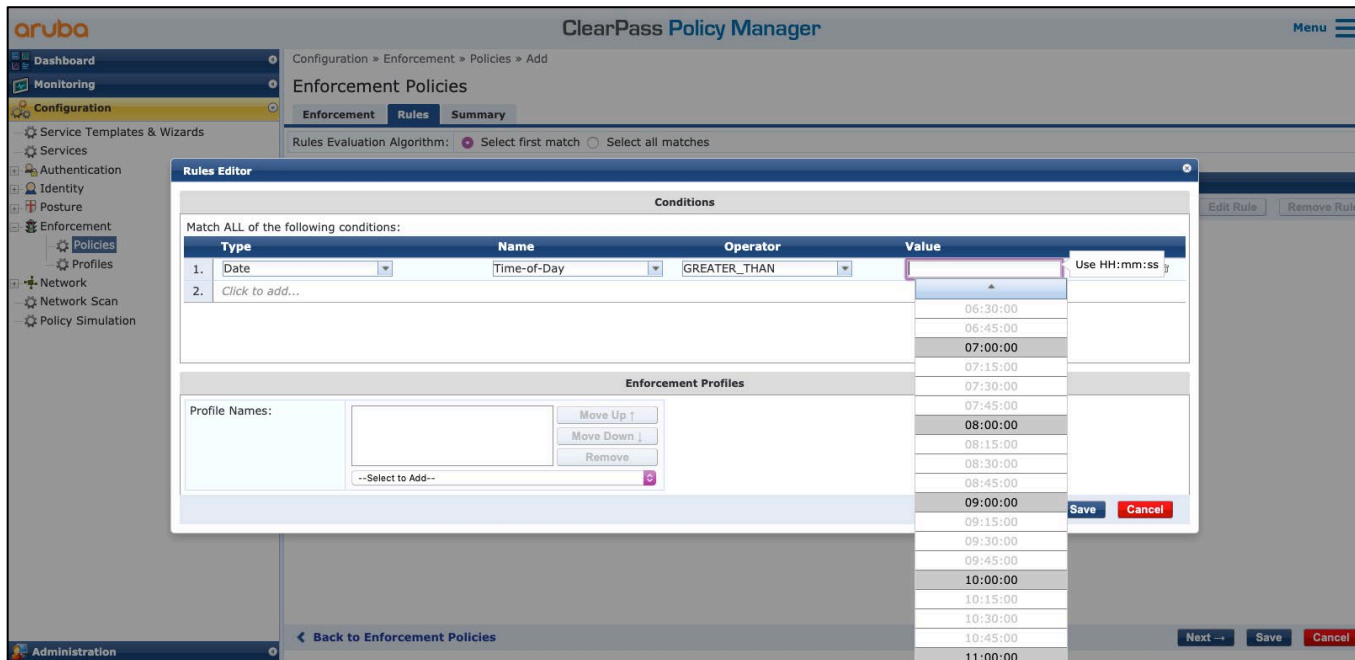
Showing 1-10 of 10

The following examples illustrate RADIUS policies that deny access based on specified criteria.

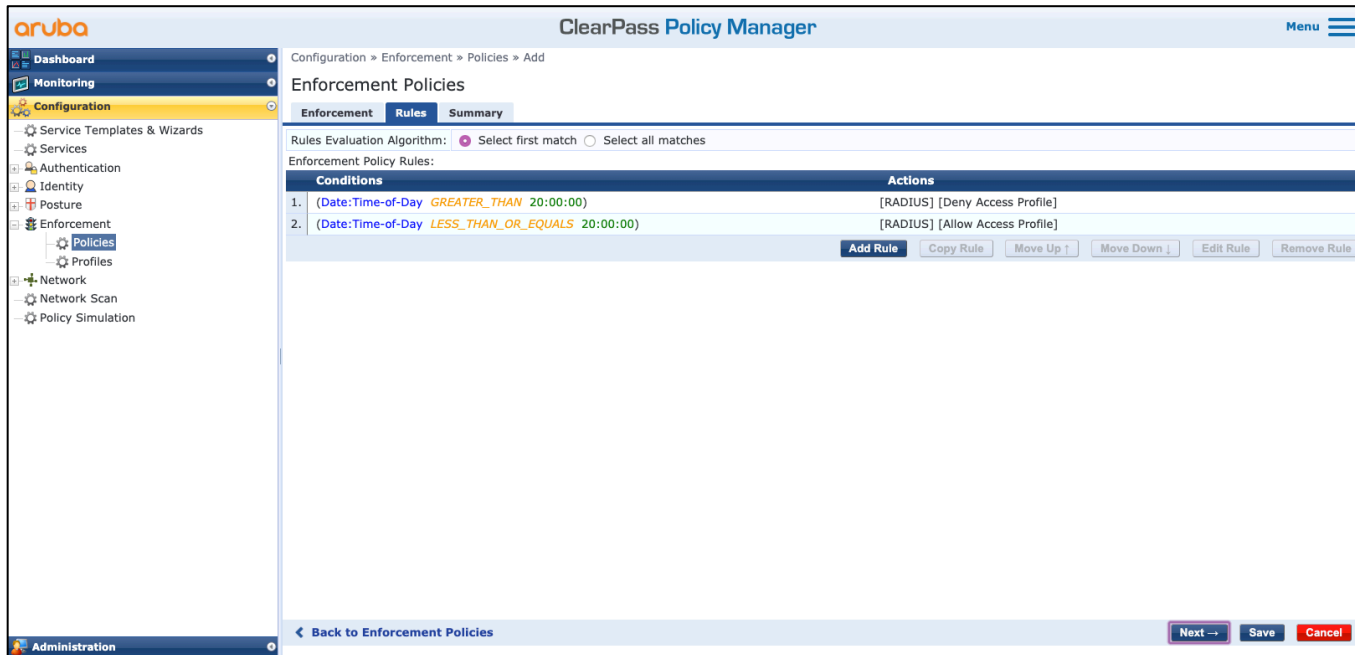
Time of day may be used for policy decisions by adding a new policy. Specify the information required on the **Enforcement** tab before proceeding.



On the **Rules** tab, rules must be created to determine the appropriate actions. Clicking the **Add Rule** button opens a pop-up window where you can build the rule and specify the appropriate action to take. This example shows specifying the values required to restrict access based on time of day.



The illustrated rule is in process of selecting a time of day that can be used to control access. Once specified, the enforcement profile can be selected to determine the available action or actions that will be applied. In this example, the policy is defined to deny access after 20:00.



Policy elements may be added to build a comprehensive rule set. Rules may be selected to be evaluated based on first match or apply all actions that evaluation would be met by. This rule builds policy based on first match.



The **Summary** tab provides a review of all configured elements.

Configuration » Enforcement » Policies » Add

Enforcement Policies

Enforcement policy has not been saved

Enforcement Rules Summary

Enforcement:

Name: Deny - Time of Day
 Description: Example RADIUS policy to block based on the time of day.
 Enforcement Type: RADIUS
 Default Profile: [Deny Access Profile]

Rules:

Rules Evaluation Algorithm: First applicable

Conditions	Actions
1. (Date:Time-of-Day GREATER_THAN 20:00:00)	[RADIUS] [Deny Access Profile]
2. (Date:Time-of-Day LESS_THAN_OR_EQUALS 20:00:00)	[RADIUS] [Allow Access Profile]

← Back to Enforcement Policies

Next → Save Cancel

When the policy is saved, it will immediately be usable. The newly created policy will be displayed with existing enforcement policies.

Authentication sources help determine the location where role information is available. ClearPass includes a local user repository, available at **Configuration > Identity > Local Users**. Users created in this location are subject to roles defined in ClearPass (available at **Configuration > Identity > Roles**). External authentication sources, such as Microsoft Active Directory, will have their roles available within the system itself. Similar to time-of-day restrictions, a policy to deny access to users with the Contractor role could be created using a rule similar to the one displayed below.

Configuration » Enforcement » Policies » Add

Enforcement Policies

Enforcement policy has not been saved

Enforcement Rules Summary

Enforcement:

Name: Role based allow
 Description: Example policy to deny contractors access to the network
 Enforcement Type: RADIUS
 Default Profile: [Deny Access Profile]

Rules:

Rules Evaluation Algorithm: First applicable

Conditions	Actions
1. (Authorization:[Local User Repository]:Role_Name EQUALS_IGNORE_CASE EMPLOYEE)	[RADIUS] [Allow Access Profile]
2. (Authorization:[Local User Repository]:Role_Name EQUALS_IGNORE_CASE Contractor)	[RADIUS] [Deny Access Profile]

← Back to Enforcement Policies

Next → Save Cancel

The operator “EQUALS_IGNORE_CASE” is used to show the flexibility of the policy engine. Remotely-defined roles may have uppercase or lowercase characters that make an exact match difficult, so this function allows for case-insensitivity.

Employees are allowed access by policy; contractors are denied access. If an employee has both roles available to them, the "allow" rule would match first in this definition.

Account status may be used to determine policy. An example policy that allows successful machine authentication on the network but denies failed or user-only authentication could be created using a policy similar to the one below.

The screenshot shows the Aruba ClearPass Policy Manager interface. The left sidebar contains navigation options: Dashboard, Monitoring, Configuration (selected), Service Templates & Wizards, Services, Authentication, Identity, Posture, Enforcement, Policies (selected), Profiles, Network, Network Scan, and Policy Simulation. The main content area is titled 'ClearPass Policy Manager' and 'Enforcement Policies'. A message states 'Enforcement policy has not been saved'. The configuration is for a policy named 'Deny on Status' with the description 'Example policy to deny based on account status for non-machine authentication'. The enforcement type is RADIUS and the default profile is '[Deny Access Profile]'. The rules evaluation algorithm is 'First applicable'. The policy has two rules:

Conditions	Actions
1. (Authentication:Status MATCHES_ANY User, Failed)	[RADIUS] [Deny Access Profile]
2. (Authentication:Status EQUALS Machine)	[RADIUS] [Allow Access Profile]

At the bottom, there are buttons for 'Back to Enforcement Policies', 'Next', 'Save', and 'Cancel'.

As with a role-based policy, the use of various authentication sources may expand the options available to be used in a policy beyond those provided in the local user system.

Location may also be used to build policy. When using remote data sources, it may be possible to use geographic controls such as country or state. When using locally-defined elements exclusively, a location-based policy is likely to originate from connection specific information.

The screenshot shows the Aruba ClearPass Policy Manager interface. The left sidebar contains navigation options: Dashboard, Monitoring, Configuration (selected), Service Templates & Wizards, Services, Authentication, Identity, Posture, Enforcement, Policies (selected), Profiles, Network, Network Scan, and Policy Simulation. The main content area is titled 'ClearPass Policy Manager' and 'Enforcement Policies'. A message states 'Enforcement policy has not been saved'. The configuration is for a policy named 'location based block' with the description 'Example policy to deny employees access based on AP location'. The enforcement type is RADIUS and the default profile is '[Deny Access Profile]'. The rules evaluation algorithm is 'First applicable'. The policy has two rules:

Conditions	Actions
1. (Authorization:[Local User Repository]:Role_Name EQUALS CONTRACTOR)	[RADIUS] [Allow Access Profile]
2. (Connection:AP-Name BEGINS_WITH aruba5) AND (Authorization:[Local User Repository]:Role_Name EQUALS_IGNORE_CASE employee)	[RADIUS] [Deny Access Profile]

At the bottom, there are buttons for 'Back to Enforcement Policies', 'Next', 'Save', and 'Cancel'.

This example policy will deny access to any employee attempting to use access points that have names starting with “aruba5”, but allow any user with the role “contractor”. This policy also combines multiple elements into a single rule: role and location.

FPT_TST_EXT.1 (self-tests)

ClearPass will execute self-tests on the cryptographic core when operating in Common Criteria mode. These tests are also executed as part of the FIPS operating mode. To ensure the integrity of the module and the correctness of the cryptographic functionality at start up, self-tests are run. In the event of a self-test error, the module will log the error and will halt, resulting in a failure to boot ClearPass. The module must be initialized into memory to resume function.

Power-on self-tests are executed automatically when the module is loaded into memory. The module verifies the integrity of the runtime executable using a HMAC-SHA-256 digest computed at build time. If the fingerprints match, the power-up self-tests are then performed. If the power-up self-test is successful, a flag is set to place the module in FIPS mode.

TYPE	DETAIL
Software Integrity Check	<ul style="list-style-type: none"> • HMAC-SHA1 on all module components
Known Answer Tests	<ul style="list-style-type: none"> • AES ECB • AES GCM • AES CCM • AES XTS • AES CMAC • Triple-DES ECB • Triple-DES CMAC • Diffie-Hellman • EC Diffie-Hellman • HMAC-SHA-1, HMAC-SHA-224, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512 • RSA • SHA-1, SHA-256 and SHA-512 • SHA3-256, SHA3-512, SHAKE-128 and SHAKE-256 • SP 800-90 DRBG (CTR_DRBG) • TLS KDF • SSH KDF • PBKDF KDF • HKDF KDF • KDKDF KDF
Pair-wise Consistency Tests	<ul style="list-style-type: none"> • RSA

	<ul style="list-style-type: none"> • ECDSA • DSA
--	--

Power-on self-tests include capabilities not available in Common Criteria mode.

Input, output, and cryptographic functions cannot be performed while the module is in a self-test or error state because the module is single-threaded and will not return to the calling application until the power-up self-tests are complete. If the power-up self-tests fail, subsequent calls to the module will also fail - thus no further cryptographic operations are possible.

The module implements the following conditional self-tests upon key generation or upon random number generation, respectively:

TYPE	DETAIL
Pair-wise Consistency Tests	<ul style="list-style-type: none"> • RSA • ECDSA • DSA

The module verifies the integrity of the runtime executable using a HMAC-SHA1 digest which is computed at build time. If this computed HMAC-SHA1 digest matches the stored, known digest, then the power-up self-test (consisting of the algorithm-specific Pairwise Consistency and Known Answer tests) is performed. If any component of the power-up self-test fails, an internal global error flag is set to prevent subsequent invocation of any cryptographic function calls. Any such power-up self-test failure is a hard error that can only be recovered by reinstalling the module. The power-up self-tests may be performed at any time by reloading the module. Additionally, the pair-wise consistency tests are run as a conditional test each time a key pair is generated.

No operator intervention is required during the running of the self-tests.

FCS_EAP-TLS_EXT.1

When operating in Common Criteria mode, ClearPass will only use the cipher suites specified in section FCS_TLSS_EXT.2.1. TLS_ECDSA ciphers will not be used without an ECDSA key available for RADIUS.

APPENDIX A: FAU_GEN.1 AUDITABLE EVENTS

Many implementations use external syslog servers instead of locally hosted audit messages. ClearPass supports four (4) export event formats: Standard, Log Enhanced Event Format (LEEF), Common Event Format (CEF), and the RFC 5424 compliant format (RFC 5424). The default export syslog format is standard, sometimes referred to as raw.

Samples of the export event format syslog information can be found in the ClearPass User Guide <https://www.arubanetworks.com/techdocs/ClearPass/6.11/PolicyManager/index.htm>, in the Administration section under the heading “Export Event Format Types—Examples”. The User Guide will also describe the format of the various messages that are displayed.

List of auditable events by Common Criteria requirement. Events that include audit by ClearPass will specify the location to observe the audit message. These will be specified as “Audit Observed in” and specify the Web UI location messages of this type are located. Some events are logged in more than one observable location and will have examples specified for each event.

Audit events located in the **Monitoring > Audit Viewer** location will be noted based upon the tab the event is notified in.

Most events in the Audit Viewer will have the ability to note three (3) tabs: Old Data, New Data, Inline Difference. This allows the administrator to see the original value (Old Data), the value that was set (New Data), and the single view to note both old and new together (Inline Difference).

Version note: The ClearPass version information displayed in syslog entries will update according to the operating ClearPass release. The message content will not change between versions.

Format of entries noted below

Common Criteria Requirement	
Auditable Events	The criteria requirement of stated entries to note. Requirements with no auditable events required will be stated as "None" and shaded.
Additional Content	Any additional audit requirements to include. Requirements with no additional content to auditable events required will be stated as "None" and shaded.
Audit Observed In	The location of the audit message when viewed through the Web UI. Navigation to location in the Web UI is stated.
Audit Event Details	Generalized example audit message. Fields will be distributed to match the available offerings within individual audit records. Note that italicized values in square braces (<i>[]</i>) indicate values that will be populated uniquely for the sample audit message. Examples include IP addresses, time stamps, etc. Not all events are fully described in this section, but at least one sample is provided for each activity.
syslog example(s)	Real examples of output sent from ClearPass to an external syslog server for all observable events with appropriate auditable events and additional content. Audit messages were exported using Common Export Format (CEF) and Comments are typically in <i>italic</i> font. Areas are broken up by bold font.

NDCPP22e: FAU_GEN.1	
Auditable Events	None
Additional Content	None
syslog example(s)	<p>Shutdown of the Audit Function (All TOE services stopped):</p> <pre>2023-02-21T20:44:33.611-05:00 arubacp-phys [] [R:] DEBUG com.avenda.tips.syslog.Syslogger - 1 2023-02-21T20:44:33.610-05:00 192.168.144.3 ClearPass 55408 1-1-0 [timeQuality tzKnown="1"][origin swVersion="6.11.1.251216" software="PolicyManager" ip="192.168.144.3" enterpriseId="1.3.6.1.4.1.14823"][clearPass@14823 eventId="3002" Action="Success" Category="System" Description="System is restarting" Level="INFO" Component="shutdown" CppmNode.CPPM-Node="192.168.144.3" Timestamp="2023-02-21T20:31:04.079-05:00"]</pre> <p>The TOE logs shutdown of all of its services one by one. Each service is responsible for its own logging. The audits follow this format with only the service changing:</p> <pre>2023-02-20T11:03:22.666-05:00 arubacp-phys [] [R:] DEBUG com.avenda.tips.syslog.Syslogger - 2023-02-20 11:03:22,666 192.168.144.3 System Events 962 1 0 Timestamp=Feb 20 2023 11:03:05.960 EST,Component=Policy server,Level=INFO,Category=stop,Action=Success,Description=Performed action stop on Policy server</pre>

	<p>Startup of the Audit Function (all TOE services startup)</p> <p>The TOE logs startup of all of its services one by one. Each service is responsible for its own logging. The audits follow this format with only the service changing:</p> <p>2023-02-20T11:09:04.535-05:00 arubacp-phys [] [R:] DEBUG com.avenda.tips.syslog.Syslogger - 2023-02-20 11:09:04,535 192.168.144.3 System Events 22 1 0 Timestamp=Feb 20 2023 11:06:15.399 EST,Component=Policy server,Level=INFO,Category=start,Action=Success,Description=Performed action start on Policy server</p>
--	---

NDcPP22e: FAU_GEN.2	Auditable Events	None	Additional Content	None
---------------------	------------------	------	--------------------	------

NDcPP22e: FAU_STG_EXT.1	Auditable Events	None	Additional Content	None
----------------------------	------------------	------	--------------------	------

AUTHSVREP10: FCO_NRO.1	
Auditable Events	Client request for which the TOE does not have a shared secret
Additional Content	Identity of the client, contents of EAP-response (if present).
Audit Observed In	Monitoring > Event Viewer
Audit Event Details	<p>Source: RADIUS</p> <p>Level: ERROR</p> <p>Category: Authentication</p> <p>Action: Unknown</p> <p>Timestamp: <i>[time]</i></p> <p>Description: RADIUS authentication attempt from unknown NAD <i>[IP:Port]</i></p> <p>Description: Failed to decode RADIUS packet – Received packet from <i>[IP]</i> with invalid Message-Authenticator! (Shared secret may be incorrect.)</p>
syslog example(s)	<p>2022-11-01T11:36:32.089758-04:00 2022-11-01 11: 36:32,88 192.168.144.3 Audit Records 226 1 0</p> <p>Timestamp=Nov 01 2022 11:36:01.496</p> <p>EDT,Component=RADIUS,Level=ERROR,Category=Authentication,Action=Unknown,Description=Failed to decode RADIUS packet - Received packet from 192.168.144.36 with invalid Message-Authenticator! (Shared secret may be incorrect.)</p>

AUTHSVREP10: FCO_NRR.1	Auditable Events	None	Additional Content	None
---------------------------	------------------	------	--------------------	------

NDcPP22e: FCS_CKM.1	Auditable Events	None	Additional Content	None
---------------------	------------------	------	--------------------	------

NDcPP22e: FCS_CKM.2	Auditable Events	None	Additional Content	None
---------------------	------------------	------	--------------------	------

NDcPP22e: FCS_CKM.4	Auditable Events	None	Additional Content	None
---------------------	------------------	------	--------------------	------

NDcPP22e: FCS_COP.1/DATAENCRYPTION	Auditable Events	None	Additional Content	None
---------------------------------------	------------------	------	--------------------	------

NDcPP22e: FCS_COP.1/SIGGEN	Auditable Events	None	Additional Content	None
-------------------------------	------------------	------	--------------------	------

NDcPP22e: FCS_COP.1/HASH	Auditable Events	None	Additional Content	None
-----------------------------	------------------	------	--------------------	------

NDcPP22e: FCS_COP.1/KEYEDHASH	Auditable Events	None	Additional Content	None
----------------------------------	------------------	------	--------------------	------

AUTHSVREP10: FCS_EAP-TLS_EXT.1	
Auditable Events	Protocol failures. Establishment of a TLS session
Additional Content	If failure occurs, record a descriptive reason for the failure
Audit Observed In	Configuration > Access Tracker
Audit Event Details	Error Code: 215 Error Category: Authentication failure Error Message: TLS session error Alerts for this Request [AUTHENTICATOR] [Failure] [failure location] [details] [reason] <i>[authenticator-method]: Error in establishing TLS session</i>
	[sample audit] Error Code: 215 Error Category: Authentication failure Error Message: TLS session error

	<p>Alerts for this Request</p> <p>RADIUS</p> <p>TLS Handshake failed in SSL_read with error:140760FC:SSL routines:SSL23_GET_CLIENT_HELLO:unknown protocol</p> <p>eap-tls: Error in establishing TLS session</p>
<p>syslog example(s)</p>	<p>Establishment of a TLS Session:</p> <p>The following messages below together comprise the required auditable information for a successful EAP TLS session. After the initial Access Request, the audit records include the Session ID which verifies that they are all from the same session:</p> <p>2023-02-19T17:20:44.969650-05:00 192.168.144.3 2023-02-19 17: 20:44,969 [main] DEBUG RadiusServer.Radius - rad_recv: Access-Request packet from host 192.168.144.36 ,port:52534, id=6, length=1575 time=1676845244969652863</p> <p>2023-02-19T17:20:44.970093-05:00 192.168.144.3 2023-02-19 17: 20:44,970 [Th 36 Req 357] DEBUG RadiusServer.Radius - User-Name = "client-rsa"</p> <p>2023-02-19T17:20:44.970608-05:00 192.168.144.3 2023-02-19 17: 20:44,970 [Th 36 Req 357] DEBUG RadiusServer.Radius - NAS-IP-Address = 192.168.144.36</p> <p>2023-02-19T17:20:44.986121-05:00 192.168.144.3 2023-02-19 17: 20:44,986 [Th 37 Req 358 SessId R00000039-01-63f2a0bc] DEBUG RadiusServer.Radius - rlm_eap: EAP/tls</p> <p>2023-02-19T17:20:44.994634-05:00 192.168.144.3 2023-02-19 17: 20:44,994 [Th 37 Req 358 SessId R00000039-01-63f2a0bc] DEBUG RadiusServer.Radius - rlm_eap_tls: >>> TLS 1.2 Handshake [length 0010], Finished</p> <p>2023-02-19T17:20:45.201000-05:00 192.168.144.3 2023-02-19 17: 20:45,200 [Th 38 Req 359 SessId R00000039-01-63f2a0bc] INFO RadiusServer.Radius - rlm_policy: Received Accept Enforcement Profile</p> <p>Protocol Failure:</p> <p>The following 6 messages comprise the required auditable information identifying a failed EAP TLS session. After the initial Access Request, the audit records include the Session ID which verifies that they are all from the same session. All protocol failures are audited with the above set of messages with the exception of the error messages with reason for failure changing:</p> <p>2023-02-19T16:45:06.920459-05:00 192.168.144.3 2023-02-19 16: 45:07,179 [main] DEBUG RadiusServer.Radius - rad_recv: Access-Request packet from host 192.168.144.36 ,port:33246, id=1, length=302 time=1676843107179943425</p> <p>2023-02-19T16:45:06.920529-05:00 192.168.144.3 2023-02-19 16: 45:07,180 [Th 38 Req 103] DEBUG RadiusServer.Radius - User-Name = "client-rsa"</p> <p>2023-02-19T16:45:06.921105-05:00 192.168.144.3 2023-02-19 16: 45:07,181 [Th 38 Req 103] DEBUG RadiusServer.Radius - NAS-IP-Address = 192.168.144.36</p> <p>2023-02-19T16:45:06.927466-05:00 192.168.144.3 2023-02-19 16: 45:07,187 [Th 38 Req 103 SessId R00000011-01-63f29863] ERROR RadiusServer.Radius - TLS Alert write:fatal:handshake failure</p>

	<p>2023-02-19T16:45:06.927657-05:00 192.168.144.3 2023-02-19 16: 45:07,187 [Th 38 Req 103 SessId R00000011-01-63f29863] ERROR RadiusServer.Radius - rlm_eap_tls: SSL_read failed in a system call (-1), TLS session fails. error:1417A0C1:SSL routines:tls_post_process_client_hello:no shared cipher</p> <p>2023-02-19T16:45:32.478524-05:00 192.168.144.3 2023-02-19 16: 45:32,668 [Th 40 Req 153 SessId R00000016-01-63f2987c] INFO RadiusServer.Radius - rlm_policy: Received Deny Enforcement Profile</p>
--	--

NDcPP22e: FCS_HTTPS_EXT.1	
Auditable Events	Failure to establish a HTTPS Session.
Additional Content	Reason for failure.
Audit Observed In	Monitoring > Event Viewer
Audit Event Details	<p>Source: Admin UI</p> <p>Level: ERROR</p> <p>Category: Login Failed</p> <p>Action: None</p> <p>Timestamp: <i>[time]</i></p> <p>Description: error:[error] [information] [possible reason] Client IP address: [IP]</p> <hr/> <p>[example audit]</p> <p>Source: Admin UI</p> <p>Level: ERROR</p> <p>Category: Login Failed</p> <p>Action: None</p> <p>Timestamp: <i>[time]</i></p> <p>Description: error:1408A0C1:SSL routines:ssl3_get_client_hello:no shared cipher -- Too restrictive SSLCipherSuite or using DSA server certificate? Client IP address: <i>[IP]</i></p> <hr/> <p>[example audit]</p> <p>Source: Admin UI</p> <p>Level: ERROR</p> <p>Category: Login Failed</p> <p>Action: None</p> <p>Timestamp: <i>[time]</i></p> <p>Description: error:1408A10B:SSL routines:ssl3_get_client_hello:wrong version number Client IP address: <i>[IP]</i></p>
syslog example(s)	Refer to FCS_TLSS_EXT.2 for cert auth related failures and NDcPP22e:FIA_UIA_EXT.1 for username/password failure

NDcPP22e: FCS_IPSEC_EXT.1	
Auditable Events	Failure to establish an IPsec SA.
Additional Content	Reason for failure.
Audit Observed In	Monitoring > Event Viewer
Audit Event Details	<p>Source: ClearPass IPsec Tunnel</p> <p>Level: ERROR</p> <p>Category: Tunnel Action</p> <p>Action: [empty]</p> <p>Timestamp: <i>[time]</i></p> <p>Description: Tunnel (Remote IP : <i>[IP]</i>):</p> <p>Constraint check failed: <i>[reason]</i></p>
syslog example(s)	<p>2023-02-24T16:05:19-05:00 192.168.144.3 cppm.ipsec[336580]: Feb 24 16:05:19 12[IKE] <ipsec-3076 2> tried 1 shared key for '%any' - '192.168.145.36', but MAC mismatched</p> <p>2023-02-24T16:05:19-05:00 192.168.144.3 cppm.ipsec[336580]: Feb 24 16:05:19 12[ENC] <ipsec-3076 2> generating IKE_AUTH response 1 [N(AUTH_FAILED)]</p> <p>2023-02-24T16:07:42-05:00 192.168.144.3 cppm.ipsec[336580]: Feb 24 16:07:42 14[IKE] <5> received proposals unacceptable</p> <p>2023-02-24T16:09:17-05:00 192.168.144.3 cppm.ipsec[336580]: Feb 24 16:09:17 07[IKE] <ipsec-3076 6> no acceptable proposal found</p> <p>2023-02-24T16:09:17-05:00 192.168.144.3 cppm.ipsec[336580]: Feb 24 16:09:17 07[IKE] <ipsec-3076 6> failed to establish CHILD_SA, keeping IKE_SA</p> <p>2023-02-24T16:11:51-05:00 192.168.144.3 cppm.ipsec[336580]: Feb 24 16:11:51 05[ENC] <9> parsed AGGRESSIVE request 0 [SA KE No ID V V V V]</p> <p>2023-02-24T16:11:51-05:00 192.168.144.3 cppm.ipsec[336580]: Feb 24 16:11:51 05[IKE] <9> no IKE config found for 192.168.145.3...192.168.145.36, sending NO_PROPOSAL_CHOSEN</p> <p>2023-02-24T18:25:17-05:00 192.168.144.3 cppm.ipsec[336580]: Feb 24 18:25:17 13[CFG] <13> looking for peer configs matching 192.168.145.3[%any]...192.168.145.36[C=US, ST=MD, L=Catonsville, O=GSS, CN=tl39-16x.example.com]</p> <p>2023-02-24T18:25:17-05:00 192.168.144.3 cppm.ipsec[336580]: Feb 24 18:25:17 13[CFG] <13> no matching peer config found</p>

NDcPP22e: FCS_NTP_EXT.1	
Auditable Events	Configuration of a new time server Removal of configured time server
Additional Content	Identity if new/removed time server
syslog example(s)	<p>Configuring new NTP server</p> <p>2023-02-20T16:03:09.579-05:00 arubacp-phys [] [R:] DEBUG com.avenda.tips.syslog.Syslogger - 2023-02-20 16:03:09,579 192.168.144.3 Audit Records 25 1 0 Timestamp=Feb 20 2023 16:02:52.737 EST,EntityName=192.168.145.36,Category=Remote Time Server,Action=ADD,User=admin</p> <p>Removing configured NTP server</p> <p>2023-02-20T16:03:09.580-05:00 arubacp-phys [] [R:] DEBUG com.avenda.tips.syslog.Syslogger - 2023-02-20 16:03:09,580 192.168.144.3 Audit Records 26 1 0 Timestamp=Feb 20 2023 16:02:52.587 EST,EntityName=192.168.145.36,Category=Remote Time Server,Action=REMOVE,User=admin</p>

AUTHSVR10: FCS_RADIUS_EXT.1	
Auditable Events	Protocol failures. Success/Failure of authentication
Additional Content	If failure occurs, record a descriptive reason for the failure
Audit Observed In	Monitoring > Event Viewer
Audit Event Details	<p>Source: RADIUS</p> <p>Level: ERROR</p> <p>Category: Authentication</p> <p>Action: Unknown</p> <p>Timestamp: <i>[time]</i></p> <p>Description: Received EAP-Request message from Client (MAC address=UnKnown) via NAS (Source IP:<i>[IP]</i>). Sending EAP-Response with NAK.</p> <hr/> <p>Source: RADIUS</p> <p>Level: ERROR</p> <p>Category: Authentication</p> <p>Action: Unknown</p> <p>Timestamp: <i>[time]</i></p> <p>Description: Received INVALID RADIUS packet – WARNING: Malformed RADIUS packet from host <i>[IP]</i>: EAP Message and one more authentication vector(<i>[method]</i>) are present</p>

	<p>Source: RADIUS</p> <p>Level: ERROR</p> <p>Category: Authentication</p> <p>Action: Unknown</p> <p>Timestamp: <i>[time]</i></p> <p>Description: Received EAP message with invalid EAP code from Client (MAC address=UnKnown) via NAS (Source IP:<i>[IP]</i>).</p>
	<p>Source: RADIUS</p> <p>Level: ERROR</p> <p>Category: Authentication</p> <p>Action: Unknown</p> <p>Timestamp: <i>[time]</i></p> <p>Description: Failed to decode RADIUS packet – Received packet from <i>[IP]</i> with invalid Message-Authenticator! (Shared secret may be incorrect.)</p>
syslog example(s)	<p>Successful Authentication</p> <p>2023-02-01T13:16:02.797139-05:00 192.168.144.3 2023-02-01 13: 16:02,796 [Th 37 Req 229 SessId R00000016-01-63daac62] DEBUG RadiusServer.Radius - Sending Access-Accept of id 9 to 192.168.144.36 port 44005</p> <p>Protocol Failures</p> <p>2022-10-25T15:36:02.076939-04:00 2022-10-25 15: 36:02,76 192.168.144.3 Audit Records 1277 1 0 Timestamp=Oct 25 2022 15:35:49.480 EDT,Component=RADIUS,Level=ERROR,Category=Authentication,Action=Unknown,Description Failed to decode RADIUS packet - Received packet from 192.168.145.36 with invalid Message-Authenticator! (Shared secret may be incorrect.)</p> <p>2022-10-26T09:20:14.579167-04:00 2022-10-26 09: 20:14,578 192.168.144.3 Audit Records 1470 1 0 Timestamp=Oct 26 2022 09:19:44.614 EDT,Component=RADIUS,Level=ERROR,Category=Authentication,Action=Unknown,Description=Received INVALID RADIUS packet - WARNING: Malformed RADIUS packet from host 192.168.145.36: too long (length 65413 > maximum 4096</p> <p>2022-10-26T09:20:44.584678-04:00 2022-10-26 09: 20:44,583 192.168.144.3 Audit Records 1475 1 0 Timestamp=Oct 26 2022 09:20:29.821 EDT,Component=RADIUS,Level=ERROR,Category=Authentication,Action=Unknown,Description=Received INVALID RADIUS packet - WARNING: Bad RADIUS packet from host 192.168.145.36: unknown packet code 55</p>

	<p>2022-10-26T09:14:44.537801-04:00 2022-10-26 09: 14:44,512 192.168.144.3 Audit Records 1466 1 0 Timestamp=Oct 26 2022 09:14:14.108 EDT,Component=RADIUS,Level=ERROR,Category=Authentication,Action=Unknown,Description=Received INVALID RADIUS packet - WARNING: Insecure packet from host 192.168.145.36: Received EAP-Message with no Message-Authenticator.</p> <p>2022-12-06T13:04:37.706983-05:00 2022-12-06 13: 04:37,705 192.168.144.3 Audit Records 103 1 0 Timestamp=Dec 06 2022 13:04:13.062 EST,Component=RADIUS,Level=ERROR,Category=Authentication,Action=Unknown,Description=Received INVALID RADIUS packet - WARNING: Malformed RADIUS packet from host 192.168.144.36: Access- Request contains response attribute(Error-Cause).</p> <p>2022-12-06T13:14:07.763127-05:00 2022-12-06 13: 14:07,762 192.168.144.3 Audit Records 137 1 0 Timestamp=Dec 06 2022 13:13:46.426 EST,Component=RADIUS,Level=ERROR,Category=Authentication,Action=Unknown,Description=Received INVALID RADIUS packet - WARNING: Malformed RADIUS packet from host 192.168.144.36: EAP Message and one more authentication vector(User-Password) are present.</p>
--	---

AUTHSVR10: FCS_RADSEC_EXT.1	
Auditable Events	Failure to establish RadSec session
Additional Content	Reason for failure
syslog example(s)	<p>2023-02-25T15:49:28.092419-05:00 192.168.144.3 2023-02-25 15: 49:28,092 [192.168.144.36-12] ERROR RadSec - tlsservernew: SSL: error:1417C0C7:SSL routines:tls_process_client_certificate:peer did not return a certificate</p> <p>2023-02-25T15:52:31.313945-05:00 192.168.144.3 2023-02-25 15: 52:31,448 [192.168.144.36-6] WARN RadSec - verify error: num=68:CA signature digest algorithm too weak:depth=0:/C=US/ST=MD/L=Catonsville/O=GSS/CN=client-bears-md5-sig-rsa</p> <p>2023-02-25T15:53:34.583943-05:00 192.168.144.3 2023-02-25 15: 53:34,609 [192.168.144.36-12] WARN RadSec - verify error: num=19:self signed certificate in certificate chain:depth=1:/C=US/ST=MD/L=Catonsville/O=GSS/emailAddress=rootca-unacceptable- rsa@gossamersec.com/CN=rootca-unacceptable-rsa</p> <p>2023-02-25T15:54:31.524128-05:00 192.168.144.3 2023-02-25 15: 54:31,504 [192.168.144.36-6] WARN RadSec - verify error: num=26:unsupported certificate purpose:depth=0:/C=US/ST=MD/L=Catonsville/O=GSS/CN=client-no-auth-eku-rsa</p> <p>2023-02-25T15:55:26.560072-05:00 192.168.144.3 2023-02-25 15: 55:26,559 [192.168.144.36-12] ERROR RadSec - tlsservernew: SSL: error:0D08303A:asn1 encoding routines:asn1_template_noexp_d2i:nested asn1 error</p> <p>2023-02-25T15:56:54.860977-05:00 192.168.144.3 2023-02-25 15: 56:54,860 [192.168.144.36-6] ERROR RadSec - tlsservernew: SSL: error:0407008A:rsa routines:RSA_padding_check_PKCS1_type_1:invalid padding</p>

<p>2023-02-25T16:02:16.972347-05:00 192.168.144.3 2023-02-25 16: 02:16,972 [192.168.144.36-6] ERROR RadSec - tlsservernew: SSL: error:04091068:rsa routines:int_rsa_verify:bad signature</p> <p>2023-02-25T16:03:28.244100-05:00 192.168.144.3 2023-02-25 16: 03:28,244 [192.168.144.36-12] ERROR RadSec - tlsservernew: SSL: error:1417A0C1:SSL routines:tls_post_process_client_hello:no shared cipher</p> <p>2023-02-27T10:28:56.679413-05:00 192.168.144.3 2023-02-27 10: 28:56,678 [192.168.144.36-6] ERROR RadSec - tlsservernew: SSL: error:1408F119:SSL routines:ssl3_get_record:decryption failed or bad record mac</p> <p>2023-02-27T10:36:27.115147-05:00 192.168.144.3 2023-02-27 10: 36:27,611 [192.168.144.36-12] ERROR RadSec - tlsservernew: SSL: error:142090FC:SSL routines:tls_early_post_process_client_hello:unknown protocol</p>
--

NDcPP22e: FCS_RBG_EXT.1	Auditable Events	None	Additional Content	None
----------------------------	------------------	------	--------------------	------

NDcPP22e: FCS_SSHS_EXT.1	
Auditable Events	Failure to establish an SSH session. Successful SSH rekey.
Additional Content	Reason for failure. Non-TOE endpoint of connection (IP Address).
Audit Observed In	Monitoring > Event Viewer
Audit Event Details	<p>Source: Command Line</p> <p>Level: Info</p> <p>Category: Logged In</p> <p>Action: None</p> <p>Timestamp: <i>[time]</i></p> <p>Description: user: appadmin</p> <p>Group: Local Administrator</p> <p>Client IP address: <i>[IP]</i></p>
syslog example(s)	<p>2023-02-28T10:24:36.270354-05:00 clearpass sshd 1222640 - - Unable to negotiate with 192.168.144.36 port 47762: no matching host key type found. Their offer: ecdsa-sha2-nistp521 [preauth]</p> <p>2023-02-28T10:37:33.011769-05:00 clearpass sshd 1298205 - - Unable to negotiate with 192.168.144.36 port 50096: no matching key exchange method found. Their offer: diffie-hellman-group1-sha1,ext-info-c [preauth]</p> <p>2023-02-28T10:31:05.732120-05:00 clearpass sshd 1259512 - - Unable to negotiate with 192.168.144.36 port 49112: no matching MAC found. Their offer: hmac-md5 [preauth]</p> <p>2023-02-28T10:14:37.909482-05:00 clearpass sshd 1163780 - - Failed publickey for admin from</p>

	192.168.144.36 port 45832 ssh2: RSA SHA256:dGNsTSE74Xej7yTnPOOInvjtVppeB/6l/NCrGBGDyY 2023-02-28T10:15:46.172091-05:00 clearpass sshd 1169808 - - Failed password for admin from 192.168.144.36 port 45958 ssh2
--	--

NDcPP22e: FCS_TLSS_EXT.2	
Auditable Events	Failure to establish a TLS Session.
Additional Content	Reason for failure.
Audit Observed In	Monitoring > Event Viewer
Audit Event Details	Source: Admin UI Level: ERROR Category: Login Failed Action: None Timestamp: <i>[time]</i> Description: error:[error] [information] [possible reason] Client IP address: [IP]
	[example audit] Source: Admin UI Level: ERROR Category: Login Failed Action: None Timestamp: <i>[time]</i> Description: error:1408A0C1:SSL routines:ssl3_get_client_hello:no shared cipher -- Too restrictive SSLCipherSuite or using DSA server certificate? Client IP address: <i>[IP]</i>
	[example audit] Source: Admin UI Level: ERROR Category: Login Failed Action: None Timestamp: <i>[time]</i> Description: error:1408A10B:SSL routines:ssl3_get_client_hello:wrong version number Client IP address: <i>[IP]</i>
syslog example(s)	2023-02-27 12:23:44.371151-05:00 192.168.144.3 2023-02-27 12:23:44.371 [ssl:warn] [pid 1341221] [client 192.168.144.36:55959] SSL Library Error: error:14094416:SSL routines:ssl3_read_bytes:ssl3 alert certificate unknown (SSL alert number 46) 2023-02-27 12:15:12.181775-05:00 192.168.144.3 2023-02-27 12:15:12.181 [ssl:error] [pid 1196757] [client 192.168.144.36:48046] AH02039: Certificate Verification: Error (68): CA signature digest

	<p>algorithm too weak</p> <p>2023-02-27 12:23:41.854845-05:00 192.168.144.3 2023-02-27 12:23:41.854 [ssl:error] [pid 1303623] SSL Library Error: error:1417B07B:SSL routines:tls_process_cert_verify:bad signature</p> <p>2023-02-27 12:48:03.350247-05:00 192.168.144.3 2023-02-27 12:48:03.350 [ssl:error] [pid 1453625] [client 192.168.144.36:48362] AH02039: Certificate Verification: Error (26): unsupported certificate purpose</p> <p>2023-02-27T15:30:35.167639-05:00 192.168.144.3 2023-02-27 15: 30:35,167 [R:W00000013-01-63fd12eb] ERROR com.avenda.tips.dataaccess.db.DbAuthenSession - User 'client-no-eku-ecdsa' not present in [Local User Repository](localhost)</p>
--	---

AUTHSVREP10: FIA_AFL.1	
Auditable Events	<p>The reaching of the threshold for the unsuccessful authentication attempts.</p> <p>Disabling an account due to the threshold being reached</p>
Additional Content	The claimed identity of the user attempting to gain access or the IP where the attempts originated.
Audit Observed In	Configuration > Access Tracker
Audit Event Details	<p>Error Code: 225</p> <p>Error Category: Authentication failure</p> <p>Error Message: User account disabled</p> <p>Alerts for this Request</p> <p>[AUTHENTICATOR]</p> <p>[auth-type]: [information]</p> <p>AUTHORIZATION: <i>[reason]</i></p> <hr/> <p>(example audit)</p> <p>Error Code: 225</p> <p>Error Category: Authentication failure</p> <p>Error Message: User account disabled</p> <p>Alerts for this Request</p> <p>RADIUS</p> <p>MAC-AUTH: Password in request doesn't match username. Not attempting MAC authentication.</p> <p>Cannot select appropriate authentication method</p> <p>AUTHORIZATION: User account expired/disabled</p>
Audit Observed In	Configuration > Audit Viewer
Audit Event Details	<p>Old Data tab</p> <p>Local User Details:</p> <p>Enabled User: Enabled</p>

	<p>New Data tab</p> <p>Local User Details:</p> <p>Enabled User: Disabled</p> <p>Attributes: DisabledBy = TIPS</p> <p>DisabledReason = Account-Settings:Attempts-Exceeded</p>
	<p>Inline Difference tab</p> <p>Local User Details:</p> <p>Enabled User: Enabled Disabled</p> <p>Attributes: DisabledBy = TIPS</p> <p>DisabledReason = Account-Settings:Attempts-Exceeded</p>
syslog example(s)	<p>Web UI</p> <p>2023-02-16T08:51:36.792-05:00 arubacp-phys [] [R:] DEBUG com.avenda.tips.syslog.Syslogger - 2023-02-16 08:51:36,792 192.168.144.3 System Events 330 1 0 Timestamp=Feb 16 2023 08:51:19.325 EST,Component=User Account Settings,Level=INFO,Category=Admin User Disable,Action=None,Description=User IDs disabled by Account-Settings:Attempts-Exceeded for configured threshold of 3 - testuser</p> <p>SSH</p> <p>2023-02-16T11:39:09.478035-05:00 2023-02-16 11: 39:09,477 192.168.144.3 System Events 383 1 0 Timestamp=Feb 16 2023 11:38:38.905 EST,Component=Command Line,Level=ERROR,Category=Account Locked,Action=Failure,Description=Failed SSH login attempts 3 exceeded the configured threshold of 2. SSH access via appadmin account locked for 180 secs.\nUser: appadmin</p>

NDcPP22e: FIA_PMG_EXT.1	Auditable Events	None	Additional Content	None
----------------------------	------------------	------	--------------------	------

AUTHSVR10: FIA_PSK_EXT.1	Auditable Events	None	Additional Content	None
-----------------------------	------------------	------	--------------------	------

NDcPP22e: FIA_UAU.7	Auditable Events	None	Additional Content	None
---------------------	------------------	------	--------------------	------

NDcPP22e: FIA_UIA_EXT.1 & NDcPP22e:FIA_UAU_EXT.2	
Auditable Events	All use of identification and authentication mechanism.
Additional Content	Origin of the attempt (e.g., IP address).

Audit Observed In	Monitoring > Event Viewer
Audit Event Details	<p>Source: Command Line</p> <p>Level: Info</p> <p>Category: Logged In</p> <p>Action: None</p> <p>Timestamp: <i>[time]</i></p> <p>Description: user: appadmin</p> <p>Group: Local Administrator</p> <p>Client IP address: <i>[IP]</i></p>
	<p>Source: Command Line</p> <p>Level: WARN</p> <p>Category: Login Failed</p> <p>Action: Failure</p> <p>Timestamp: <i>[time]</i></p> <p>Description: Failed SSH <i>[authentication method]</i> login attempt using appadmin account. Last login attempt from the remote host <i>[IP]</i></p>
	<p>Source: Admin UI</p> <p>Level: INFO</p> <p>Category: Logged In</p> <p>Action: None</p> <p>Timestamp: <i>[time]</i></p> <p>Description: user: <i>[username]</i></p> <p>Role: <i>[role]</i></p> <p>Authentication Source: <i>[auth source]</i></p> <p>Session ID: <i>[ID]</i></p> <p>Client IP Address: <i>[IP]</i></p> <p>Session Inactive Expiry Time: <i>[timeout]</i></p>
	<p>Source: Admin UI</p> <p>Level: WARN</p> <p>Category: Login Failed</p> <p>Action: None</p> <p>Timestamp: <i>[time]</i></p> <p>Description: user: <i>[username]</i></p>

	Client IP Address: <i>[IP]</i>
Audit Observed In	Monitoring > Live Monitoring > Access Tracker
Audit Event Details	<p>Error Code: 211</p> <p>Error Category: Authentication Failure</p> <p>Error Message: <i>[reason]</i> (example: Client certificate not valid)</p> <p>Alerts for this Request</p> <p>WebAuthService</p> <p>User [username] not present in [authentication source]</p> <p>Failed to update certificate auth status</p> <p>Client certificate not valid</p>
syslog example(s)	<p>CLI Password Login Success and Failure</p> <p>2023-02-20T11:06:36.918024-05:00 clearpass sudo 1329255 - - pam_unix(sudo:session): session opened for user appadmin by (uid=0)</p> <p>2023-03-01T16:09:20.083090-05:00 clearpass login 3382986 - - FAILED LOGIN 1 FROM ttyS0 FOR appadmin, Authentication failure</p> <p>SSH Public Key Login - Success and Failure</p> <p>2023-02-28T12:16:27.987878-05:00 clearpass sshd 1879889 - - Accepted publickey for appadmin from 192.168.144.36 port 50602 ssh2: RSA SHA256:7XdswzGhnYzQgMQ3syAGixppdLNwicOKf1vfwEMQjdE</p> <p>2023-02-28T10:14:37.909482-05:00 clearpass sshd 1163780 - - Failed publickey for admin from 192.168.144.36 port 45832 ssh2: RSA SHA256:dGNsTSE74XeJ7yTnPOOInvjtVppeB/6l/NCrGBGDyY</p> <p>SSH Password Login – Success and Failure</p> <p>2023-02-28T10:37:14.840466-05:00 clearpass sshd 1295943 - - Accepted password for admin from 192.168.144.36 port 50014 ssh2</p> <p>2023-02-28T10:15:46.172091-05:00 clearpass sshd 1169808 - - Failed password for admin from 192.168.144.36 port 45958 ssh2</p> <p>Web UI Password Auth Success and Failure</p> <p>2023-02-23T07:46:43.554-05:00 arubacp-phys [] [R:]</p> <p>DEBUG com.avenda.tips.syslog.Syslogger - 1 2023-02-23T07:46:43.553-05:00 192.168.144.3 ClearPass 59610 155-1-0 [timeQuality tzKnown="1"] [origin swVersion="6.11.1.251216" software="PolicyManager" ip="192.168.144.3" enterpriseId="1.3.6.1.4.1.14823"] [clearPass@14823 eventId="3002" Action="None" Category="Logged in" Description="User: admin\\nRole: Super Administrator\\nAuthentication Source: Policy Manager Network Login (TACACS+)\\nSession ID: 0267e5f190b0c3b34d48b5f91fb371a6\\nClient IP Address: 192.168.144.5\\nSession Inactive Expiry Time: 360 mins" Level="INFO" Component="Policy Manager UI" CppmNode.CPPM-</p>

	<p>Node="192.168.144.3" Timestamp="2023-02-23T07:46:12.543-05:00"]</p> <p>2023-02-24T13:05:43.765-05:00 arubacp-phys [] [R:]</p> <p>DEBUG com.avenda.tips.syslog.Syslogger - 1 2023-02-24T13:05:43.765-05:00 192.168.144.3 ClearPass 59610 360-1-0 [timeQuality tzKnown="1"][origin swVersion="6.11.1.251216" software="PolicyManager" ip="192.168.144.3" enterpriseId="1.3.6.1.4.1.14823"][clearPass@14823 eventId="3002" Action="None" Category="Login Failed" Description="User: admin\\nClient IP Address: 192.168.144.5" Level="WARN" Component="Policy Manager UI" CppmNode.CPPM-Node="192.168.144.3" Timestamp="2023-02-24T13:05:27.262-05:00"]</p> <p>Web UI Cert Auth Success</p> <p>2023-02-28T17:38:09.803-05:00 192.168.144.3 [] DEBUG dashboard.DashboardOperations - getRadiusSession Details returning bean =W00000025-01-63fe8170 superadmin - - 2023-02-28 17:34:26.454 TLS-SSO ClearPass Certificate SSO Login Not applicable null 2023-02-28 17:34:26.454 [User Authenticated] UNKNOWN (100) UNKNOWN (100) new ClearPass Certificate SSO Login Profile1, TLS-SSO ClearPass Certificate SSO Login Profile1 2023-02-28 17:34:26.43 null null null null [Application:Name=GuestOperators, Application:SSO:AuthRequestId=W00000026-01-63fe8171, Application:...<143>...SSO:Cert-Subject-CN=superadmin, Authentication:Full-Username=superadmin, Authentication:Full-Username-Normalized=superadmin, Authentication:Status=User, Authentication:Type=SSO, Authentication:Username=superadmin, Authorization:Sources=[Local User Repository], Connection:Protocol=Application, Connection:Src-IP-Address=192.168.144.5, Date:Date-of-Year=2023-02-28, Date:Date-Time=2023-02-28 17:34:26, Date:Day-of-Week=Tuesday, Date:Time-of-Day=17:34:26] null null null [Application:SSORole=Super Administrator] null 0 Success Success ACCEPT Disabled</p> <p>Failure</p> <p>See NDcPP22e:FCS_TLSS_EXT.2.</p>
--	---

NDcPP22e: FIA_X509_EXT.1/Rev	
Auditable Events	Unsuccessful attempt to validate a certificate.
Additional Content	Reason for failure.
Audit Observed In	Monitoring > Live Monitoring > Access Tracker
Audit Event Details	Error Code: 211 Error Category: Authentication Failure

	<p>Error Message: Client certificate not valid</p> <p>Alerts for this Request</p> <p>WebAuthService</p> <p>Client certificate not valid</p>
Audit Observed In	Monitoring > Event Viewer
Audit Event Details	<p>Source: ClearPass IPsec Tunnel</p> <p>Level: ERROR</p> <p>Category: Tunnel Action</p> <p>Action: [empty]</p> <p>Timestamp: <i>[time]</i></p> <p>Description: Tunnel (Remote IP : <i>[IP]</i>): ocsrp request to <i>[OCSP server]</i> failed</p>
syslog example(s)	<p>IPsec</p> <p>2023-02-27T21:32:54-05:00 192.168.144.3 cppm.ipsec[20011]: Feb 27 21:32:54 07[CFG] <ipsec-3028 74> subject certificate invalid (valid from Jan 23 15:55:57 2023 to Jan 23 16:00:00 2023)</p> <p>2023-02-27T21:35:37-05:00 192.168.144.3 cppm.ipsec[20011]: Feb 27 21:35:37 15[CFG] <ipsec-3028 75> certificate was revoked on Jan 23 20:56:42 UTC 2023, reason: unspecified</p> <p>2023-02-27T21:40:08-05:00 192.168.144.3 cppm.ipsec[20011]: Feb 27 21:40:08 13[CFG] <ipsec-3028 76> ocsrp response verification failed, no signer certificate 'C=US, ST=MD, L=Catonsville, O=GSS, CN=tl39-16x.example.com' found</p> <p>2023-02-27T21:44:03-05:00 192.168.144.3 cppm.ipsec[20011]: Feb 27 21:44:03 10[LIB] <77> OpenSSL X.509 parsing failed</p> <p>2023-02-27T21:48:00-05:00 192.168.144.4 cppm.ipsec[20011]: Feb 27 21:48:00 09[CFG] <ipsec-3028 78> no issuer certificate found for "C=US, ST=MD, L=Catonsville, O=GSS, CN=tl39-16x.example.com"</p> <p>2023-02-27T21:54:12-05:00 192.168.144.4 cppm.ipsec[20011]: Feb 27 21:54:12 11[CFG] <ipsec-3028 79> ocsrp request to http://192.168.144.34:7826 failed</p> <p>TLS/HTTPS</p> <p>2023-03-01 11:12:26.612838-05:00 192.168.144.3 11:12:26.612 [ssl:error] [pid 1919639] [client 192.168.144.36:45660] AH02039: Certificate Verification: Error (24): invalid CA certificate</p> <p>2023-03-01 11:12:06.466319-05:00 192.168.144.3 11:12:06.466 [ssl:error] [pid 1919643] [client 192.168.144.36:45532] AH02039: Certificate Verification: Error (66): EE certificate key too weak</p> <p>2023-03-01 11:12:00.078063-05:00 192.168.144.3 11:12:00.078 [ssl:error] [pid 1983483] [client 192.168.144.36:45468] AH02039: Certificate Verification: Error (7): certificate signature failure</p> <p>2023-03-01 11:11:34.768132-05:00 192.168.144.3 11:11:34.768 [ssl:error] [pid 1919638] [client 192.168.144.36:45320] AH02039: Certificate Verification: Error (10): certificate has expired</p> <p>2023-03-02T12:40:08.220948-05:00 192.168.144.3 2023-03-02 12: 40:08,262 [R:W00000002-01-6400df76] ERROR com.avenda.tips.webauthservice.WebAuthHandler - Client certificate OCSP</p>

	<p>verification failed</p> <p>Addition and Removal of trust anchors</p> <p>2023-03-02T11:08:24-05:00 192.168.144.3 cppm.apache[336580]: 192.168.144.5 - - [02/Mar/2023:11:08:21 -0500] "POST /tips/tipsUploadImport.action HTTP/1.1" 200 87 "https://192.168.144.3/tips/tipsContent.action" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/110.0.0.0 Safari/537.36" TLSv1.2 ECDHE-ECDSA-AES256-GCM-SHA384 3275781µs</p> <p>2023-03-02T11:07:50-05:00 192.168.144.3 cppm.apache[336580]: 192.168.144.5 - - [02/Mar/2023:11:07:50 -0500] "POST /tips/dwr/call/plaincall/certTrustList.deleteCertsFromCTL.dwr HTTP/1.1" 200 255 "https://192.168.144.3/tips/tipsContent.action" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/110.0.0.0 Safari/537.36" TLSv1.2 ECDHE-ECDSA-AES256-GCM-SHA384 92071µs</p>
--	---

NDcPP22e: FIA_X509_EXT.2	Auditable Events	None	Additional Content	None
-----------------------------	------------------	------	--------------------	------

NDcPP22e: FIA_X509_EXT.3	Auditable Events	None	Additional Content	None
-----------------------------	------------------	------	--------------------	------

NDcPP22e: FMT_MOF.1/AutoUpdate	Auditable Events	None	Additional Content	None
-----------------------------------	------------------	------	--------------------	------

NDcPP22e: FMT_MOF.1/Functions	Auditable Events	None	Additional Content	None
----------------------------------	------------------	------	--------------------	------

NDcPP22e: FMT_MOF.1/ManualUpdate	
Auditable Events	Any attempt to initiate a manual update.
Additional Content	None
Audit Observed In	Monitoring > Event Viewer

Audit Event Details	<p>Source: Admin UI</p> <p>Level: ERROR</p> <p>Category: File Upload Failed</p> <p>Action: None</p> <p>Timestamp: <i>[time]</i></p> <p>Description: User:<i>[username]</i></p> <p>Client IP Address: <i>[IP]</i></p> <p>Error: <i>[reason]</i></p>
	<p>Source: Install Update</p> <p>Level: INFO</p> <p>Category: Installed Update</p> <p>Action: Success</p> <p>Timestamp: <i>[time]</i></p> <p>Description: User:<i>[username]</i> Client IP Address: <i>[IP]</i> System update using image file <i>[patch name]</i></p>
	<p>Source: Install Update</p> <p>Level: INFO</p> <p>Category: Installed Update</p> <p>Action: Success</p> <p>Timestamp: <i>[time]</i></p> <p>Description: User:<i>[username]</i></p> <p>Client IP Address: <i>[IP]</i></p> <p>File: <i>[patch name]</i></p>
	<p>[example audit]</p> <p>Source: Admin UI</p> <p>Level: ERROR</p> <p>Category: File Upload Failed</p> <p>Action: None</p> <p>Timestamp: <i>[time]</i></p> <p>Description: User:<i>[username]</i></p> <p>Client IP Address: <i>[IP]</i></p> <p>Error: Uploaded file is invalid: does not have the meta file or unrecognized type or does not have a valid signature.</p>
syslog example(s)	See NDcPP22e:FPT_TUD_EXT.1

NDcPP22e: FMT_MOF.1/Services	Auditable Events	None	Additional Content	None
---------------------------------	------------------	------	--------------------	------

NDcPP22e: FMT_MTD.1/CoreData	Auditable Events	None	Additional Content	None
---------------------------------	------------------	------	--------------------	------

NDcPP22e: FMT_MTD.1/CryptoKeys	Auditable Events	None	Additional Content	None
-----------------------------------	------------------	------	--------------------	------

FMT_SMF.1	
Auditable Events	All management activities of TSF data.
Additional Content	None
Audit Observed In	Configuration > Audit Viewer
Audit Event Details	[event information unique to addition/deletion/modification made]
syslog example(s)	<p>Ability to administer the TOE locally and remotely Refer to NDcPP22E:FIA_UAU_EXT.2</p> <p>Ability to configure the access banner 2023-03-01T10:47:47.494673-05:00 192.168.144.3 2023-03-01 10: 47:47,494 [DbcnHandlerThread-0x7fd3352a7700] INFO Common.ClusterwideParamsTable - updateFromDb: Param=LoginBannerText, Value=Login banner: Welcome to Gossamersec Baltimore, MD 1</p> <p>Ability to configure the session inactivity time before session termination or locking 2023-03-01T10:49:33.369097-05:00 192.168.144.3 2023-03-01 10: 49:33,368 [DbcnHandlerThread-0x7fd3352a7700] INFO Common.ClusterwideParamsTable - updateFromDb: Param=AdminSessionIdleTimeout, Value=30</p> <p>Ability to update the TOE, and to verify the updates using [digital signature] capability prior to installing those updates Refer to NDcPP22E:FPT_TUD_EXT.1</p> <p>Ability to configure the authentication failure parameters for FIA_AFL.1 2023-02-16T08:55:50-05:00 192.168.144.3 cppm.apache[44451]: 192.168.144.5 - - [16/Feb/2023:08:55:50 -0500] "POST /tips/dwr/call/plaincall/adminUsers.savePasswordPolicy.dwr HTTP/1.1" 200 270 "https://clearpass.example.com/tips/tipsContent.action" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/110.0.0.0 Safari/537.36"</p>

	<p>TLSv1.2 ECDHE-ECDSA-AES256-GCM-SHA384 50379µs</p> <p>2023-03-02T12:49:03.856681-05:00 clearpass sudo 3171641 - - appadmin : TTY=pts/0 ; PWD=/home/appadmin ; USER=root ; COMMAND=/usr/local/avenda/tips/bin/do-sshops.sh lockout count 3</p> <p>Ability to configure audit behavior</p> <p>2023-02-10T11:14:06.748-05:00 192.168.145.3 [] [R:] INFO com.avenda.tips.syslogclient.syslogtasks.SyslogTaskConfig - Initializing the SyslogTaskConfig with Id=3003 Name=Session Logs</p> <p>Ability to modify the behavior of the transmission of audit data to an external IT entity, the handling of audit data, the audit functionality when Local Audit Storage Space is full</p> <p>2023-03-02T13:04:45.137513-05:00 192.168.144.3 2023-03-02 13: 04:45,291 [DbcnHandlerThread-0x7fd3352a7700] INFO Common.ClusterwideParamsTable - updateFromDb: Param=AuditRecordsCleanupInterval, Value=7</p> <p>Ability to manage the cryptographic keys</p> <p>2023-02-27T11:54:29-05:00 192.168.144.3 cppm.apache[336580]: 192.168.144.5 - - [27/Feb/2023:11:54:28 -0500] "POST /tips/tipsServerCertUploadPKCS12Cert.action HTTP/1.1" 200 87 "https://192.168.144.3/tips/tipsContent.action" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/110.0.0.0 Safari/537.36" TLSv1.2 ECDHE-ECDSA-AES256-GCM-SHA384 1307170µs</p> <p>Ability to configure the lifetime for IPsec SAs & Ability to configure the IPsec functionality</p> <p>2023-02-24T18:19:51-05:00 192.168.144.3 cppm.ipsec[336580]: 2023-02-24 18:19:51,456 INFO Platform.IPsec UpdateIPsecConfig Generating IPsec configuration file connId 3076</p> <p>Ability to enable or disable automatic checking for updates or automatic updates;</p> <p>2023-03-01T12:04:21.016818-05:00 192.168.144.3 2023-03-01 12: 04:21,016 [DbcnHandlerThread-0x7fd3352a7700] INFO Common.ClusterwideParamsTable - updateFromDb: Param=SoftwareAutoUpdatesFlag, Value=FALSE</p> <p>Ability to re-enable an Administrator account</p> <p>2023-02-16T08:45:21-05:00 192.168.144.3 cppm.apache[44451]: 192.168.144.5 - - [16/Feb/2023:08:45:21 -0500] "POST /tips/dwr/call/plaincall/adminUsers.resetFailedAttemptsCount.dwr HTTP/1.1" 200 271 "https://clearpass.example.com/tips/tipsContent.action" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/110.0.0.0 Safari/537.36" TLSv1.2 ECDHE-ECDSA-</p>
--	---

	<p>AES256-GCM-SHA384 12730µs</p> <p>2023-03-02T12:49:11.690200-05:00 clearpass sudo 3175223 -- appadmin : TTY=pts/0 ; PWD=/home/appadmin ; USER=root ; COMMAND=/usr/local/avenda/tips/bin/do-sshops.sh unlock appadmin</p> <p>Ability to set the time which is used for time-stamps</p> <p>Refer to NDCPP22E:FPT_STM_EXT.1</p> <p>Ability to configure NTP</p> <p>Refer to NDCPP22E:FCS_NTP_EXT.1</p> <p>Ability to manage the TOE's trust store and designate X509.v3 certificates as trust anchors, & Ability to import X509v3 certificates to the TOE's trust store</p> <p>Refer to NDCPP22e:FIA_X509_EXT.1/Rev</p> <p>Ability to manage the trusted public keys database</p> <p>2023-02-28T12:16:11-05:00 192.168.144.3 cppm.apache[336580]: 192.168.144.5 -- [28/Feb/2023:12:16:11 -0500] "POST /tips/dwr/call/plaincall/serverConfigDetails.addSSHPublicKey.dwr HTTP/1.1" 200 256 "https://192.168.144.3/tips/tipsContent.action" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/110.0.0.0 Safari/537.36" TLSv1.2 ECDHE-ECDSA-AES256-GCM-SHA384 251629µs</p> <p>Ability to configure the RADIUS shared secret & Ability to define an authorized NAS</p> <p>2023-02-21T12:11:45.253682-05:00 192.168.144.3 2023-02-21 12: 11:45,253 [DbcnHandlerThread-0x7fbb2527b700] DEBUG DB.NadClientDAO - createNadClient: Id=3001 name=tl39-16x IpAddress=192.168.144.36 CoACapable=0 Attributes=null#012</p> <p>2023-02-21T12:11:45.255223-05:00 2023-02-21 12: 11:45,254 [DbcnHandlerThread-0x7fbb2527b700] INFO Common.TagDefinitionCacheTable - handleDbcn: Processing DBCN event: DbcnInfo::<id=10291, entity=NAD_CLIENT, entityId=3001, event=UPDATE></p> <p>Resetting passwords (name of related user account shall be logged).</p> <p>2023-03-02T21:29:24.486-05:00 arubacp-phys [] DEBUG adminUser.AdminUserOperations - adminBean:{dept:{ },title:{ },groupName:{ },extras:{ },passwordUpdatedAt:{ },extrasJsonB:{{ },name:{aruba-test },attributes:{ },enabled:{true },groupId:{1 },userName:{Aruba Test },userId:{aruba-test },id:{-1, }}</p>
--	--

NDcPP22e: FMT_SMF.1(1)	Auditable Events	None	Additional Content	None
---------------------------	------------------	------	--------------------	------

NDcPP22e: FMT_SMR.2	Auditable Events	None	Additional Content	None
---------------------	------------------	------	--------------------	------

NDcPP22e: FPT_APW_EXT.1	Auditable Events	None	Additional Content	None
----------------------------	------------------	------	--------------------	------

NDcPP22e: FPT_SKP_EXT.1	Auditable Events	None	Additional Content	None
----------------------------	------------------	------	--------------------	------

NDcPP22e: FPT_STM_EXT.1	
Auditable Events	Discontinuous changes to time - either Administrator actuated or changed via an automated process. (Note that no continuous changes to time need to be logged. See also application note on FPT_STM_EXT.1)
Additional Content	For discontinuous changes to time: The old and new values for the time. Origin of the attempt to change time for success and failure (e.g., IP address).
Audit Observed In	Monitoring > Event Viewer
Audit Event Details	<p>Source: datetime</p> <p>Level: INFO</p> <p>Category: configuration</p> <p>Action: Success</p> <p>Timestamp: <i>[time]</i></p> <p>Description: Successfully changed system datetime. Old time was <i>[previous time]</i></p>
syslog example(s)	<p>2022-11-01T09:19:12.823936-05:00 2022-11-01T09:19:12,823 192.168.144.3 Audit Records 5254 1 0 Timestamp=Nov 11 2022 09:19:12,823 EST,Component=Admin UI,Level=INFO,Category=Set Date and Time,Action=None,Description=User: admin\nRole: Super Administrator</p> <p>2022-11-01T09:24:59.941343-04:00 2022-11-01 09: 24:59,878 192.168.144.3 Audit Records 0 1 0 Timestamp=Nov 01 2022 09:20:50.965 EDT,Component=Time Config,Level=INFO,Category=Remote Time server,Action=None,Description=Old List: 192.168.144.36\nNew List: 192.168.144.36</p> <p>2022-11-01T09:24:59.946016-04:00 2022-11-01 09: 24:59,940 192.168.144.3 Audit Records 1 1 0 Timestamp=Nov 01 2022 09:20:52.520 EDT,Component=datetime,Level=INFO,Category=configuration,Action=Success,Description=Successfully changed system datetime.\nOld time was Nov 1, 2022 09:20:44 AM EDT.</p>

NDcPP22e: FPT_TST_EXT.1	Auditable Events	None	Additional Content	None
----------------------------	------------------	------	--------------------	------

NDcPP22e: FPT_TUD_EXT.1	
Auditable Events	Initiation of update; result of the update attempt (success or failure).
Additional Content	None
Audit Observed In	Monitoring > Event Viewer
Audit Event Details	<p>Source: Update</p> <p>Level: INFO</p> <p>Category: Update status</p> <p>Action: None</p> <p>Timestamp: <i>[time]</i></p> <p>Description: User:<i>[username]</i> Client IP Address: <i>[IP]</i> System update using image file <i>[patchname]</i>.</p>
	<p>Source: Update</p> <p>Level: INFO</p> <p>Category: Update status</p> <p>Action: None</p> <p>Timestamp: <i>[time]</i></p> <p>Description: User:<i>[username]</i> Client IP Address: <i>[IP]</i> Completed update using image file=<i>[patchname]</i>. Will continue after reboot</p>
syslog example(s)	<p>Successful Update</p> <p>2023-02-22T11:11:18.928-05:00 arubacp-phys [] [R:] DEBUG com.avenda.tips.syslog.Syslogger - 1 2023-02-22T11:11:18.928-05:00 192.168.144.3 ClearPass 55408 141-1-0 [timeQuality tzKnown="1"][origin swVersion="6.11.1.251216" software="PolicyManager" ip="192.168.144.3" enterpriseld="1.3.6.1.4.1.14823"][clearPass@14823 eventId="3002" Action="None" Category="Update Status" Description="User:admin Client IP Address:192.168.144.5 Completed update using image file=CPPM-x86_64-20230201-cc-hotfix-aruba-611-patch.bin." Level="INFO" Component="Update" CppmNode.CPPM-Node="192.168.144.3" Timestamp="2023-02- 22T11:11:07.158-05:00"]</p> <p>Update Failure</p> <p>2023-02-18T15:11:03.256342-05:00 2023-02-18 15: 11:03,329 192.168.144.3 System Events 701 1 0 Timestamp=Feb 18 2023 15:10:55.485 EST,Component=Admin UI,Level=ERROR,Category=Import,Action=Failed,Description=User: admin\nRole: Super Administrator\nEntity: serverConfigUpload\nClient IP Address: 192.168.144.5\nUser admin tried to import serverConfigUpload Details\nReason for Failure: Uploaded file is invalid: does not have the meta file or unrecognized type or does not have a valid signature.</p>

NDcPP22e: FTA_SSL.3

Auditable Events	The termination of a remote session by the session locking mechanism.
Additional Content	None
Audit Observed In	Monitoring > Event Viewer
Audit Event Details	<p>Source: Admin UI</p> <p>Level: INFO</p> <p>Category: Session destroyed</p> <p>Action: None</p> <p>Timestamp: <i>[time]</i></p> <p>Description: Session ID: <i>[ID]</i></p> <p>Client IP Address: <i>[IP]</i></p> <p>Session Inactive Expiry Time: <i>[timeout]</i></p>
	<p>Source: Command Line</p> <p>Level: WARN</p> <p>Category: Session Inactivity</p> <p>Action: None</p> <p>Timestamp: <i>[time]</i></p> <p>Description: Disconnecting SSH session due to session inactivity. Client IP Address: <i>[IP]</i></p>
syslog example(s)	<p>SSH</p> <p>2023-02-18T21:11:09.533560-05:00 2023-02-18 21: 11:09,532 192.168.144.3 System Events 725 1 0 Timestamp=Feb 18 2023 21:11:01.499 EST,Component=Command Line,Level=WARN,Category=Session Inactivity,Action=None,Description=Disconnecting SSH session due to session inactivity. Client IP Address : 192.168.144.36</p> <p>Web UI</p> <p>2023-02-13T20:59:31.527-05:00 192.168.145.3 [] [R:] DEBUG com.avenda.tips.syslog.Syslogger - 1 2023-02-13T20:59:31.527-05:00 192.168.144.3 ClearPass 51984 530-1-0 [timeQuality tzKnown="1"][origin swVersion="6.11.1.251216" software="PolicyManager" ip="192.168.144.3" enterpriseld="1.3.6.1.4.1.14823"][clearPass@14823 eventId="3002" Action="None" Category="Logged in" Description="User: admin\\nRole: Super Administrator\\nAuthentication Source: Policy Manager Network Login (TACACS+)\\nSession ID: dab5a369d73adfaf8416bba5779e45ce\\nClient IP Address: 192.168.144.5\\nSession Inactive Expiry Time: 360 mins" Level="INFO" Component="Policy Manager UI" CppmNode.CPPM- Node="192.168.144.3" Timestamp="2023-02-13T20:59:27.670-05:00"]</p>

NDcPP22e: FTA_SSL.4	
Auditable Events	The termination of an interactive session.
Additional Content	None
Audit Observed In	Monitoring > Event Viewer

Audit Event Details	<p>Source: Admin UI</p> <p>Level: INFO</p> <p>Category: Logged out</p> <p>Action: None</p> <p>Timestamp: <i>[time]</i></p> <p>Description: User: <i>[username]</i></p> <p>Role: <i>[role]</i></p> <p>Session ID: <i>[ID]</i></p> <p>Client IP Address: <i>[IP]</i></p> <hr/> <p>Source: Command Line</p> <p>Level: INFO</p> <p>Category: Logged out</p> <p>Action: None</p> <p>Timestamp: <i>[time]</i></p> <p>Description: User: appadmin</p> <p>Client IP Address: <i>[IP]</i></p>
syslog example(s)	<p>Console Logout</p> <p>2023-02-21T14:43:54.398-05:00 arubacp-phys [] [R:] DEBUG com.avenda.tips.syslog.Syslogger - 2023-02-21 14:43:54,398 192.168.144.3 System Events 9 1 0 Timestamp=Feb 21 2023 14:38:20.343 EST,Component=Command Line,Level=INFO,Category=Logged out,Action=None,Description=User: appadmin\nClient IP Address:</p> <p>SSH Logout</p> <p>2023-02-16T13:34:11.663364-05:00 2023-02-16 13: 34:11,616 192.168.144.3 System Events 402 1 0 Timestamp=Feb 16 2023 13:33:40.586 EST,Component=Command Line,Level=INFO,Category=Logged out,Action=None,Description=User: appadmin\nClient IP Address: 192.168.144.36</p> <p>Web UI Logout</p> <p>2023-02-16T08:47:36.642600-05:00 2023-02-16 08: 47:36,657 192.168.144.3 System Events 314 1 0 Timestamp=Feb 16 2023 08:47:08.444 EST,Component=Policy Manager UI,Level=INFO,Category=Logged out,Action=None,Description=User: admin\nRole: Super Administrator\nSession ID: 0620788171e718cecc104fc0a078f431\nClient IP Address: 192.168.144.5</p>

NDcPP22e: FTA_SSL_EXT.1	
Auditable Events	(if 'lock the session' is selected) Any attempts at unlocking of an interactive session. (if 'terminate the session' is selected) The termination of a local session by the session locking mechanism.
Additional Content	None

Audit Observed In	Monitoring > Event Viewer
Audit Event Details	<p>Source: User Account Settings</p> <p>Level: INFO</p> <p>Category: Local User Disable</p> <p>Action: None</p> <p>Timestamp: <i>[time]</i></p> <p>Description: User IDs disabled by Account-Settings:Attempts-Exceeded for configured threshold of <i>[threshold]</i> – <i>[username]</i></p>
Audit Observed In	Configuration > Audit Viewer
Audit Event Details	<p>Old Data tab</p> <p>Local User Details:</p> <p>Enabled User: Enabled</p>
	<p>New Data tab</p> <p>Local User Details:</p> <p>Enabled User: Disabled</p> <p>Attributes: DisabledBy = TIPS</p> <p>DisabledReason = Account-Settings:Attempts-Exceeded</p> <p>DisabledBy = TIPS</p>
	<p>Inline Difference tab</p> <p>Local User Details:</p> <p>Enabled User: Enabled Disabled</p> <p>Attributes: DisabledBy = TIPS</p> <p>DisabledReason = Account-Settings:Attempts-Exceeded</p> <p>DisabledBy = TIPS</p>
syslog example(s)	<p>2022-11-11T18:33:29.850796-05:00 2022-11-11 18: 33:29,817 192.168.144.3 Audit Records 4372 1 0</p> <p>Timestamp=Nov 11 2022 18:33:02.220 EST,Component=Command</p> <p>Line,Level=WARN,Category=Session Inactivity,Action=None,Description=Disconnecting CLI session due to session inactivity.\nUser: appadmin</p>

NDcPP22e: FTA_TAB.1	Auditable Events	None	Additional Content	None
---------------------	------------------	------	--------------------	------

AUTHSVR10: FTA_TSE.1	
Auditable Events	Denial of session establishment due to the session establishment mechanism
Additional Content	Reason for denial, origin of establishment attempt.

Audit Observed In	Monitoring > Event Viewer
Audit Event Details	<p>Source: Admin UI</p> <p>Level: WARN</p> <p>Category: Login Failed</p> <p>Action: None</p> <p>Timestamp: <i>[time]</i></p> <p>Description: User: <i>[username]</i></p> <p>Client IP Address: <i>[IP]</i></p>
Audit Observed In	Monitoring > Live Monitoring > Access Tracker
Audit Event Details	<p>Error Category: <i>[service type]</i> authentication</p> <p>Error Code: <i>[reason]</i></p> <p>Alerts for this Request</p> <p><i>[service]</i></p> <p><i>[technical reason]</i></p>
	<p><i>[example audit]</i></p> <p>Error Category: Tacacs authentication</p> <p>Error Code: Authentication privilege level mismatch</p> <p>Alerts for this Request</p> <p>Tacacs server</p> <p>Requested priv_level=<i>[01]</i> greater than Max Allowed priv_level=<i>[00]</i></p>
	<p><i>[example audit]</i></p> <p>Error Category: Tacacs authentication</p> <p>Error Code: User not found</p> <p>Alerts for this Request</p> <p>Tacacs server</p> <p>User <i>[username]</i> account disabled in[Local User repository](localhost)</p> <p>User <i>[username]</i> not present in [Admin User Repository](localhost).</p> <p>Failed to authenticate user=<i>[username]</i></p>
syslog example(s)	2023-02-24T18:56:37.993755-05:00 192.168.144.3 2023-02-24 18: 56:38,242 [RequestHandler-1-0x7f2e15dee700 h=563 c=R00000004-01-63f94eb6] DEBUG Common.BaseRadiusEnfProfileInfo - Enf profile Id=2 name=[Deny Access Profile] is applicable for IP=192.168.144.36 NAD ID=3001. Profile not restricted to any NAD groups

NDCPP22e: FTP_ITC.1

Auditable Events	Initiation of the trusted channel. Termination of the trusted channel. Failure of the trusted channel functions.
Additional Content	Identification of the initiator and target of failed trusted channels establishment attempt.
Audit Observed In	Monitoring > Event Viewer
Audit Event Details	<p>Source: ClearPass IPsec Tunnel</p> <p>Level: INFO</p> <p>Category: Up</p> <p>Action: [empty]</p> <p>Timestamp: [time]</p> <p>Description: Tunnel (Remote IP : [IP]): CHILD_SA ipsec-[value] established with SPIs [SPI #1] and [SPI #2] ===[IP]/32</p>
	<p>Source: ClearPass IPsec Tunnel</p> <p>Level: INFO</p> <p>Category: Down</p> <p>Action: [empty]</p> <p>Timestamp: [time]</p> <p>Description: Tunnel (Remote IP : [IP]): Deleting IKE_SA ipsec-[value] between [IP ([DN]])</p>
syslog example(s)	<p>Initiation</p> <p>2023-02-24T09:00:16-05:00 192.168.144.3 cppm.ipsec[20011]: Feb 24 09:00:16 08[IKE] <ipsec-3026 29> IKE_SA ipsec-3026[29] established between 192.168.145.3[192.168.145.3]...192.168.145.36[192.168.145.36]</p> <p>2023-02-24T09:00:16-05:00 192.168.144.3 cppm.ipsec[20011]: Feb 24 09:00:16 10[IKE] <ipsec-3026 29> CHILD_SA ipsec-3026{36} established with SPIs c1b6f9bb_i c78f4820_o and TS 192.168.145.3/32 == 192.168.145.36/32</p> <p>Termination</p> <p>2023-02-24T12:39:44-05:00 192.168.144.3 cppm.ipsec[20011]: closing CHILD_SA ipsec-3026{38} with SPIs c753afac_i (76 bytes) cd1a758d_o (76 bytes) and TS 192.168.145.3/32 == 192.168.145.36/32</p> <p>2023-02-24T12:39:44-05:00 192.168.144.3 cppm.ipsec[20011]: Feb 24 12:39:44 06[IKE] <ipsec-3026 32> deleting IKE_SA ipsec-3026[32] between 192.168.145.3[192.168.145.3]...192.168.145.36[192.168.145.36]</p> <p>Failure</p> <p>See NDCPP22E:FCS_IPSEC_EXT.1</p>

AUTHSVR10: FTP_ITC.1(1)

Auditable Events	Initiation of the trusted channel. Termination of the trusted channel. Failure of trusted channel functions
Additional Content	Identification of the initiator and target of failed trusted channels establishment attempt.
Audit Observed In	Monitoring > Event Viewer
Audit Event Details	<p>Source: ClearPass IPsec Tunnel</p> <p>Level: ERROR</p> <p>Category: Tunnel Action</p> <p>Action: [empty]</p> <p>Timestamp: <i>[time]</i></p> <p>Description: Tunnel (Remote IP : <i>[IP]</i>):</p> <p>Constraint check failed: <i>[reason]</i></p>
syslog example(s)	<p>IPsec</p> <p>See NDcPP22e:FTP_ITC.1 above</p> <p>RadSec</p> <p>Initiation</p> <p>2023-02-25T13:25:07.872258-05:00 192.168.144.3 2023-02-25 13: 25:07,871 [Tunnel ID: 14, From Client: 192.168.144.36:51310] DEBUG RadSec - tlsserverrd: starting for 192.168.144.36:51310</p> <p>Termination</p> <p>2023-02-25T13:25:07.876495-05:00 192.168.144.3 2023-02-25 13: 25:07,876 [Tunnel ID: 14, From Client: 192.168.144.36:51310] DEBUG RadSec - tlsserverrd: reader for 192.168.144.36 exiting</p> <p>Failure</p> <p>See AUTHSRVEP10:FCS_RADSEC_EXT.1</p>

NDcPP22e: FTP_TRP.1/Admin	
Auditable Events	Initiation of the trusted path. Termination of the trusted path. Failure of the trusted path functions.
Additional Content	Identification of the claimed user identity.
Audit Observed In	Monitoring > Event Viewer
Audit Event Details	<p>Source: Command Line</p> <p>Level: INFO</p> <p>Category: Logged in</p> <p>Action: None</p> <p>Timestamp: <i>[time]</i></p> <p>Description: User: appadmin</p>

	<p>Group: Local Administrator Client IP Address: <i>[IP]</i></p>
	<p>Source: Command Line Level: INFO Category: Logged out Action: None Timestamp: <i>[time]</i> Description: User: appadmin Client IP Address: <i>[IP]</i></p>
	<p>Source: Command Line Level: WARN Category: Login Failed Action: Failure Timestamp: <i>[time]</i> Description: Failed SSH public key login using appadmin account. Last login attempt from the remote host <i>[IP]</i></p>
	<p>Source: Command Line Level: WARN Category: Login Failed Action: Failure Timestamp: <i>[time]</i> Description: Failed SSH password login using appadmin account. Last login attempt from the remote host <i>[IP]</i></p>
	<p>Source: Admin UI Level: INFO Category: Logged in Action: None Timestamp: <i>[time]</i> Description: User: <i>[username]</i> Role: <i>[role]</i> Authentication Source: <i>[source]</i> Session ID: <i>[session]</i> Client IP address: <i>[IP]</i> Session Inactivity Expiry Time: <i>[timer]</i></p>

	<p>Source: Admin UI</p> <p>Level: INFO</p> <p>Category: Logged out</p> <p>Action: None</p> <p>Timestamp: <i>[time]</i></p> <p>Description: User: <i>[username]</i></p> <p>Role: <i>[role]</i></p> <p>Session ID: <i>[session]</i></p> <p>Client IP address: <i>[IP]</i></p>
Audit Observed In	Monitoring > Live Monitoring > Access Tracker
Audit Event Details	<p>Error Code: 211</p> <p>Error Category: Authentication Failure</p> <p>Error Message: <i>[reason]</i> (example: Client certificate not valid)</p> <p>Alerts for this Request</p> <p>WebAuthService</p> <p>User <i>[username]</i> not present in <i>[authentication source]</i></p> <p>User <i>[username]</i> not present in <i>[authentication source]</i></p> <p>Failed to update certificate auth status</p> <p>Client certificate not valid</p>
syslog example(s)	<p>Initiation</p> <p>See NDCPP22e:FIA_UIA_EXT.1 for successful WebUI and SSH login</p> <p>Termination</p> <p>See NDCPP22e:FTA_SSL.4 for logout of WebUI and SSH</p> <p>Failure</p> <p>Refer to FCS_TLSS_EXT.2 for WebUI cert auth related failures. FCS_SSHS_EXT.1 for SSH protocol related failures and NDCPP22e:FIA_UIA_EXT.1 for username/password failure for both WebUI and SSH.</p>

APPENDIX B

IPsec Traffic Selector Rules

The default behavior for IPsec rules is to encrypt all traffic between ClearPass and the VPN peer. Traffic can be separated on a per-port and/or per-protocol level for encrypt, bypass, or drop actions. When implementing IKEv1, only one (1) rule of each type may be created. When implementing IKEv2, a maximum of ten (10) rules may be created for each IPsec tunnel.

The actions associated with each rule type are:

Encrypt Rules

All outbound packets matching these rules will be encrypted through the IPsec tunnel. When no subordinate actions are specified, this is the default for all traffic between hosts.

Bypass Rules

All outbound packets matching these rules will bypass the IPsec tunnel and flow to the remote peer outside of the VPN. This is commonly known as traffic “in the clear”, even though it may already be encrypted.

When using bypass rules, both peers must be configured to bypass selected traffic, or the remote peer will not correctly process the packets.

Drop Rules

All outbound packets matching these rules will be dropped.

Final Rule

An implicit rule is created with all IPsec traffic selection that will drop any outbound traffic not processed. This rule will create a behavior where all traffic that should be encrypted or dropped between peers will always be blocked when the VPN is inactive. Bypass traffic is unaffected by tunnel status.

Processing Order

IPsec rules are processed using both order and specificity. Order is established beginning by rule position #1 and descending within a rule group.

Specificity is established based on the exactness of a rule to match against. Rules with specific ports and protocols will be evaluated prior to more general rules that apply to all ports or protocols prior to rules that catch “any” traffic.

A series of rules defined in the following scenarios will have the appropriate results

Encrypt	Bypass	Deny	Result
123	443	22	Encrypt TCP/UDP 123, Bypass TCP/UDP 443, Deny all other traffic
Any	123	22	Bypass TCP/UDP 123, Deny TCP/UDP 22, Encrypt all other traffic
22	Any	123	Deny TCP/UDP 123, Encrypt TCP/UDP 22, Bypass all other traffic
123	443	Any	Encrypt TCP/UDP 123, Bypass TCP/UDP 443, Deny all other traffic
22	-	-	Encrypt TCP/UDP 22, Deny all other traffic (Bypass none)
-	22	-	Bypass TCP/UDP 22, Encrypt all other traffic (Deny none)
-	-	22	Deny TCP/UDP 22, Encrypt all other traffic (Bypass none)