Copyright

© Copyright 2018 Hewlett Packard Enterprise Development LP

Change Log

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Modified By</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>2018-01</td>
<td>8/31/18</td>
<td>Dennis Boas</td>
<td>• Reformatted</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Updated for release 6.7.4</td>
</tr>
<tr>
<td>2017-01</td>
<td>9/1/17</td>
<td>Dennis Boas</td>
<td>• Updated for release 6.6.7</td>
</tr>
</tbody>
</table>
Contents

Copyright ........................................................................................................................................... 2
Change Log .......................................................................................................................................... 2
Introduction ......................................................................................................................................... 6
ClearPass Security Overview .............................................................................................................. 6
External Security Testing and Accreditation ....................................................................................... 6

  Common Criteria .............................................................................................................................. 7
  FIPS 140-2 ........................................................................................................................................ 7
  Suite B cryptographic support .......................................................................................................... 7
Internal Security Testing ...................................................................................................................... 8
Vulnerability Management Process ..................................................................................................... 8
Ports ................................................................................................................................................... 9

  SMB Port Range Note ...................................................................................................................... 11
Locking Down Services ....................................................................................................................... 11

  Cryptography ................................................................................................................................. 11
  AD over SSL .................................................................................................................................. 11
  FIPS Mode ..................................................................................................................................... 11
  Enabling FIPS ............................................................................................................................... 12
  OCSP ............................................................................................................................................. 12
  OCSP Server Fail-Open to CRL ...................................................................................................... 13
  OCSP validation check Intermediate Certificates ......................................................................... 13
  OCSP/CRL Status Messages .......................................................................................................... 14
  NTP Authentication ....................................................................................................................... 14
  SMBv2/v3 support ........................................................................................................................ 15
SNMP ............................................................................................................................................... 15
  SNMP Traps ................................................................................................................................... 15
  System Cleanup Options ............................................................................................................... 16
  SNMP Private Enterprise MIB ......................................................................................................... 16
  SNMP Trap Receivers .................................................................................................................... 17
  External syslog .............................................................................................................................. 17
  LEEF and CEF format Syslog ......................................................................................................... 18
RADIUS Protocol ............................................................................................................................ 19
ClearPass Hardening Guide ................................................................................................................ 3
GUI admin user................................................................................................................................. 34
CLI appadmin user................................................................................................................................. 34
Database appexternal user...................................................................................................................... 34
API apiadmin user.................................................................................................................................. 35
ArubaSupport........................................................................................................................................ 35
AppSuperUser....................................................................................................................................... 35
AppUser ................................................................................................................................................ 35
For More Information............................................................................................................................ 36
Introduction

This document is intended to assist Aruba customers and partners in securely configuring and deploying Aruba ClearPass. It should be noted that security recommendations often involve tradeoffs; not every recommendation in this document will be appropriate for every situation. In general recommendations in this document represent security best practices and should be followed wherever network security is a priority.

ClearPass Security Overview

ClearPass provides numerous security checks and balances including:

- All management and configuration actions including create, delete and modify operations are recorded in an audit log. The Audit Viewer provides real time searchable access that allows an administrator to review all policy level actions.
- Policy simulations allow all policies to be verified before they are deployed.
- A "Monitor Only" mode allows administrators to deploy the policies without actually enforcing any access control. This enables administrators to fine-tune their policies and resolve policy exceptions before enabling enforcement.
- Once the policies are deployed, ClearPass provides administrators with multiple ways to track authentications and authorizations:
  - Access Tracker is a real-time searchable log that shows which policies are being applied and what actions are being taken. Access Tracker also shows all exceptions and failures.
  - Insight is a reporting, analytics and alerting tool that can be configured to generate historical reports on authenticating users and devices, policies applied, and enforcement action taken. Insight also allows administrators to specify alert thresholds and conditions for policy exceptions or other system level failures. When the conditions and thresholds are satisfied the system sends out Email and SMS text alerts.
- At a system level ClearPass has been hardened in numerous ways:
  - ClearPass runs on a hardened Linux based operating system.
  - All sensitive data directories are protected using AES -128 encryption.
  - CLI access into the operating system is through a restricted shell
  - Only required services are run
  - The appliance is firewalled internally to only allow limited traffic
  - Separate management and data interfaces, with the ability to restrict access to the management interface to authorized end stations.
  - Timely security patches are provided for critical and high-level OS and application level security advisories
- Before every release of ClearPass, system level vulnerability scans are performed using tools such as QualysGuard, and IBM AppScan.

External Security Testing and Accreditation

Aruba invests heavily in independent third-party security testing of its products. While the majority of this testing is relevant to - and required by - government agencies, it has value to all types of users. In some cases, organizations may choose to rely on recognized security testing authorities rather than conducting their own product testing.
Common Criteria

ClearPass was awarded Common Criteria certification under both the Network Device collaborative Protection Profile (NDcPP) and the Authentication Server Extended Package.

FIPS 140-2

The Federal Information Processing Standard 140-2 is a system for testing and certifying cryptographic modules. As part of this testing, a laboratory accredited by the US and Canadian governments examines design documentation, source code, and development practices, in addition to conducting extensive testing of cryptographic functions. Products that implement FIPS 140-2 validated cryptography are assured to be using cryptography correctly.


When operated in FIPS mode ClearPass Policy Manager, Guest and Onboard are FIPS 140-2 compliant through incorporation of a FIPS-validated module, which provides all cryptography functions for the application. ClearPass incorporates the Aruba Linux Cryptographic Module which implements full and approved cryptographic algorithm support, including Suite B algorithm compliance, for Aruba products. It provides secure key management, data integrity, data at rest encryption, and secure communications.

[Suite B cryptography](http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm#2577)

Suite B cryptographic support

ClearPass Policy Manager and RADIUS server include Suite B cryptographic support.

Suite B cryptographic algorithms are specified by the National Institute of Standards and Technology (NIST) and are used by NSA's Information Assurance Directorate in solutions approved for protecting National Security Systems (NSS). Suite B includes cryptographic algorithms for encryption, key exchange, digital signature, and hashing.

<table>
<thead>
<tr>
<th>Algorithm</th>
<th>Function</th>
<th>Specification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Advanced Encryption Standard (AES)</td>
<td>Encryption</td>
<td>FIPS Pub 197</td>
</tr>
<tr>
<td>Elliptic Curve Diffie-Hellman (ECDH)</td>
<td>Key Exchange</td>
<td>NIST SP 800-56A</td>
</tr>
<tr>
<td>Elliptic Curve Digital Signature Algorithm (ECDSA)</td>
<td>Digital Signature</td>
<td>FIPS Pub 186-4</td>
</tr>
<tr>
<td>Secure Hash Algorithm (SHA)</td>
<td>Hashing</td>
<td>FIPS Pub 180-4</td>
</tr>
</tbody>
</table>
Internal Security Testing

Each ClearPass release goes through extensive quality assurance testing. As part of the testing process, several commercial vulnerability scanners are used. These include:

- QualysGuard
- IBM AppScan

Any findings returned by these scanners are examined to determine if they are genuine vulnerabilities or false positives. Actual vulnerabilities will cause a bug to be opened.

In addition to quality assurance testing, an internal group known as Aruba Threat Labs provides advanced vulnerability research against Aruba products. Aruba Threat Labs conducts penetration testing through both black-box and white-box testing, also including source code analysis. From time to time, Aruba Threat Labs also contracts with external third-party penetration testing firms to conduct targeted testing. Aruba Threat Labs maintains a database of common findings reported by popular vulnerability scanning tools. This database is available at [http://www.arubanetworks.com/support-services/security-bulletins/](http://www.arubanetworks.com/support-services/security-bulletins/)

Vulnerability Management Process

## Ports

The following table lists the ports that are used by ClearPass.

<table>
<thead>
<tr>
<th>Between</th>
<th>Protocol</th>
<th>Port</th>
<th>Service Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ClearPass UI Management Station</td>
<td>TCP</td>
<td>443</td>
<td>HTTPS</td>
</tr>
<tr>
<td>Secure Shell Client</td>
<td>TCP</td>
<td>22</td>
<td>SSH</td>
</tr>
<tr>
<td>Guest Portal Controller</td>
<td>TCP</td>
<td>443 / 80</td>
<td>HTTP not recommended but can be configured</td>
</tr>
<tr>
<td>Update service ClearPass</td>
<td>TCP</td>
<td>443</td>
<td>HTTPS</td>
</tr>
<tr>
<td>OnGuard Agent Endpoints</td>
<td>TCP</td>
<td>443</td>
<td>HTTPS</td>
</tr>
<tr>
<td>OnGuard Agent Endpoints</td>
<td>TCP</td>
<td>6658</td>
<td>OnGuard to CPPM</td>
</tr>
<tr>
<td>NAS Devices ClearPass</td>
<td>TCP/UDP</td>
<td>1812</td>
<td>RADIUS</td>
</tr>
<tr>
<td>NAS Devices ClearPass</td>
<td>TCP/UDP</td>
<td>1645</td>
<td>RADIUS</td>
</tr>
<tr>
<td>NAS Devices ClearPass</td>
<td>TCP/UDP</td>
<td>1813</td>
<td>RADIUS Accounting</td>
</tr>
<tr>
<td>NAS Devices ClearPass</td>
<td>TCP/UDP</td>
<td>1646</td>
<td>RADIUS Accounting</td>
</tr>
<tr>
<td>NAS Devices ClearPass</td>
<td>TCP/UDP</td>
<td>3799</td>
<td>RADIUS CoA - RFC3576</td>
</tr>
<tr>
<td>NAS Devices ClearPass</td>
<td>TCP/UDP</td>
<td>49</td>
<td>TACACS</td>
</tr>
<tr>
<td>ClearPass to Active Directory</td>
<td>ICMP echo (8) and echo-reply (0) between CPPM host and Domain Controller used during domain join</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ClearPass AD Servers</td>
<td>TCP/UDP</td>
<td>389</td>
<td>LDAP</td>
</tr>
<tr>
<td>ClearPass AD Servers</td>
<td>TCP/UDP</td>
<td>636</td>
<td>LDAP over SSL</td>
</tr>
<tr>
<td>ClearPass AD Servers</td>
<td>TCP/UDP</td>
<td>445</td>
<td>NetLogon</td>
</tr>
<tr>
<td>ClearPass AD Servers</td>
<td>TCP</td>
<td>49152</td>
<td>SMBv2 / v3 RPC randomly allocated high TCP ports see SMB Ports Range Note</td>
</tr>
<tr>
<td>ClearPass AD Servers</td>
<td>TCP</td>
<td>1025 - 5000</td>
<td>SMBv1 RPC randomly allocated low TCP ports see SMB Ports Range Note</td>
</tr>
<tr>
<td>Service Type</td>
<td>Service</td>
<td>Port</td>
<td>Protocol</td>
</tr>
<tr>
<td>-------------------</td>
<td>--------------</td>
<td>------</td>
<td>----------</td>
</tr>
<tr>
<td>ClearPass Misc Services</td>
<td>AD Servers</td>
<td>88</td>
<td>UDP</td>
</tr>
<tr>
<td>ClearPass Misc Services</td>
<td>AD Servers</td>
<td>464</td>
<td>TCP</td>
</tr>
<tr>
<td>ClearPass Misc Services</td>
<td>AD Servers</td>
<td>139</td>
<td>TCP</td>
</tr>
<tr>
<td>SNMP</td>
<td>ClearPass Endpoint</td>
<td>161</td>
<td>UDP</td>
</tr>
<tr>
<td>SNMP</td>
<td>Endpoint</td>
<td>162</td>
<td>UDP</td>
</tr>
<tr>
<td>WMI</td>
<td>ClearPass Endpoint</td>
<td>135</td>
<td>TCP</td>
</tr>
<tr>
<td></td>
<td>Publisher Subscriber</td>
<td>443</td>
<td>TCP</td>
</tr>
<tr>
<td></td>
<td>Subscriber Publisher</td>
<td>443</td>
<td>TCP</td>
</tr>
<tr>
<td></td>
<td>Publisher Subscriber</td>
<td>5432</td>
<td>TCP</td>
</tr>
<tr>
<td></td>
<td>Subscriber Publisher</td>
<td>5432</td>
<td>TCP</td>
</tr>
<tr>
<td></td>
<td>Subscriber Publisher</td>
<td>123</td>
<td>UDP</td>
</tr>
<tr>
<td></td>
<td>ClearPass NTP Servers</td>
<td>123</td>
<td>UDP</td>
</tr>
<tr>
<td></td>
<td>ClearPass SMTP Servers</td>
<td>25</td>
<td>TCP</td>
</tr>
<tr>
<td></td>
<td>ClearPass SMTP Servers</td>
<td>465</td>
<td>TCP</td>
</tr>
<tr>
<td></td>
<td>ClearPass DNS Servers</td>
<td>53</td>
<td>TCP</td>
</tr>
<tr>
<td></td>
<td>Network ClearPass</td>
<td>67</td>
<td>UDP</td>
</tr>
<tr>
<td></td>
<td>Network ClearPass</td>
<td>2055</td>
<td>UDP</td>
</tr>
<tr>
<td></td>
<td>Network ClearPass</td>
<td>6343</td>
<td>UDP</td>
</tr>
<tr>
<td></td>
<td>Network ClearPass</td>
<td>514</td>
<td>UDP</td>
</tr>
</tbody>
</table>

**Note:** Ports required will vary based on features configured.
SMB Port Range Note

SMBv2 and SMBv3 protocols use an increased remote procedure call (RPC) port range for Windows Server 2008 and later. The following AD deployments determine the ports used:

- Active Directory deployments that use only Windows Server 2008 or later use the high port range of 49152 through 65535.
- Active Directory deployment that use Windows Server 2008 or later and earlier versions of Windows Server use both the low port range of 1025 through 5000 and the high port range of 49152 through 65535.
- Active Directory deployment that use only versions earlier than Windows Server 2008 use the low port range of 1025 through 5000.

Locking Down Services

Cryptography

Aruba ClearPass employs cryptography as a part of several services, including HTTPS, SSH, IPsec, and others.

AD over SSL

When using Active Directory as an authentication source with connection security “AD over SSL” the following cipher suites are supported:

- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384_P384
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA_P384
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA_P384
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA_P256
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA_P256
- TLS_DHE_DSS_WITH_AES_256_CBC_SHA256
- TLS_DHE_DSS_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA

FIPS Mode

In the FIPS mode all cryptographic services provide a minimum strength of 112 bits as mandated by FIPS 140-2. Services which provide less than 112 bits of security (such as RSA-1024, SHA1 for digital signatures, MD5, DES) may not be configured. In non-FIPS mode there are no restrictions on minimum security strength. Algorithms such as DES (56-bits of strength) and MD5 (<64 bits of strength) are permitted to be used, although this is not the default configuration.
Enabling FIPS

- Review the following important points, before enabling FIPS mode in ClearPass Policy Manager:
- The database is reset when FIPS mode is enabled. Ensure that a secure current back up of the ClearPass database exists before enabling FIPS mode.
- Configuration backup files from Policy Manager in non-FIPS mode cannot be restored to Policy Manager in FIPS mode.
- Configuration backup files from Policy Manager in FIPS mode can be restored to Policy Manager in the non-FIPS mode.
- The server will be removed from the cluster when FIPS mode is enabled.
- All nodes in a cluster must be either in FIPS or non-FIPS mode.
- Legacy authentication methods such as EAP-MD5 and MD5 message digest algorithm are not supported in FIPS mode.
- Certificates that are created with MD5 authentication cannot be imported to the Certificates Trust List (Administration > Certificates > Certificate Trust List).
- The server reboots when FIPS mode is enabled.

OCSP

- **Include Nonce in OCSP request.** If the OCSP server doesn't support the nonce then set this value to FALSE to avoid an EAP-TLS authentication failure. A nonce is a cryptographic value that is used to protect against record and replay attacks
- **Enable Signing for OSCP Requests.** Enables ClearPass to sign the OCSP request with the Radius server certificate. The default value for this parameter is set to FALSE to disable the signing process. Signing verifies the integrity of the data and the identity of the sender.
OCSP Server Fail-Open to CRL
For EAP-TLS authentication methods, if the OCSP server is not accessible to perform certificate validation, ClearPass provides an option to validate against a CRL instead (fallback).

OCSP validation check Intermediate Certificates
To enhance certificate security the RADIUS service parameter, Check the validity of intermediary certificates in the chain using OCSP, can be enabled. Enabling this validates the entire certificate chain. Enabling this feature will put greater load on the system and is not intended for all customer use cases.
OCSP/CRL Status Messages

The Event Viewer provides a notification when

- The connection to an OCSP server times out
- No response is received from an OCSP server
- CRL has expired
- CRL download fails

NTP Authentication

If Network Time Protocol is not authenticated, an attacker can introduce a rogue NTP server. This rogue server can then be used to send incorrect time information to network devices, which will make log timestamps inaccurate and affect scheduled actions. NTP authentication is used to prevent this tampering by authenticating the time source. ClearPass supports authenticating its network time sources using SHA or SHA1. In FIPS mode, only SHA1 is supported. The authentication leverages the Linux NTP service. In a cluster the publisher is the time source for all subscribers and subscribers do not authenticate the publisher.
**SMBv2/v3 support**

ClearPass supports SMBv2/v3 for PEAPv0/EAP-MSCHAPv2 and Microsoft Active Directory Domain Services. ClearPass will use the highest version available on the controller;

- SMBv3 will be automatically used by default for AD joins and any requests that use PEAPv0/EAP-MSCHAPv2
- If SMBv3 is not enabled, ClearPass will then automatically failover to SMBv2.
- If SMBv2 is also not enabled, ClearPass will then failover to use SMBv1

If higher SMB versions are later enabled on the client, ClearPass will then detect the changes and attempt to use the highest available SMB version automatically

**SNMP**

The Simple Network Management Protocol is commonly used by network management systems to poll devices for information such as port configuration, status, and interface counters. SNMP versions 1 and 2 provide very little security beyond the community string. If an attacker has network access to a device and can guess the community string, it may lead to disclosure of sensitive information. Aruba strongly recommends the use of SNMPv3, which includes much stronger security through authentication and encryption.

Navigate to Administration > Server Manager > Server Configuration > System Monitor tab to configure the SNMP parameters. This ensures that external Management Information Base (MIB) browsers can browse the system level MIB objects exposed by the Policy Manager appliance. The options in this page vary based on the SNMP version selected.

**SNMP Traps**

SNMP Trap Receivers can be configured to receive traps for critical system events.

Policy Manager sends SNMP traps that expose the following server information:

- System uptime. Conveys information about how long the system is running
- Network interface statistics [up/down]. Provides information if the network interface is up or down
- Process monitoring information. Check for the processes that should be running. Maximum and minimum number of allowed instances. Sends traps if there is a change in value of maximum and minimum numbers
- Disk usage. Check for disk space usage of a partition. The agent can check the amount of available disk space, and make sure it is above a set limit. The value can be in % as well. Sends traps if there is a change in the value
• CPU load information. Check for unreasonable load average values. For example, if 1 minute CPU load average exceeds the configured value [in percentage] then system would send the trap to the configured destination
• Memory usage. Report the memory usage of the system

Free Disk and CPU Load thresholds are configured under the service parameters tab

System Cleanup Options
In order to prevent disk space exhaustion ClearPass includes a Cluster wide parameter “Free Disk Space Threshold Value” that can be used to trigger a disk cleanup. The default value is 30%.

Once an hour ClearPass checks the free disk space, if it's below the threshold an alert is logged and an aggressive cleanup job is run. The job cleans up any records that are older than one day from the following:

• Log database records
• Core files
• System load monitor files
• Application and system log files
• Auto and manual backup files
• Stored reports
• Expired guest accounts
• Audit records

SNMP Private Enterprise MIB
ClearPass includes a Private Enterprise MIB that exposes over 70 OID’s. Information and traps include
• Performance counters
  o Authentication counters
  o Authorization counters
  o Request processing time/delays
  o Authorization time/delays
• System statistics
  o Disk statistics (available, total, used)
  o Memory statistics (available, total, used)
  o CPU load averages
• Network traffic counters
  o Application name
  o Application port
  o Total network traffic in bytes
• SNMP Traps
  o Free disk space is lower than the configured threshold
  o Low system memory
  o High CPU utilization
  o License expiration
  o Certificate expiration
  o Cluster node add
  o Cluster node promote
  o Cluster node delete
  o Cluster password change
  o Cluster license utilization

**SNMP Trap Receivers**
External trap receivers are added at: Administration » External Servers » SNMP Trap Receivers

![Add SNMP Trap Server](image)

**External syslog**
When a system is compromised, one of the first things an attacker will do is to remove evidence of the intrusion from the system logs. For this reason, it is important to send logs to an external system – preferably one with automated log analysis tools that can identify and flag unusual activity. ClearPass supports the syslog standards for log distribution. Log information can be sent to one or more syslog targets (servers).

Syslog Targets and Export Filters are configured under the External Servers Tab
Policy Manager uses Syslog to export session data from access tracker, audit records from audit viewer, event records from event viewer and Insight logs. Syslog Export Filters are configured to tell Policy Manager where to send the log information, and what information should be included in the logs sent to each Syslog Target. If desired, different information can be sent to each syslog target. The Insight Log filters provide the option to select predefined groups of fields or to select individual fields. The Active Session filter adds the option for customized SQL Queries.

**LEEF and CEF format Syslog**

ClearPass supports CEF (Common Event Format) and LEEF (Log Event Extended Format) Syslog formats. The Event Format can be selected from the Syslog Export Filters.
RADIUS Protocol

ClearPass uses the RADIUS protocol to exchange authentication information with Network Access Devices. The RADIUS protocol provides a weak form of encryption, which uses a static RADIUS shared secret as the basis for the encryption key. To maximize security the RADIUS shared secret should be both long and complex. Since there is no need for this secret to be memorable by a human, the use of a service such as http://www.random.org/ to generate a truly random string is recommended. To minimize the damage from a compromised shared secret each Network Access Device that communicates with ClearPass should be configured to use a different RADIUS shared secret.

Disabling TLS 1.0 and TLS 1.1 in the Web UI and the RADIUS server

For enhanced security a cluster-wide parameter allows disabling TLSv1.0 and TLSv1.1.

Locking Down Administrative Access

A primary intrusion attack vector used against network devices is the device’s administrative console. The ClearPass Admin Web UI and command line interface (CLI) should be made as secure as possible to minimize the chances of a successful compromise.
Management Access Control

Aruba recommends permitting administrative access only from authorized end systems. If the network design permits, it is best practice to separate management and user-facing services (data traffic) by creating a dedicated management network and attaching the ClearPass management interface to that network. In this type of deployment, the ClearPass management interface provides Web UI and CLI access for server and cluster administration and configuration. The Management interface also handles internal cluster (Publisher / Subscriber) communication. The Data interface provides point of contact for all user-facing services including authentication and authorization requests using RADIUS, TACACS+ and web authentication. Data Port security is enhanced by restricting the SSH protocol. SSH is not permitted to the Data Port, it is denied by default internal firewall rules.

<table>
<thead>
<tr>
<th>IPv4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management Port</td>
</tr>
<tr>
<td>IP Address</td>
</tr>
<tr>
<td>Subnet Mask</td>
</tr>
<tr>
<td>Default Gateway</td>
</tr>
<tr>
<td>Data/External Port</td>
</tr>
<tr>
<td>IP Address</td>
</tr>
<tr>
<td>Subnet Mask</td>
</tr>
<tr>
<td>Default Gateway</td>
</tr>
</tbody>
</table>

Restrict Concurrent Admin logins

When the Allow Concurrent Admin Logins is set to false and a new user logs in as Admin, earlier sessions using the same credentials that are still active on other cluster appliances will automatically be logged out.

<table>
<thead>
<tr>
<th>Cluster-Wide Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>General</strong></td>
</tr>
<tr>
<td>Policy result cache timeout</td>
</tr>
<tr>
<td>Free disk space threshold value</td>
</tr>
<tr>
<td>Free memory threshold value</td>
</tr>
<tr>
<td>Endpoint Context Servers polling interval</td>
</tr>
<tr>
<td>Syslog Export Interval</td>
</tr>
<tr>
<td>Automatically check for available Software Updates</td>
</tr>
<tr>
<td>Automatically download Posture Signature and Windows Hotfixes Updates</td>
</tr>
<tr>
<td>Automatically download Endpoint Profile Fingerprints</td>
</tr>
<tr>
<td>Login Banner Text</td>
</tr>
<tr>
<td><strong>Parameter Name</strong></td>
</tr>
<tr>
<td>Allow Concurrent Admin Login</td>
</tr>
<tr>
<td>Admin Session Idle Timeout</td>
</tr>
<tr>
<td>CLI Session Idle Timeout</td>
</tr>
<tr>
<td>Console Session Idle Timeout</td>
</tr>
<tr>
<td>Disable TLSv1.0 support</td>
</tr>
<tr>
<td>Disable TLSv1.1 support</td>
</tr>
<tr>
<td>Content Security Policy (CSP)</td>
</tr>
</tbody>
</table>

Content Security Policy (CSP) option

When enabled the Content Security Policy (CSP) option helps reduce the cross-site scripting (XSS) risks in browsers by declaring which dynamic resources can be loaded via an HTTP Header. When this parameter is enabled, it can negatively affect any customized HTML code customers might have for skins, captive portals, self-registration workflows, and so on in ClearPass Guest. If the configuration includes customized HTML code that references images, media, scripts, or other resources on servers outside ClearPass, the CSP parameter should not be enabled or a different approach for accessing these resources should be used.
**IPsec Tunnel Support**

ClearPass supports IPsec tunnels for the management and data interfaces. IPsec provides encrypted tunnels that guarantee the confidentiality of the communications and the identity of the endpoints. This is critical in high security environments or when the communications path crosses a public network.

Traffic selectors can be used to control the IPsec tunnel traffic. Selector options include:

- Encrypt
- Drop
- Bypass
Application Access Control

ClearPass provides application level restrictions that can define networks / end systems and allow or deny them access to specific applications. Applications include; Policy Manager, OnGuard, Graphite, Guest Operator and Insight. To configure these restrictions, go to Administration > Server Manager > Server Configuration, click on the server, go to the Network tab and select the option “Application access control”. In a cluster, restrictions need to be configured on each node.

In this example only the defined IP Addresses, 192.168.1.12 and 192.168.1.20, will be able to access ClearPass Policy Manager.

Smart card and Certificate based login

ClearPass supports smart card and TLS certificate-based login for all ClearPass applications; ClearPass Policy Manager, ClearPass Guest, ClearPass Onboard and ClearPass Insight

- Certificate can come from a smart card or certificate store
- Certificate can be mandatory or optional
- Certificate can be in addition to username / password or standalone
When the user attempts to login to the ClearPass application they will be prompted to select a certificate before moving to the login screen.

![Select Certificate](image)

In this example logging in requires both a valid certificate and a valid password.

![Login](image)

**Restricting Administrator Privileges**

Admin users should be assigned privileges appropriate to their job responsibilities. By default, there are seven levels of Administrative privilege.

<table>
<thead>
<tr>
<th>#</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>API Administrator</td>
<td>An API administrator is only allowed API access to read/write all configuration elements</td>
</tr>
<tr>
<td>2</td>
<td>Aruba User Role Download</td>
<td>Privilege level used for Aruba User Role Download API operations</td>
</tr>
<tr>
<td>3</td>
<td>Help Desk</td>
<td>A help desk person logs in to troubleshoot problems reported by end users</td>
</tr>
<tr>
<td>4</td>
<td>Network Administrator</td>
<td>A network administrator is allowed to configure all the policies in the system</td>
</tr>
<tr>
<td>5</td>
<td>Read-only Administrator</td>
<td>A read-only administrator is only allowed to read all configuration elements</td>
</tr>
<tr>
<td>6</td>
<td>Receptionist</td>
<td>A receptionist is allowed access to main monitoring screens</td>
</tr>
<tr>
<td>7</td>
<td>Super Administrator</td>
<td>A super administrator is allowed read/write access to all configuration elements</td>
</tr>
</tbody>
</table>

For API access the “API Administrator” privilege level should be used. This privilege level allows programmatic access but denies UI logins.

If necessary Admin access can be further restricted by creating Custom privileges. These policies can be tailored to provide fine-grained control of access to ClearPass components and services. Admin privileges can be customized for both Policy Manager and Insight.
Password Policy

Authentication with username/password does not provide the strongest form of security, yet it is extremely common. To strengthen administrator access both the Admin account username and password should be changed. Changing the Admin account username means an attacker would have to guess not only the password but also the username, increasing the difficulty of the attack. The account name should not be descriptive or easily guessed. Apply the same strong password policy, mixed case, mixed alphanumeric characters and special characters (only – and _ permitted for username) for both username and password. To provide audit control every Administrator should have their own account and accounts should never be shared between users.

The Cluster (appadmin) password should also be changed to strong value. Go to Administration > Server Manager > Server Configuration and click on the Change Cluster Password link.
Password Policy Enforcement

Allows administrators to set enforcement rules for Admin and Local User Account passwords. Separate policies can be set for Admin and Local users.

The policy includes:

- Minimum password length
- Password complexity
- Additional checks
- Password expiration
- History
- Reminder (TACACS+ only)
- Disable settings

Accounts can be automatically disabled based on account lifetime and passwords failed attempts or password expiration

- Days exceeded
- Date exceeds
- Failed attempts
- Password not changed for
Centralized Authentication and Authorization

In an organization with multiple administrators, the use of centralized authentication helps to prevent insider attacks. With centralized authentication, ClearPass does not need multiple local administrative accounts. Instead, administrative users log in with credentials that are authenticated remotely by an Active Directory or LDAP server. The remote server should return both authentication and authorization information. After authenticating the user, attribute information such as group membership or primary security affiliation should be used to assign the correct administrative privilege level.

The following example assigns Super Admin access if the user authenticates successfully and is a member of the Active Directory group CP Admin

\[ \text{(Tips: Role} \text{ EQUALS [User Authenticated] AND (Authorization:lab ad:memberOf CONTAINS CP Admins)} \text{)}\]

Enhanced Security for Admin and local user accounts

Store hash for Admin and Local User passwords

Admin and Local User passwords are stored in PBKDF2_SHA1 based password hashes. A global setting is provided to optionally also store the NTLM hash of the password. This is required for MSCHAPv2-based authentications.
against the local database. The Guest user password fields in the DB are individually encrypted and the DB itself is stored encrypted (data at reset encryption).

### Session timeouts

Session timeouts are enforced to eliminate stale sessions.

**Admin Session Timeout**

The Cluster-wide Admin Session Timeout Parameter allow Admins to configure the maximum idle time permitted for Admin access. This Admin timeout limit applies to Policy Manager, Guest and Insight. The default is 30 mins.

**Caution:** There are several monitoring screens in the Admin UI (Dashboard, Access Tracker, OnGuard Activity, etc.) with Auto refresh enabled by default. If there is constant activity on these screens the UI session will never time out, so Administrators should be careful leaving the browser open on these screens or they should disable “Auto refresh” wherever applicable.

**CLI Session Timeout (SSH)**

A cluster wide service parameter "CLI Session Idle Timeout" allows administrators to control how long a CLI session may be idle before it is automatically terminated. If this parameter is changed, the changes will take effect when the client opens a new CLI session. Any active CLI sessions will continue to use the old timeout or they have to be disconnected and reconnected for the new changes to take effect.

**Console Session Timeout**

A cluster wide service parameter "Console Session Idle Timeout" allows administrators to control how long a console session may be idle before it is automatically terminated. Note: Since background processes are not counted as a part of active session, setting low console timeout value may lead to auto logout during system upgrade.
Enable Public Key Authentication

ClearPass supports public key-based SSH logins on a per-appliance basis. The SSH Public Keys option is available at Administration > Server Manager > Server Configuration > Network.

Monitoring

Excessive Failed Admin Login Attempts

One of the most common attack vectors is password guessing. The attacker attempts to gain access to Administrator and privileged accounts by first trying the default Admin password then trying the most commonly used passwords and finally using a brute force tool that tries large numbers of potential passwords from an attack dictionary. The indicator of this type of attack is a large number of failed authentications in a short period of time to the same account.

Insight Alert

Compliance and local security policies often require logging and alerting on potential brute force attacks on administrator and privileged accounts. The Insight alert shown below will send an Email and SMS text message when three login failures for the Admin username occur in a one-minute interval. The values should be adjusted to meet local security policy requirements.
Last admin login notification – GUI

Admin GUI shows when the most recent successful login occurred and the number of failed attempts that were made since the most recent successful login. The Messages are displayed on the Dashboard or Home Page of:

- Policy Manager
- Guest
- Onboard
- Insight

Policy Manger

Guest
Last admin login notification – CLI

The Console and SSH now show a message with the source and timestamp of the most recent successful login and the number of failed attempts that were made through both SSH and the console since the most recent successful login.

Details of the events are also displayed in the Event Viewer.

Access tracker

ClearPass will log authentication failures to Access Tracker. The Access Tracker entry includes valuable information that can be used for analysis:

- Username
- Date and Time
- Status
- Client IP (typically 127.0.0.1)
- Remote IP
Audit trail

An Audit Trail is a sequential record of which users have accessed the Admin UI and what changes they have made to the system. Access Tracker and the Event Viewer record all successful and unsuccessful login attempts. The event detail below shows User dennis successfully logging into the Admin UI in the role of Super Administrator on Sept 30 at 13:04:59 EDT from IP address 192.168.1.12

Audit Viewer shows user dennis modified the lab guest access service at 13:09:07

The detailed Audit record includes a complete record of the old data the new data and as shown below the inline differences. In this case user dennis added the local user repository as an authentication source for the lab guest access service.
Exporting Audit Records

By default, the ClearPass server only retains Audit records for seven days. This value is configurable at Administration » Server Manager » Server Configuration >> cluster wide Parameters.

If a longer audit trail is required audit records can be sent to an external syslog target for security and long-term storage. Administration » External Servers » Syslog Export Filters » Add

Automated backup recovery

By default, ClearPass does automatic backups at 1:00 am every night.

The backup files are stored in the local shared folders.
Storing Backups externally

To guarantee business continuity and for disaster recovery it is recommended that backup files are stored on an external server. ClearPass can be configured to automatically push backup files to a remote server.

![Add File Backup Server](image)

Locking Down User Access

User Roles and Firewall Policies

Aruba recommends deployment of role-based access controls for all wired and wireless users. Rather than granting one-size-fits-all access to the network once they have authenticated, users are only granted access appropriate for that user’s role in the organization. For example, only ClearPass administrators should be assigned roles that permit access to the ClearPass management Interface. Roles are enforced on the Network Access Device so the wireless controller or switch would apply a role to ClearPass administrators that permits access to the ClearPass management interface while all other users would be assigned roles that deny access the management interface.

Remote Assistance

ClearPass includes two remote support interfaces that allow Aruba TAC engineers to access the ClearPass server to help resolve customer issues.

Support Shell

The Support Shell gives TAC engineers CLI root access to the ClearPass server. The customer uses the CLI to generate a one-time use key for the TAC engineer. The key allows the engineer root level access.

Use the `gen-support-key` command to generate the support key for the system.

Syntax

```plaintext
system gen-support-key
```
Example

The following example generates the support key for the system:

```
[appadmin]# system gen-support-key
```

```
system gen-support-key

Support key='01U2FsdGVkX1+/WS9jZKQajERyzXhM8mF6zAKrzxrHvaM='
```

The Aruba support account by default is valid for 24 hours, We recommend administrators deactivate this account as soon as the debugging session is over.

Remote Assistance

The Remote Assistance feature enables the ClearPass Policy Manager administrator to allow an Aruba Networks support engineer to remotely log in using ssh to the ClearPass Policy Manager server and also view the Administration UI to debug any issues the customer is facing or to perform pro-active monitoring of the server.

The Remote Assistance account can specify time as one time for 1-24 hours and weekly or monthly re-occurrences.

The Administrator should make sure that accounts/sessions are terminated once the debugging session is done.

GUI and CLI Accounts

ClearPass makes use of a number of specialized accounts

**GUI admin user**

Administrative user with full access to the CPPM GUI. The GUI Admin user also has full access to the ClearPass API.

**CLI appadmin user**

User access to CPPM CLI, to run CLI commands and update the values. The appadmin password can be changed from the cluster settings page.

**Database appexternal user**

READ only access to the "tipsLogDb" database (system events, session logs, RADIUS accounting, alerts, etc), the "insightdb" database (information Insight uses to generate reports), and some tables in the "tipsdb" database.
The password should be changed using cluster wide parameters.

The database connections are made over TCP port 5432 to CPPM's management port. Remote database connections are allowed on CPPM's data port. Ensure that port 5432 is open when attempting to remotely connect to the CPPM's database.

**API apiadmin user**

Read and Write access to API's only. The apiadmin password should be changed from Administrator > Users and Privileges > Admin Users.

The following accounts are for **ARUBA INTERNAL USE ONLY** and are used for ClearPass troubleshooting.

**ArubaSupport**

Provides Full shell access to ClearPass CLI. This is strictly for ARUBA INTERNAL purposes. The "system gen-support-key" resets the support password and provides a token from which Aruba TAC can recover the password and login. Running the command again will reset the support password. There is also a periodic cron job that resets this password around midnight everyday. The Remote Assistance feature, which must be triggered by the customer, builds on this to provide remote access capability to TAC.

**AppSuperUser**

Full access to the postgres db on ClearPass after logging in as ArubaSupport. This is strictly for ARUBA INTERNAL purposes.

**AppUser**

Read only access to postgresql after logging in as ArubaSupport. This is strictly for ARUBA INTERNAL purposes.
Note: The appuser and appsuperuser accounts are critical internal accounts that do not permit remote logins (ssh or console).

For More Information
The best source of information on Aruba products, outside of official documentation, is the Airheads Social community. For security-related discussions, please visit the “Security” forum at http://community.arubanetworks.com/.