Aruba ClearPass As Built Report

|  |  |
| --- | --- |
| Author: | Alexis La Goutte |
| Date: | vendredi 23 février 2024 |
| Version: | 1.0 |

# 1 Implementation Report ALG-CPPM-612

The following section provides a summary of the implemented components on the Aruba ClearPass infrastructure.

## 1.1 Version

The following section details Version settings configured on ClearPass.

| Version | Build | Hardware Version | FIPS | Evaluation | Cloud |
| --- | --- | --- | --- | --- | --- |
| 6.12.0 | 300732 | CLABV | False | True | False |

Table - Version

## 1.2 Server Configuration

The following section details Server Configuration settings configured on ClearPass.

| Name | DNS Name | MGMT IP | DATA IP | Publisher | Insight (Primary) |
| --- | --- | --- | --- | --- | --- |
| ALG-CPPM-612 | ALG-CPPM-612 | 10.200.4.163 |  | True | False (False) |

Table - Server Configuration

## 1.3 License

The following section details License settings configured on ClearPass.

### 1.3.1 Summary

The following section details license Summary configured on ClearPass.

| Type | Count | Used | Updated |
| --- | --- | --- | --- |
| Onboard | 0 | 0 | 02/23/2024 17:00:04 |
| OnGuard | 0 | 0 | 02/23/2024 17:00:03 |
| Access | 100 | 0 | 02/23/2024 17:00:03 |

Table - License Summary

### 1.3.2 Application License

The following section details license Application License configured on ClearPass.

| Product Name | Licence Type | User Count | Licence Added | Activation Status |
| --- | --- | --- | --- | --- |
| Access | Evaluation | 100 | 12/08/2023 11:21:23 | False |

Table - Application License Summary

The following section details license Application License configured on ClearPass.

### 1.3.2.1 Application License: Access 1

|  |  |
| --- | --- |
| Product Id | 1 |
| Product Name | Access |
| Licence Key | -----BEGIN [ANONYMISED] KEY----- |
| Licence Type | Evaluation |
| User Count | 100 |
| Duration | 90 days |
| Licence Added | 12/08/2023 11:21:23 |
| Activation Status | False |

Table - Application License: Access 1

## 1.4 Authentication

The following section details Authentication settings configured on ClearPass.

### 1.4.1 Summary

The following section provides a summary of Authentication settings.

|  |  |
| --- | --- |
| Method | 20 (default: 20) |
| Source | 16 (default: 11) |

Table - Authentication Summary

### 1.4.2 Authentication Method

The following section details Authentication Method configured on ClearPass.

| Id | Name | Description | Method Type | Inner Methods | Details Count |
| --- | --- | --- | --- | --- | --- |
| 1 | [PAP] | Default settings for PAP | PAP |  | 1 |
| 2 | [MSCHAP] | Default settings for MSCHAP | MSCHAP |  | 1 |
| 3 | [EAP TLS] | Default settings for EAP-TLS | EAP-TLS |  | 6 |
| 4 | [EAP TTLS] | Default settings for EAP-TTLS | EAP-TTLS | [PAP] [EAP TLS] [EAP GTC] [EAP MSCHAPv2] [MSCHAP] [CHAP] | 2 |
| 5 | [EAP PEAP] | Default settings for EAP-PEAP | EAP-PEAP | [EAP MSCHAPv2] [EAP TLS] [EAP GTC] | 6 |
| 6 | [CHAP] | Default settings for CHAP | CHAP |  | 0 |
| 7 | [EAP MD5] | Default settings for EAP-MD5 | EAP-MD5 |  | 0 |
| 8 | [EAP MSCHAPv2] | Default settings for EAP-MSCHAPv2 | EAP-MSCHAPv2 |  | 1 |
| 9 | [EAP GTC] | Default settings for EAP-GTC | EAP-GTC |  | 1 |
| 10 | [EAP FAST] | Default settings for EAP-FAST | EAP-FAST | [EAP MSCHAPv2] [EAP GTC] [EAP TLS] | 19 |
| 11 | [MAC AUTH] | Default settings for MAC-AUTH | MAC-AUTH |  | 1 |
| 12 | [Allow All MAC AUTH] | Default settings for Allow All MAC-AUTH | MAC-AUTH |  | 1 |
| 13 | [EAP TLS With OCSP Enabled] | EAP-TLS with OCSP enabled; recommended for Onboard | EAP-TLS |  | 7 |
| 14 | [EAP PEAP Without Fast Reconnect] | EAP-PEAP with Fast Reconnect disabled; recommended for Onboard | EAP-PEAP | [EAP MSCHAPv2] [EAP TLS] [EAP GTC] | 6 |
| 15 | [Authorize] | Default settings for Authorize | Authorize |  | 0 |
| 16 | [SSO] | Default settings for SSO | PAP |  | 1 |
| 17 | [Aruba EAP GTC] | EAP-GTC method to use with Aruba EAP-GTC plugin for Windows | EAP-GTC |  | 1 |
| 20 | [EAP PEAP Public] | Default settings for EAP-PEAP-Public | EAP-PEAP-Public | [EAP MSCHAPv2] | 5 |
| 23 | [EAP PWD] | Default settings for EAP-PWD | EAP-PWD |  | 2 |
| 25 | [EAP TLS With CN Check] | EAP-TLS with Certificate Comparison configured to Compare Common Name (CN) | EAP-TLS |  | 6 |

Table - Authentication Method

The following section details Authentification Method configured on ClearPass.

### 1.4.2.1 Authentication Method: [PAP]

|  |  |
| --- | --- |
| Id | 1 |
| Name | [PAP] |
| Description | Default settings for PAP |
| Method Type | PAP |
| Inner Methods |  |

Table - Authentification Method: [PAP]

| Name | Value |
| --- | --- |
| encryption\_scheme | auto |

Table - Details : [PAP]

### 1.4.2.2 Authentication Method: [MSCHAP]

|  |  |
| --- | --- |
| Id | 2 |
| Name | [MSCHAP] |
| Description | Default settings for MSCHAP |
| Method Type | MSCHAP |
| Inner Methods |  |

Table - Authentification Method: [MSCHAP]

| Name | Value |
| --- | --- |
| pass\_reset\_flow | Challenge |

Table - Details : [MSCHAP]

### 1.4.2.3 Authentication Method: [EAP TLS]

|  |  |
| --- | --- |
| Id | 3 |
| Name | [EAP TLS] |
| Description | Default settings for EAP-TLS |
| Method Type | EAP-TLS |
| Inner Methods |  |

Table - Authentification Method: [EAP TLS]

| Name | Value |
| --- | --- |
| override\_cert\_url | false |
| ocsp\_enable | none |
| session\_cache\_enable | true |
| autz\_required | true |
| certificate\_comparison | none |
| session\_timeout | 6 |

Table - Details : [EAP TLS]

### 1.4.2.4 Authentication Method: [EAP TTLS]

|  |  |
| --- | --- |
| Id | 4 |
| Name | [EAP TTLS] |
| Description | Default settings for EAP-TTLS |
| Method Type | EAP-TTLS |
| Inner Methods | [PAP] [EAP TLS] [EAP GTC] [EAP MSCHAPv2] [MSCHAP] [CHAP] |

Table - Authentification Method: [EAP TTLS]

| Name | Value |
| --- | --- |
| session\_cache\_enable | true |
| session\_timeout | 6 |

Table - Details : [EAP TTLS]

### 1.4.2.5 Authentication Method: [EAP PEAP]

|  |  |
| --- | --- |
| Id | 5 |
| Name | [EAP PEAP] |
| Description | Default settings for EAP-PEAP |
| Method Type | EAP-PEAP |
| Inner Methods | [EAP MSCHAPv2] [EAP TLS] [EAP GTC] |

Table - Authentification Method: [EAP PEAP]

| Name | Value |
| --- | --- |
| allow\_fast\_reconnect | true |
| nap\_support\_enable | true |
| session\_cache\_enable | true |
| eap\_peap\_skip\_auth | false |
| session\_timeout | 6 |
| enforce\_crypto\_binding | none |

Table - Details : [EAP PEAP]

### 1.4.2.6 Authentication Method: [CHAP]

|  |  |
| --- | --- |
| Id | 6 |
| Name | [CHAP] |
| Description | Default settings for CHAP |
| Method Type | CHAP |
| Inner Methods |  |

Table - Authentification Method: [CHAP]

### 1.4.2.7 Authentication Method: [EAP MD5]

|  |  |
| --- | --- |
| Id | 7 |
| Name | [EAP MD5] |
| Description | Default settings for EAP-MD5 |
| Method Type | EAP-MD5 |
| Inner Methods |  |

Table - Authentification Method: [EAP MD5]

### 1.4.2.8 Authentication Method: [EAP MSCHAPv2]

|  |  |
| --- | --- |
| Id | 8 |
| Name | [EAP MSCHAPv2] |
| Description | Default settings for EAP-MSCHAPv2 |
| Method Type | EAP-MSCHAPv2 |
| Inner Methods |  |

Table - Authentification Method: [EAP MSCHAPv2]

| Name | Value |
| --- | --- |
| no\_of\_retries | 3 |

Table - Details : [EAP MSCHAPv2]

### 1.4.2.9 Authentication Method: [EAP GTC]

|  |  |
| --- | --- |
| Id | 9 |
| Name | [EAP GTC] |
| Description | Default settings for EAP-GTC |
| Method Type | EAP-GTC |
| Inner Methods |  |

Table - Authentification Method: [EAP GTC]

| Name | Value |
| --- | --- |
| challenge | Password: |

Table - Details : [EAP GTC]

### 1.4.2.10 Authentication Method: [EAP FAST]

|  |  |
| --- | --- |
| Id | 10 |
| Name | [EAP FAST] |
| Description | Default settings for EAP-FAST |
| Method Type | EAP-FAST |
| Inner Methods | [EAP MSCHAPv2] [EAP GTC] [EAP TLS] |

Table - Authentification Method: [EAP FAST]

| Name | Value |
| --- | --- |
| machine\_pac\_enable | true |
| machine\_pac\_lifetime | 1 |
| tunnel\_pac\_lifetime\_units | days |
| allow\_anonymous\_provisioning | true |
| posture\_pac\_enable | true |
| auth\_provisioning\_accept\_client | true |
| allow\_authenticated\_provisioning | true |
| posture\_pac\_lifetime | 1 |
| user\_auth\_pac\_lifetime | 1 |
| tunnel\_pac\_lifetime | 1 |
| user\_auth\_pac\_enable | true |
| user\_auth\_pac\_lifetime\_units | days |
| session\_cache\_enable | true |
| client\_certificate\_auth | false |
| posture\_pac\_lifetime\_units | days |
| machine\_pac\_lifetime\_units | days |
| auth\_provisioning\_require\_client\_cert | false |
| certificate\_comparison | none |
| session\_timeout | 6 |

Table - Details : [EAP FAST]

### 1.4.2.11 Authentication Method: [MAC AUTH]

|  |  |
| --- | --- |
| Id | 11 |
| Name | [MAC AUTH] |
| Description | Default settings for MAC-AUTH |
| Method Type | MAC-AUTH |
| Inner Methods |  |

Table - Authentification Method: [MAC AUTH]

| Name | Value |
| --- | --- |
| allow\_unknown\_clients | false |

Table - Details : [MAC AUTH]

### 1.4.2.12 Authentication Method: [Allow All MAC AUTH]

|  |  |
| --- | --- |
| Id | 12 |
| Name | [Allow All MAC AUTH] |
| Description | Default settings for Allow All MAC-AUTH |
| Method Type | MAC-AUTH |
| Inner Methods |  |

Table - Authentification Method: [Allow All MAC AUTH]

| Name | Value |
| --- | --- |
| allow\_unknown\_clients | true |

Table - Details : [Allow All MAC AUTH]

### 1.4.2.13 Authentication Method: [EAP TLS With OCSP Enabled]

|  |  |
| --- | --- |
| Id | 13 |
| Name | [EAP TLS With OCSP Enabled] |
| Description | EAP-TLS with OCSP enabled; recommended for Onboard |
| Method Type | EAP-TLS |
| Inner Methods |  |

Table - Authentification Method: [EAP TLS With OCSP Enabled]

| Name | Value |
| --- | --- |
| override\_cert\_url | true |
| ocsp\_enable | required |
| session\_cache\_enable | false |
| autz\_required | true |
| certificate\_comparison | none |
| session\_timeout | 6 |
| ocsp\_url | http://localhost/guest/mdps\_ocsp.php/1 |

Table - Details : [EAP TLS With OCSP Enabled]

### 1.4.2.14 Authentication Method: [EAP PEAP Without Fast Reconnect]

|  |  |
| --- | --- |
| Id | 14 |
| Name | [EAP PEAP Without Fast Reconnect] |
| Description | EAP-PEAP with Fast Reconnect disabled; recommended for Onboard |
| Method Type | EAP-PEAP |
| Inner Methods | [EAP MSCHAPv2] [EAP TLS] [EAP GTC] |

Table - Authentification Method: [EAP PEAP Without Fast Reconnect]

| Name | Value |
| --- | --- |
| allow\_fast\_reconnect | false |
| nap\_support\_enable | true |
| session\_cache\_enable | true |
| eap\_peap\_skip\_auth | false |
| session\_timeout | 6 |
| enforce\_crypto\_binding | none |

Table - Details : [EAP PEAP Without Fast Reconnect]

### 1.4.2.15 Authentication Method: [Authorize]

|  |  |
| --- | --- |
| Id | 15 |
| Name | [Authorize] |
| Description | Default settings for Authorize |
| Method Type | Authorize |
| Inner Methods |  |

Table - Authentification Method: [Authorize]

### 1.4.2.16 Authentication Method: [SSO]

|  |  |
| --- | --- |
| Id | 16 |
| Name | [SSO] |
| Description | Default settings for SSO |
| Method Type | PAP |
| Inner Methods |  |

Table - Authentification Method: [SSO]

| Name | Value |
| --- | --- |
| encryption\_scheme | sso |

Table - Details : [SSO]

### 1.4.2.17 Authentication Method: [Aruba EAP GTC]

|  |  |
| --- | --- |
| Id | 17 |
| Name | [Aruba EAP GTC] |
| Description | EAP-GTC method to use with Aruba EAP-GTC plugin for Windows |
| Method Type | EAP-GTC |
| Inner Methods |  |

Table - Authentification Method: [Aruba EAP GTC]

| Name | Value |
| --- | --- |
| challenge | Enter Aruba Login |

Table - Details : [Aruba EAP GTC]

### 1.4.2.18 Authentication Method: [EAP PEAP Public]

|  |  |
| --- | --- |
| Id | 20 |
| Name | [EAP PEAP Public] |
| Description | Default settings for EAP-PEAP-Public |
| Method Type | EAP-PEAP-Public |
| Inner Methods | [EAP MSCHAPv2] |

Table - Authentification Method: [EAP PEAP Public]

| Name | Value |
| --- | --- |
| allow\_fast\_reconnect | true |
| public\_username | public |
| session\_cache\_enable | true |
| public\_password | public |
| session\_timeout | 6 |

Table - Details : [EAP PEAP Public]

### 1.4.2.19 Authentication Method: [EAP PWD]

|  |  |
| --- | --- |
| Id | 23 |
| Name | [EAP PWD] |
| Description | Default settings for EAP-PWD |
| Method Type | EAP-PWD |
| Inner Methods |  |

Table - Authentification Method: [EAP PWD]

| Name | Value |
| --- | --- |
| group\_name | 256-bit random ECP group |
| server\_id | CPPM |

Table - Details : [EAP PWD]

### 1.4.2.20 Authentication Method: [EAP TLS With CN Check]

|  |  |
| --- | --- |
| Id | 25 |
| Name | [EAP TLS With CN Check] |
| Description | EAP-TLS with Certificate Comparison configured to Compare Common Name (CN) |
| Method Type | EAP-TLS |
| Inner Methods |  |

Table - Authentification Method: [EAP TLS With CN Check]

| Name | Value |
| --- | --- |
| override\_cert\_url | false |
| ocsp\_enable | none |
| session\_cache\_enable | true |
| autz\_required | true |
| session\_timeout | 6 |
| certificate\_comparison | cn |

Table - Details : [EAP TLS With CN Check]

### 1.4.3 Authentication Source

The following section details Authentication Source configured on ClearPass.

| Id | Name | Description | Type | Authorization |
| --- | --- | --- | --- | --- |
| 1 | [Local User Repository] | Authenticate users against Policy Manager local user database | Local | True |
| 2 | [Guest User Repository] | Authenticate guest users against Policy Manager local database | Local | True |
| 3 | [Guest Device Repository] | Authenticate guest devices against Policy Manager local database | Local | True |
| 4 | [Endpoints Repository] | Authenticate endpoints against Policy Manager local database | Local | True |
| 5 | [Onboard Devices Repository] | Authenticate Onboard devices against Policy Manager local database | Local | True |
| 6 | [Admin User Repository] | Authenticate users against Policy Manager admin user database | Local | True |
| 7 | [Denylist User Repository] | Denylist database with users who have exceeded bandwidth or session related limits | Local | True |
| 8 | [Insight Repository] | Insight database with session information for users and devices | Local | True |
| 9 | [Time Source] | Authorization source for implementing various time functions | Local | True |
| 10 | [Social Login Repository] | Authenticate users against Policy Manager social login database | Local | True |
| 100 | [Zone Cache Repository] | Access attributes cached by Context Server Actions in previous sessions | HTTP | True |
| 3002 | AD-arubalab.loc | Active Directory LDAPS | AD | True |
| 3004 | CarbonBlack-HTTP |  | HTTP | True |
| 3006 | AD-arubalab.loc-deep-nested | AD with deep nested groups https://www.arubanetworks.com/techdocs/ClearPass/6.9/PolicyManager/Content/CPPM\_UserGuide/Enforce/Enforce\_policy\_rapid\_LDAP\_queries.htm?Highlight=nested%20groups | AD | True |
| 3007 | AD-arubalab.loc-NestedDN | Active Directory LDAPS | AD | True |
| 3008 | AD-arubalab.loc-UPN | Active Directory LDAPS for demo UPN | AD | True |

Table - Authentication Source

The following section details Authentification Source configured on ClearPass.

### 1.4.3.1 Authentication Source: [Local User Repository]

|  |  |
| --- | --- |
| Id | 1 |
| Name | [Local User Repository] |
| Description | Authenticate users against Policy Manager local user database |
| Type | Local |
| Authorization | True |

Table - Authentification Source: [Local User Repository]

| Name | Query | Attribute |
| --- | --- | --- |
| Authentication | SELECT user\_credential(password) AS User\_Password, user\_credential(password\_hash) AS Password\_Hash,  user\_credential(password\_ntlm\_hash) AS Password\_Ntlm\_Hash,  CASE WHEN enabled = FALSE THEN 225  WHEN ((expire\_time is not null AND expire\_time <= now()) OR (passwordPolicy.expiry\_days > 0 AND  (PASSWORD\_UPDATED\_AT <= (now() - interval '1 days' \* passwordPolicy.expiry\_days))) ) THEN 226  ELSE 0  END AS Account\_Status,  tips\_role.name as Role\_Name,  case when enabled=true then 'true' else 'false' end as enabled,  row\_to\_json((SELECT d FROM (SELECT  CASE WHEN extract(DAY FROM (age(password\_updated\_at)))+1 >= passwordPolicy.pwd\_reminder\_days THEN passwordPolicy.pwd\_reminder\_text ELSE '' END AS Show\_Message,  CASE WHEN tips\_auth\_local\_users.change\_pwd\_next\_login = TRUE THEN 'true'  ELSE '' END AS Change\_Password)d )) as Account\_Actions  FROM tips\_auth\_local\_users JOIN tips\_role ON  (tips\_auth\_local\_users.user\_role = tips\_role.id), password\_policy passwordPolicy WHERE  passwordPolicy.usertype='LOCAL\_USERS' AND user\_id = '%{Authentication:Username}' | role\_name enabled |

Table - Auth Source Filters : [Local User Repository]

### 1.4.3.2 Authentication Source: [Guest User Repository]

|  |  |
| --- | --- |
| Id | 2 |
| Name | [Guest User Repository] |
| Description | Authenticate guest users against Policy Manager local database |
| Type | Local |
| Authorization | True |

Table - Authentification Source: [Guest User Repository]

| Name | Query | Attribute |
| --- | --- | --- |
| Authentication | SELECT user\_credential(password) AS User\_Password,  CASE WHEN enabled = FALSE THEN 225  WHEN ((start\_time > now()) OR ((expire\_time is not null) AND (expire\_time <= now()))) THEN 226  WHEN approval\_status != 'Approved' THEN 227  ELSE 0  END AS Account\_Status, sponsor\_name,  CASE WHEN expire\_time > now() THEN CAST(EXTRACT(epoch FROM (expire\_time - NOW())) AS INTEGER)  ELSE 0  END AS remaining\_expiration, expire\_time::timestamp FROM tips\_guest\_users WHERE ((guest\_type = 'USER') AND (user\_id = '%{Authentication:Username}') AND (app\_name != 'Onboard')) | sponsor\_name remaining\_expiration expire\_time |
| Authorization | SELECT  CASE WHEN expire\_time is null or expire\_time > now() THEN 'false'  ELSE 'true'  END AS is\_expired,  CASE WHEN enabled = true THEN 'true' ELSE 'false' END as is\_enabled FROM tips\_guest\_users WHERE ((guest\_type = 'USER') AND (user\_id = '%{Endpoint:Username}') AND (app\_name != 'Onboard')) | is\_expired is\_enabled |

Table - Auth Source Filters : [Guest User Repository]

### 1.4.3.3 Authentication Source: [Guest Device Repository]

|  |  |
| --- | --- |
| Id | 3 |
| Name | [Guest Device Repository] |
| Description | Authenticate guest devices against Policy Manager local database |
| Type | Local |
| Authorization | True |

Table - Authentification Source: [Guest Device Repository]

| Name | Query | Attribute |
| --- | --- | --- |
| Authentication | SELECT user\_credential(password) AS User\_Password,  CASE WHEN enabled = FALSE THEN 225  WHEN ((expire\_time is not null AND expire\_time <= now())) THEN 226  ELSE 0  END AS Account\_Status, sponsor\_name,  CASE WHEN expire\_time > now() THEN CAST(EXTRACT(epoch FROM (expire\_time - NOW())) AS INTEGER)  ELSE 0  END AS remaining\_expiration FROM tips\_guest\_users WHERE ((guest\_type = 'DEVICE') AND (user\_id = '%{Connection:Client-Mac-Address-Hyphen}')) | sponsor\_name remaining\_expiration account\_status |
| Device Role ID | SELECT tgu.attributes->>'Role ID' AS device\_role\_id FROM tips\_guest\_users as tgu WHERE tgu.guest\_type = 'DEVICE' AND tgu.user\_id = '%{Connection:Client-Mac-Address-Hyphen}' | device\_role\_id |
| Device MPSK | SELECT user\_credential(tgu.attributes->>'mpsk') AS device\_mpsk FROM tips\_guest\_users as tgu WHERE tgu.guest\_type = 'DEVICE' AND tgu.user\_id = '%{Connection:Client-Mac-Address-Hyphen}' | device\_mpsk |
| Authorization | SELECT   CASE WHEN expire\_time is null or expire\_time > now() THEN 'false'   ELSE 'true'  END AS is\_expired,  CASE WHEN enabled = true THEN 'true' ELSE 'false' END as is\_enabled,  CASE WHEN (expire\_time is null or expire\_time > now()) and (start\_time < now()) and (enabled = true) THEN 'true' ELSE 'false' END as is\_active FROM tips\_guest\_users  WHERE ((guest\_type = 'DEVICE') AND (user\_id = '%{Connection:Client-Mac-Address-Upper-Hyphen}') AND (app\_name = 'Guest')) | is\_expired is\_enabled is\_active |

Table - Auth Source Filters : [Guest Device Repository]

### 1.4.3.4 Authentication Source: [Endpoints Repository]

|  |  |
| --- | --- |
| Id | 4 |
| Name | [Endpoints Repository] |
| Description | Authenticate endpoints against Policy Manager local database |
| Type | Local |
| Authorization | True |

Table - Authentification Source: [Endpoints Repository]

| Name | Query | Attribute |
| --- | --- | --- |
| Authentication | SELECT mac\_address AS User\_Password FROM tips\_endpoints WHERE mac\_address = LOWER('%{Connection:Client-Mac-Address-NoDelim}') AND status = 'Known' |  |
| Status | SELECT t1.status,t1.mac\_vendor, (case when t2.device\_family is NULL then 'false' else 'true' end) as is\_profiled FROM tips\_endpoints t1 LEFT OUTER JOIN tips\_endpoint\_profiles t2 ON (t1.mac\_address = t2.mac) WHERE t1.mac\_address = LOWER('%{Connection:Client-Mac-Address-NoDelim}') | status mac\_vendor is\_profiled |
| Profile | SELECT hostname,(case when static\_ip is false then 'false' else 'true' end) as static\_ip, device\_category, device\_family, device\_name, other\_category, other\_family, other\_name, (case when conflict is false then 'false' else 'true' end) as conflict FROM tips\_endpoint\_profiles WHERE mac = LOWER('%{Connection:Client-Mac-Address-NoDelim}') | hostname static\_ip device\_category device\_family device\_name other\_category other\_family other\_name conflict |
| Fingerprint | SELECT fingerprint, CAST(fingerprint as jsonb)->'host'->>'app\_id' as app\_id, CAST(fingerprint as jsonb)->'host'->>'app\_group' as app\_group, CAST(fingerprint as jsonb)->'host'->>'user\_agent' as user\_agent, CAST(fingerprint as jsonb)->'host'->>'dst\_conns' as dst\_conns, CAST(fingerprint as jsonb)->'host'->>'ports' as open\_port,CAST(fingerprint as jsonb)->'nmap'->>'device' as nmap\_device\_name, CAST(fingerprint as jsonb)->'nmap'->>'os\_family' as nmap\_device\_family, CAST(fingerprint as jsonb)->'nmap'->>'os\_type' as nmap\_device\_type, CAST(fingerprint as jsonb)->'nmap'->>'os\_vendor' as nmap\_device\_vendor, CAST(fingerprint as jsonb)->'nmap'->>'os\_gen' as nmap\_device\_os\_version FROM tips\_endpoint\_profiles WHERE mac = LOWER('%{Connection:Client-Mac-Address-NoDelim}') | app\_id app\_group user\_agent dst\_conns open\_port nmap\_device\_name nmap\_device\_type nmap\_device\_family nmap\_device\_vendor nmap\_device\_os\_version fingerprint |
| MAC Caching | SELECT COUNT(te.id) + 1 AS num\_endpoints FROM tips\_endpoints as te WHERE LOWER( te.attributes->>'Username') = LOWER( '%{Authentication:Username}') and te.mac\_address != '%{Connection:Client-Mac-Address-NoDelim}' | num\_endpoints |

Table - Auth Source Filters : [Endpoints Repository]

### 1.4.3.5 Authentication Source: [Onboard Devices Repository]

|  |  |
| --- | --- |
| Id | 5 |
| Name | [Onboard Devices Repository] |
| Description | Authenticate Onboard devices against Policy Manager local database |
| Type | Local |
| Authorization | True |

Table - Authentification Source: [Onboard Devices Repository]

| Name | Query | Attribute |
| --- | --- | --- |
| Authentication | SELECT user\_credential(password) AS User\_Password,  CASE WHEN enabled = FALSE THEN 225  WHEN ((start\_time > now()) OR ((expire\_time is not null) AND (expire\_time <= now()))) THEN 226  WHEN approval\_status != 'Approved' THEN 227  ELSE 0  END AS Account\_Status, sponsor\_name FROM tips\_guest\_users WHERE ((guest\_type = 'USER') AND (user\_id = mdps\_username\_to\_serial('%{Authentication:Username}')::text) AND (app\_name = 'Onboard')) | sponsor\_name |

Table - Auth Source Filters : [Onboard Devices Repository]

### 1.4.3.6 Authentication Source: [Admin User Repository]

|  |  |
| --- | --- |
| Id | 6 |
| Name | [Admin User Repository] |
| Description | Authenticate users against Policy Manager admin user database |
| Type | Local |
| Authorization | True |

Table - Authentification Source: [Admin User Repository]

| Name | Query | Attribute |
| --- | --- | --- |
| Authentication | SELECT user\_credential(password\_hash) AS Password\_Hash,  user\_credential(password\_ntlm\_hash) AS Password\_Ntlm\_Hash,  CASE WHEN enabled = FALSE THEN 225  WHEN (passwordPolicy.expiry\_days > 0 AND (PASSWORD\_UPDATED\_AT <= (now() - interval '1 days' \* passwordPolicy.expiry\_days)))  THEN 226 ELSE 0 END AS Account\_Status,  tips\_admin\_user\_group.name AS Role\_Name  FROM tips\_admin\_user  JOIN tips\_admin\_user\_group ON (tips\_admin\_user.group\_id = tips\_admin\_user\_group.id), password\_policy passwordPolicy  WHERE passwordPolicy.usertype='ADMIN\_USERS' AND user\_id = '%{Authentication:Username}' | role\_name |

Table - Auth Source Filters : [Admin User Repository]

### 1.4.3.7 Authentication Source: [Denylist User Repository]

|  |  |
| --- | --- |
| Id | 7 |
| Name | [Denylist User Repository] |
| Description | Denylist database with users who have exceeded bandwidth or session related limits |
| Type | Local |
| Authorization | True |

Table - Authentification Source: [Denylist User Repository]

| Name | Query | Attribute |
| --- | --- | --- |
| Lookup | SELECT 'password' as user\_password,  CASE WHEN bandwidth\_limit\_exceed = TRUE THEN 228  WHEN session\_duration\_exceed = TRUE THEN 229  WHEN session\_count\_exceed = TRUE THEN 230  END AS Account\_Status FROM tips\_post\_auth\_enf\_log WHERE user\_id = '%{Authentication:Username}' order by timestamp desc limit 1 |  |

Table - Auth Source Filters : [Denylist User Repository]

### 1.4.3.8 Authentication Source: [Insight Repository]

|  |  |
| --- | --- |
| Id | 8 |
| Name | [Insight Repository] |
| Description | Insight database with session information for users and devices |
| Type | Local |
| Authorization | True |

Table - Authentification Source: [Insight Repository]

| Name | Query | Attribute |
| --- | --- | --- |
| WebAuth Check | SELECT 'True' AS status FROM auth WHERE  (mac = '%{Connection:Client-Mac-Address-NoDelim}') AND  (protocol = 'WEBAUTH') AND  (timestamp BETWEEN (now() - interval '10 days') AND now()) limit 1 | status |
| MAC Caching | SELECT FLOOR(EXTRACT(EPOCH FROM (NOW() - user\_auth\_at)))::integer AS seconds\_since\_auth, FLOOR((EXTRACT(EPOCH FROM (NOW() - user\_auth\_at)))/60)::integer AS minutes\_since\_auth, FLOOR((EXTRACT(EPOCH FROM (NOW() - user\_auth\_at)))/3600)::integer AS hours\_since\_auth, FLOOR((EXTRACT(EPOCH FROM (NOW() - user\_auth\_at)))/86400)::integer AS days\_since\_auth FROM endpoints WHERE endpoints.user\_auth\_at < NOW() AND endpoints.username = '%{Endpoint:Username}' AND endpoints.mac = '%{Connection:Client-Mac-Address-NoDelim}' | seconds\_since\_auth minutes\_since\_auth hours\_since\_auth days\_since\_auth |
| Successful Login count since midnight | SELECT COUNT(\*) AS login\_count FROM auth WHERE error\_code = 0 AND username = '%{Authentication:Username}' AND auth.auth\_status != 'MAB' AND timestamp BETWEEN date\_trunc('day', NOW()) AND date\_trunc('day', NOW() + INTERVAL '1 day'); | login\_count |
| Active Sessions | SELECT COUNT(\*) AS active\_count FROM radius\_acct WHERE (username = '%{Authentication:Username}' OR calling\_station\_id = '%{Connection:Client-Mac-Address-NoDelim}') AND start\_time >= NOW() - INTERVAL '2 day' AND end\_time is NULL; | active\_count |
| Online Status | SELECT end\_time IS null AS online FROM radius\_acct WHERE calling\_station\_id = '%{Connection:Client-Mac-Address-NoDelim}' AND start\_time >= NOW() - INTERVAL '2 day' ORDER BY updated\_at DESC LIMIT 1; | online |
| Daily duration | SELECT sum(duration) as daily\_duration from radius\_acct WHERE calling\_station\_id = '%{Connection:Client-Mac-Address-NoDelim}' AND start\_time >= NOW() - INTERVAL '1 day' ; | daily\_duration |
| Weekly duration | SELECT sum(duration) as weekly\_duration from radius\_acct WHERE calling\_station\_id = '%{Connection:Client-Mac-Address-NoDelim}' AND start\_time >= NOW() - INTERVAL '1 week'; | weekly\_duration |
| Monthly duration | SELECT sum(duration) as monthly\_duration from radius\_acct WHERE calling\_station\_id = '%{Connection:Client-Mac-Address-NoDelim}' AND start\_time >= NOW() - INTERVAL '1 month'; | monthly\_duration |
| Daily duration by username | SELECT sum(duration) as daily\_duration\_by\_username from radius\_acct WHERE (username = '%{Authentication:Username}' OR calling\_station\_id = '%{Connection:Client-Mac-Address-NoDelim}') AND start\_time >= NOW() - INTERVAL '1 day' ; | daily\_duration\_by\_username |
| Weekly duration by username | SELECT sum(duration) as weekly\_duration\_by\_username from radius\_acct WHERE (username = '%{Authentication:Username}' OR calling\_station\_id = '%{Connection:Client-Mac-Address-NoDelim}') AND start\_time >= NOW() - INTERVAL '1 week'; | weekly\_duration\_by\_username |
| Monthly duration by username | SELECT sum(duration) as monthly\_duration\_by\_username from radius\_acct WHERE (username = '%{Authentication:Username}' OR calling\_station\_id = '%{Connection:Client-Mac-Address-NoDelim}') AND start\_time >= NOW() - INTERVAL '1 month'; | monthly\_duration\_by\_username |

Table - Auth Source Filters : [Insight Repository]

### 1.4.3.9 Authentication Source: [Time Source]

|  |  |
| --- | --- |
| Id | 9 |
| Name | [Time Source] |
| Description | Authorization source for implementing various time functions |
| Type | Local |
| Authorization | True |

Table - Authentification Source: [Time Source]

| Name | Query | Attribute |
| --- | --- | --- |
| Current Time | SELECT (EXTRACT (EPOCH FROM NOW()))::int AS now; | now |
| Next 2 hours | SELECT (EXTRACT (EPOCH FROM NOW() + interval '2 hours'))::int AS now\_plus\_2hrs; | now\_plus\_2hrs |
| One Day | SELECT (EXTRACT (EPOCH FROM NOW() + interval '1 days'))::int AS now\_plus\_1day; | now\_plus\_1day |
| Seven Days | SELECT (EXTRACT (EPOCH FROM NOW() + interval '7 days'))::int AS now\_plus\_7days; | now\_plus\_7days |
| Current Time MS | SELECT ((EXTRACT (EPOCH FROM NOW()) + 11644473600) \* 10000000)::bigint AS now\_ms\_time; | now\_ms\_time |
| Date Time | select date\_trunc('hour', localtimestamp(0)) as today, date\_trunc('hour', localtimestamp(0)+ interval '1 days') as one\_day, date\_trunc('hour', localtimestamp(0)+interval '1 week') as one\_week, date\_trunc('hour', localtimestamp(0)+ interval '1 month') as one\_month, date\_trunc('hour', localtimestamp(0)+ interval '6 months') as six\_months | today one\_day one\_week one\_month six\_months ninety\_days |

Table - Auth Source Filters : [Time Source]

### 1.4.3.10 Authentication Source: [Social Login Repository]

|  |  |
| --- | --- |
| Id | 10 |
| Name | [Social Login Repository] |
| Description | Authenticate users against Policy Manager social login database |
| Type | Local |
| Authorization | True |

Table - Authentification Source: [Social Login Repository]

| Name | Query | Attribute |
| --- | --- | --- |
| Authentication | SELECT te.attributes->>'social\_password' AS User\_Password FROM tips\_endpoints as te WHERE te.mac\_address = LOWER('%{Connection:Client-Mac-Address-NoDelim}') and jsonb\_exists\_all(te.attributes, '{social\_password}') |  |
| Social | SELECT te.attributes->>'social\_method' AS SP FROM tips\_endpoints as te WHERE te.mac\_address = LOWER('%{Connection:Client-Mac-Address-NoDelim}') and jsonb\_exists\_all(te.attributes, '{social\_method}') | SP |

Table - Auth Source Filters : [Social Login Repository]

### 1.4.3.11 Authentication Source: [Zone Cache Repository]

|  |  |
| --- | --- |
| Id | 100 |
| Name | [Zone Cache Repository] |
| Description | Access attributes cached by Context Server Actions in previous sessions |
| Type | HTTP |
| Authorization | True |

Table - Authentification Source: [Zone Cache Repository]

| Name | Query | Attribute |
| --- | --- | --- |
| Example | /policyresult/%{Connection:Client-Mac-Address-NoDelim} | username |

Table - Auth Source Filters : [Zone Cache Repository]

| Name | Value |
| --- | --- |
| login\_user\_name | admin |
| timeout | 60 |
| base\_URL | http://localhost/battery/buckets |

Table - Primary Auth Source Connection Details : [Zone Cache Repository]

### 1.4.3.12 Authentication Source: AD-arubalab.loc

|  |  |
| --- | --- |
| Id | 3002 |
| Name | AD-arubalab.loc |
| Description | Active Directory LDAPS |
| Type | AD |
| Authorization | True |

Table - Authentification Source: AD-arubalab.loc

| Name | Query | Attribute |
| --- | --- | --- |
| Authentication | (&(|(sAMAccountName=%{Authentication:Username})(mail=%{Authentication:Username}))(objectClass=user)) | dn department title company memberOf telephoneNumber mail displayName accountExpires |
| Group | (distinguishedName=%{memberOf}) | cn |
| Machine | (&(sAMAccountName=%{Host:Name}$)(objectClass=computer)) | dNSHostName operatingSystem operatingSystemServicePack |
| Onboard Device Owner | (&(sAMAccountName=%{Onboard:Owner})(objectClass=user)) | memberOf |
| Onboard Device Owner Group | (distinguishedName=%{Onboard memberOf}) | cn |

Table - Auth Source Filters : AD-arubalab.loc

| Name | Value |
| --- | --- |
| host\_name | dc01.arubalab.loc |
| connection\_security | AD\_Over\_SSL |
| connection\_port | 636 |
| bind\_DN | svc\_clearpass@arubalab.loc |
| bind\_password | ANONYMISED |
| verify\_server\_certificate | True |
| net\_BIOS\_domain\_name | ARUBALAB |
| base\_DN | dc=arubalab,dc=loc |
| search\_scope | SubTree\_Search |
| bind\_user | True |
| user\_certificate | userCertificate |
| replace\_special\_char | True |

Table - Primary Auth Source Connection Details : AD-arubalab.loc

### 1.4.3.13 Authentication Source: CarbonBlack-HTTP

|  |  |
| --- | --- |
| Id | 3004 |
| Name | CarbonBlack-HTTP |
| Description |  |
| Type | HTTP |
| Authorization | True |

Table - Authentification Source: CarbonBlack-HTTP

| Name | Query | Attribute |
| --- | --- | --- |
| cb-response | ?macAddress=%{Connection:Client-Mac-Address-Hyphen} | isFound id status last\_checkin\_time build\_version\_string os\_environment\_display\_string computer\_dns\_name registration\_time totalAlerts sensor\_health\_status sensor\_health\_message |

Table - Auth Source Filters : CarbonBlack-HTTP

| Name | Value |
| --- | --- |
| login\_user\_name | admin |
| login\_password | ANONYMISED |
| timeout | 60 |
| base\_URL | http://172.17.0.2 |

Table - Primary Auth Source Connection Details : CarbonBlack-HTTP

### 1.4.3.14 Authentication Source: AD-arubalab.loc-deep-nested

|  |  |
| --- | --- |
| Id | 3006 |
| Name | AD-arubalab.loc-deep-nested |
| Description | AD with deep nested groups https://www.arubanetworks.com/techdocs/ClearPass/6.9/PolicyManager/Content/CPPM\_UserGuide/Enforce/Enforce\_policy\_rapid\_LDAP\_queries.htm?Highlight=nested%20groups |
| Type | AD |
| Authorization | True |

Table - Authentification Source: AD-arubalab.loc-deep-nested

| Name | Query | Attribute |
| --- | --- | --- |
| Authentication | (&(|(sAMAccountName=%{Authentication:Username})(mail=%{Authentication:Username}))(objectClass=user)) | dn department title company memberOf telephoneNumber mail displayName accountExpires |
| Group | (distinguishedName=%{memberOf}) | cn |
| Machine | (&(sAMAccountName=%{Host:Name}$)(objectClass=computer)) | dNSHostName operatingSystem operatingSystemServicePack |
| Onboard Device Owner | (&(sAMAccountName=%{Onboard:Owner})(objectClass=user)) | memberOf |
| Onboard Device Owner Group | (distinguishedName=%{Onboard memberOf}) | cn |
| Nested-SIDs | (&(objectClass=user)(sAMAccountName=%{Authentication:Username})) | tokenGroups |

Table - Auth Source Filters : AD-arubalab.loc-deep-nested

| Name | Value |
| --- | --- |
| host\_name | dc01.arubalab.loc |
| connection\_security | AD\_Over\_SSL |
| connection\_port | 636 |
| bind\_DN | svc\_clearpass@arubalab.loc |
| bind\_password | ANONYMISED |
| verify\_server\_certificate | True |
| net\_BIOS\_domain\_name | ARUBALAB |
| base\_DN | dc=arubalab,dc=loc |
| search\_scope | SubTree\_Search |
| bind\_user | True |
| user\_certificate | userCertificate |
| replace\_special\_char | True |

Table - Primary Auth Source Connection Details : AD-arubalab.loc-deep-nested

### 1.4.3.15 Authentication Source: AD-arubalab.loc-NestedDN

|  |  |
| --- | --- |
| Id | 3007 |
| Name | AD-arubalab.loc-NestedDN |
| Description | Active Directory LDAPS |
| Type | AD |
| Authorization | True |

Table - Authentification Source: AD-arubalab.loc-NestedDN

| Name | Query | Attribute |
| --- | --- | --- |
| Authentication | (&(|(sAMAccountName=%{Authentication:Username})(mail=%{Authentication:Username}))(objectClass=user)) | dn department title company memberOf telephoneNumber mail displayName accountExpires |
| Group | (distinguishedName=%{memberOf}) | cn |
| Machine | (&(sAMAccountName=%{Host:Name}$)(objectClass=computer)) | dNSHostName operatingSystem operatingSystemServicePack |
| Onboard Device Owner | (&(sAMAccountName=%{Onboard:Owner})(objectClass=user)) | memberOf |
| Onboard Device Owner Group | (distinguishedName=%{Onboard memberOf}) | cn |
| All Groups | (member:1.2.840.113556.1.4.1941:=%{UserDN}) | cn distinguishedName |

Table - Auth Source Filters : AD-arubalab.loc-NestedDN

| Name | Value |
| --- | --- |
| host\_name | dc01.arubalab.loc |
| connection\_security | AD\_Over\_SSL |
| connection\_port | 636 |
| bind\_DN | svc\_clearpass@arubalab.loc |
| bind\_password | ANONYMISED |
| verify\_server\_certificate | True |
| net\_BIOS\_domain\_name | ARUBALAB |
| base\_DN | dc=arubalab,dc=loc |
| search\_scope | SubTree\_Search |
| bind\_user | True |
| user\_certificate | userCertificate |
| replace\_special\_char | True |

Table - Primary Auth Source Connection Details : AD-arubalab.loc-NestedDN

### 1.4.3.16 Authentication Source: AD-arubalab.loc-UPN

|  |  |
| --- | --- |
| Id | 3008 |
| Name | AD-arubalab.loc-UPN |
| Description | Active Directory LDAPS for demo UPN |
| Type | AD |
| Authorization | True |

Table - Authentification Source: AD-arubalab.loc-UPN

| Name | Query | Attribute |
| --- | --- | --- |
| Authentication | (&(|(sAMAccountName=%{Authentication:Username})(userPrincipalName=%{Authentication:Username}))(objectClass=user)) | dn department title company memberOf telephoneNumber mail displayName accountExpires |
| Group | (distinguishedName=%{memberOf}) | cn |
| Machine | (&(sAMAccountName=%{Host:Name}$)(objectClass=computer)) | dNSHostName operatingSystem operatingSystemServicePack |
| Onboard Device Owner | (&(sAMAccountName=%{Onboard:Owner})(objectClass=user)) | memberOf |
| Onboard Device Owner Group | (distinguishedName=%{Onboard memberOf}) | cn |

Table - Auth Source Filters : AD-arubalab.loc-UPN

| Name | Value |
| --- | --- |
| host\_name | dc01.arubalab.loc |
| connection\_security | AD\_Over\_SSL |
| connection\_port | 636 |
| bind\_DN | svc\_clearpass@arubalab.loc |
| bind\_password | ANONYMISED |
| verify\_server\_certificate | True |
| net\_BIOS\_domain\_name | ARUBALAB |
| base\_DN | dc=arubalab,dc=loc |
| search\_scope | SubTree\_Search |
| bind\_user | True |
| user\_certificate | userCertificate |
| replace\_special\_char | True |

Table - Primary Auth Source Connection Details : AD-arubalab.loc-UPN

## 1.5 Certificate

The following section details Certificate settings configured on ClearPass.

### 1.5.1 Server Certificate

The following section provides a summary of Certificate settings.

| Id | Service Name | Subject | Issue Date | Expiry Date | Validity | Enable |
| --- | --- | --- | --- | --- | --- | --- |
| 7 | HTTPS(RSA) | O=PolicyManager, CN=ALG-CPPM-612 | Dec 08, 2023 11:12:21 CET | Dec 07, 2024 11:12:21 CET | Valid | True |
| 2 | HTTPS(ECC) | O=PolicyManager, CN=ALG-CPPM-612 | Dec 08, 2023 11:12:21 CET | Dec 07, 2024 11:12:21 CET | Valid | True |
| 1 | RADIUS | O=PolicyManager, CN=ALG-CPPM-612 | Dec 08, 2023 11:12:21 CET | Dec 07, 2024 11:12:21 CET | Valid | True |
| 21 | RadSec | O=PolicyManager, CN=ALG-CPPM-612 | Dec 08, 2023 11:12:21 CET | Dec 07, 2024 11:12:21 CET | Valid | True |
| 106 | Database | O=PolicyManager, CN=ALG-CPPM-612 | Dec 08, 2023 11:12:21 CET | Dec 07, 2028 11:12:21 CET | Valid | True |

Table - Certificate ALG-CPPM-612

### 1.5.2 Certificate Trust List Summary

The following section provides a summary of Certificate Trusted List settings.

|  |  |
| --- | --- |
| Certificate Trust List | 61 |
| Certificate Trust List (Enabled) | 24 |

Table - Certificate Summary

### 1.5.3 Certificate Trust List Detail

The following section details Certificate Trust List configured on ClearPass.

| Id | Subject DN | Issue Date | Expiry Date | Enable | Valid | Usage |
| --- | --- | --- | --- | --- | --- | --- |
| 2001 | CN=Certum CA,O=Unizeto Sp. z o.o.,C=PL | 2002/06/11 12:46:39 | 2027/06/11 12:46:39 | False | valid | Others |
| 2002 | CN=GlobalSign Root CA,OU=Root CA,O=GlobalSign nv-sa,C=BE | 1998/09/01 14:00:00 | 2028/01/28 13:00:00 | False | valid | Others |
| 2003 | OU=Go Daddy Class 2 Certification Authority,O=The Go Daddy Group\, Inc.,C=US | 2004/06/29 19:06:20 | 2034/06/29 19:06:20 | True | valid | AD/LDAP Servers, Aruba Services, Endpoint Context Servers, SAML, SMTP, Others |
| 2004 | CN=SecureTrust CA,O=SecureTrust Corporation,C=US | 2006/11/07 20:31:18 | 2029/12/31 20:40:55 | False | valid | Others |
| 2005 | CN=TC TrustCenter Universal CA I,OU=TC TrustCenter Universal CA,O=TC TrustCenter GmbH,C=DE | 2006/03/22 16:54:28 | 2025/12/31 23:59:59 | False | valid | Others |
| 2006 | CN=thawte Primary Root CA,OU=(c) 2006 thawte\, Inc. - For authorized use only,OU=Certification Services Division,O=thawte\, Inc.,C=US | 2006/11/17 01:00:00 | 2036/07/17 01:59:59 | False | valid | Others |
| 2007 | CN=VeriSign Class 1 Public Primary Certification Authority - G3,OU=(c) 1999 VeriSign\, Inc. - For authorized use only,OU=VeriSign Trust Network,O=VeriSign\, Inc.,C=US | 1999/10/01 02:00:00 | 2036/07/17 01:59:59 | True | valid | AD/LDAP Servers, Aruba Services, Endpoint Context Servers, SAML, SMTP, Others |
| 2008 | CN=VeriSign Class 3 Public Primary Certification Authority - G3,OU=(c) 1999 VeriSign\, Inc. - For authorized use only,OU=VeriSign Trust Network,O=VeriSign\, Inc.,C=US | 1999/10/01 02:00:00 | 2036/07/17 01:59:59 | False | valid | Others |
| 2009 | CN=VeriSign Class 3 Public Primary Certification Authority - G5,OU=(c) 2006 VeriSign\, Inc. - For authorized use only,OU=VeriSign Trust Network,O=VeriSign\, Inc.,C=US | 2006/11/08 01:00:00 | 2036/07/17 01:59:59 | False | valid | Others |
| 2010 | OU=VeriSign Trust Network,OU=(c) 1998 VeriSign\, Inc. - For authorized use only,OU=Class 3 Public Primary Certification Authority - G2,O=VeriSign\, Inc.,C=US | 1998/05/18 02:00:00 | 2028/08/02 01:59:59 | False | valid | Others |
| 2011 | OU=Class 3 Public Primary Certification Authority,O=VeriSign\, Inc.,C=US | 1996/01/29 01:00:00 | 2028/08/03 01:59:59 | False | valid | Others |
| 2012 | CN=Alcatel IP Touch,OU=PKI Authority,O=Alcatel,C=FR | 2005/09/28 12:02:47 | 2025/09/28 10:22:04 | False | valid | Others |
| 2013 | CN=Alcatel Contact Center Solutions,OU=PKI Authority,O=Alcatel,C=FR | 2005/09/28 10:32:18 | 2025/09/28 10:22:04 | False | valid | Others |
| 2014 | CN=Wired Phones,OU=PKI Authority,O=Alcatel-Lucent,C=FR | 2010/01/28 12:20:34 | 2040/01/28 12:30:34 | False | valid | Others |
| 2015 | CN=Alcatel Enterprise Solutions,OU=PKI Authority,O=Alcatel,C=FR | 2005/09/28 12:03:42 | 2055/09/28 12:11:08 | False | valid | Others |
| 2016 | CN=DoD Root CA 2,OU=PKI,OU=DoD,O=U.S. Government,C=US | 2004/12/13 16:00:10 | 2029/12/05 16:00:10 | False | valid | Others |
| 2017 | CN=GTS Root R1,O=Google Trust Services LLC,C=US | 2016/06/22 02:00:00 | 2036/06/22 02:00:00 | True | valid | AD/LDAP Servers, EAP, Endpoint Context Servers, SAML, SMTP, Others |
| 2018 | CN=GTS Root R2,O=Google Trust Services LLC,C=US | 2016/06/22 02:00:00 | 2036/06/22 02:00:00 | True | valid | AD/LDAP Servers, EAP, Endpoint Context Servers, SAML, SMTP, Others |
| 2019 | CN=GTS Root R3,O=Google Trust Services LLC,C=US | 2016/06/22 02:00:00 | 2036/06/22 02:00:00 | True | valid | AD/LDAP Servers, EAP, Endpoint Context Servers, SAML, SMTP, Others |
| 2020 | CN=GTS Root R4,O=Google Trust Services LLC,C=US | 2016/06/22 02:00:00 | 2036/06/22 02:00:00 | False | valid | Others |
| 2021 | CN=DigiCert Global Root CA,OU=www.digicert.com,O=DigiCert Inc,C=US | 2006/11/10 01:00:00 | 2031/11/10 01:00:00 | True | valid | AD/LDAP Servers, Aruba Services, Endpoint Context Servers, SAML, SMTP, Others |
| 2022 | CN=GlobalSign,O=GlobalSign,OU=GlobalSign ECC Root CA - R4 | 2012/11/13 01:00:00 | 2038/01/19 04:14:07 | False | valid | Others |
| 2023 | CN=Aruba Networks Trusted Computing Root CA 1.0,C=US,O=Aruba Networks,OU=Operations,OU=DeviceTrust | 2007/09/14 05:12:06 | 2032/09/14 05:21:14 | False | valid | Others |
| 2024 | CN=DigiCert Global Root G2,OU=www.digicert.com,O=DigiCert Inc,C=US | 2013/08/01 14:00:00 | 2038/01/15 13:00:00 | True | valid | AD/LDAP Servers, Aruba Services, Endpoint Context Servers, SAML, SMTP, Others |
| 2025 | C=US,ST=CA,O=Hewlett-Packard Development Company,CN=HP Devices CA 01 | 2011/01/25 02:30:27 | 2038/01/19 04:14:07 | False | valid | Aruba Infrastructure |
| 2026 | CN=USERTrust RSA Certification Authority,O=The USERTRUST Network,L=Jersey City,ST=New Jersey,C=US | 2010/02/01 01:00:00 | 2038/01/19 00:59:59 | True | valid | AD/LDAP Servers, Aruba Services, EAP, Endpoint Context Servers, SAML, SMTP, Others |
| 2027 | CN=COMODO RSA Certification Authority,O=COMODO CA Limited,L=Salford,ST=Greater Manchester,C=GB | 2010/01/19 01:00:00 | 2038/01/19 00:59:59 | True | valid | AD/LDAP Servers, Aruba Services, Endpoint Context Servers, SAML, SMTP, Others |
| 2028 | CN=Hewlett Packard Enterprise Private SSL CA,OU=Infrastructure Services,O=Hewlett Packard Enterprise Company,C=US | 2015/04/23 02:00:00 | 2025/03/16 00:59:59 | True | valid | AD/LDAP Servers, Aruba Services, Endpoint Context Servers, SAML, SMTP, Others |
| 2029 | CN=Starfield Services Root Certificate Authority - G2,O=Starfield Technologies\, Inc.,L=Scottsdale,ST=Arizona,C=US | 2009/09/02 02:00:00 | 2034/06/28 19:39:16 | True | valid | AD/LDAP Servers, Aruba Services, Endpoint Context Servers, SAML, SMTP, Others |
| 2030 | C=US,ST=CA,O=Hewlett-Packard Development Company,OU=HP Networking EVPG,CN=Device Intermediate CA 01 | 2011/01/25 02:55:09 | 2031/01/26 02:55:09 | False | valid | Others |
| 2031 | C=US,ST=CA,O=Hewlett-Packard Development Company,OU=HP Networking,CN=HP Device Intermediate CA 103 | 2013/12/03 19:35:19 | 2031/01/26 02:55:09 | False | valid | Others |
| 2032 | CN=DigiCert High Assurance EV Root CA,OU=www.digicert.com,O=DigiCert Inc,C=US | 2006/11/10 01:00:00 | 2031/11/10 01:00:00 | False | valid | Others |
| 2033 | CN=Aruba Networks Trusted Computing Issuing CA 1,DC=devicesign,DC=arubanetworks,DC=com | 2016/12/16 21:49:44 | 2032/09/14 05:21:14 | False | valid | Others |
| 2034 | CN=Aruba Networks Trusted Computing Issuing CA 2,DC=devicesign,DC=arubanetworks,DC=com | 2017/02/07 23:22:02 | 2032/09/14 05:21:14 | False | valid | Others |
| 2035 | CN=Aruba Networks Trusted Computing Issuing CA 3,DC=devicesign,DC=arubanetworks,DC=com | 2016/12/16 21:49:54 | 2032/09/14 05:21:14 | False | valid | Others |
| 2036 | CN=Aruba Networks Trusted Computing Policy CA 1.0,OU=Operations,OU=DeviceTrust,O=Aruba Networks,C=US | 2007/09/17 23:42:52 | 2032/09/14 05:21:14 | False | valid | Others |
| 2037 | CN=Aruba Networks Trusted Computing Policy CA 2.0,OU=Operations,OU=DeviceTrust,O=Aruba Networks,C=US | 2016/12/01 01:45:05 | 2032/09/14 05:21:14 | False | valid | Others |
| 2038 | CN=DEVICE-CA1,DC=ca,DC=arubanetworks,DC=com | 2008/07/26 00:01:58 | 2032/09/14 05:21:14 | False | valid | Others |
| 2039 | CN=device-ca5,DC=dc-device-ca5,DC=arubanetworks,DC=com | 2014/01/09 23:43:09 | 2032/09/14 05:21:14 | False | valid | Others |
| 2040 | CN=USERTrust RSA Certification Authority,O=The USERTRUST Network,L=Jersey City,ST=New Jersey,C=US | 2019/03/12 01:00:00 | 2029/01/01 00:59:59 | True | valid | AD/LDAP Servers, Aruba Services, Endpoint Context Servers, SAML, SMTP, Others |
| 2041 | CN=Entrust Root Certification Authority,OU=(c) 2006 Entrust\, Inc.,OU=www.entrust.net/CPS is incorporated by reference,O=Entrust\, Inc.,C=US | 2006/11/27 21:23:42 | 2026/11/27 21:53:42 | False | valid | Others |
| 2042 | 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 | 1999/12/24 18:50:51 | 2029/07/24 16:15:12 | False | valid | Others |
| 2043 | CN=GeoTrust Primary Certification Authority,O=GeoTrust Inc.,C=US | 2006/11/27 01:00:00 | 2036/07/17 01:59:59 | False | valid | Others |
| 2044 | CN=Axis device ID Root CA ECC,O=Axis Communications AB | 2020/04/29 17:16:33 | 2035/04/29 17:16:33 | False | valid | EAP |
| 2045 | CN=Axis device ID Root CA RSA,O=Axis Communications AB | 2020/04/29 17:26:08 | 2035/04/29 17:26:08 | False | valid | EAP |
| 2046 | CN=Axis device ID Intermediate CA ECC 1,O=Axis Communications AB | 2020/05/07 15:54:27 | 2032/05/06 15:54:27 | False | valid | EAP |
| 2047 | CN=Axis device ID Intermediate CA ECC 2,O=Axis Communications AB | 2020/10/26 10:08:53 | 2032/10/25 11:08:53 | False | valid | EAP |
| 2048 | CN=Axis device ID Intermediate CA RSA 1,O=Axis Communications AB | 2020/05/07 15:53:11 | 2032/05/06 15:53:11 | False | valid | EAP |
| 2049 | CN=Axis device ID Intermediate CA RSA 2,O=Axis Communications AB | 2020/10/26 10:05:29 | 2032/10/25 11:05:29 | False | valid | EAP |
| 3001 | emailAddress=3f619638-0d8f-4d33-87c8-000d3fef3a2c@example.com,CN=ClearPass Onboard Local Certificate Authority (Signing),O=Aruba Networks,L=Sunnyvale,ST=California,C=US | 2016/11/16 20:43:31 | 2026/11/17 21:13:31 | True | valid | EAP, Others |
| 3002 | emailAddress=3f619638-0d8f-4d33-87c8-000d3fef3a2c@example.com,CN=ClearPass Onboard Local Certificate Authority,O=Aruba Networks,L=Sunnyvale,ST=California,C=US | 2016/11/16 20:43:31 | 2026/11/17 21:13:31 | True | valid | EAP, Others |
| 3005 | CN=StartCom Certification Authority,OU=Secure Digital Certificate Signing,O=StartCom Ltd.,C=IL | 2006/09/17 21:46:36 | 2036/09/17 21:46:36 | True | valid | AD/LDAP Servers, EAP, Endpoint Context Servers, SAML, SMTP, Others |
| 3007 | emailAddress=17b4da7e-a29b-4f2c-8a01-9700d215cbd2@example.com,CN=Team 1 Onboard Local Certificate Authority (Signing),OU=HPE Aruba,O=HPE Aruba,L=Amstelveen,ST=Noord-Holland,C=NL | 2016/12/10 14:38:57 | 2026/12/11 15:08:57 | True | valid | AD/LDAP Servers, EAP, Endpoint Context Servers, SAML, SMTP, Others |
| 3008 | emailAddress=17b4da7e-a29b-4f2c-8a01-9700d215cbd2@example.com,CN=Team 1 Onboard Local Certificate Authority,OU=HPE Aruba,O=HPE Aruba,L=Amstelveen,ST=Noord-Holland,C=NL | 2016/12/10 14:38:57 | 2026/12/11 15:08:57 | True | valid | AD/LDAP Servers, EAP, Endpoint Context Servers, SAML, SMTP, Others |
| 3010 | CN=StartCom Class 1 DV Server CA,OU=StartCom Certification Authority,O=StartCom Ltd.,C=IL | 2015/12/16 02:00:05 | 2030/12/16 02:00:05 | True | valid | AD/LDAP Servers, EAP, Endpoint Context Servers, SAML, SMTP, Others |
| 3011 | emailAddress=17b4da7e-a29b-4f2c-8a01-9700d215cbd2@example.com,CN=Team 1 Onboard Local Certificate Authority (Signing),OU=HPE Aruba,O=HPE Aruba,L=Amstelveen,ST=Noord-Holland,C=NL | 2017/01/20 09:39:39 | 2027/01/21 10:09:39 | True | valid | AD/LDAP Servers, EAP, Endpoint Context Servers, SAML, SMTP, Others |
| 3012 | emailAddress=17b4da7e-a29b-4f2c-8a01-9700d215cbd2@example.com,CN=Team 1 Onboard Local Certificate Authority,OU=HPE Aruba,O=HPE Aruba,L=Amstelveen,ST=Noord-Holland,C=NL | 2017/01/20 09:39:39 | 2027/01/21 10:09:39 | True | valid | AD/LDAP Servers, EAP, Endpoint Context Servers, SAML, SMTP, Others |
| 3014 | CN=COMODO RSA Domain Validation Secure Server CA,O=COMODO CA Limited,L=Salford,ST=Greater Manchester,C=GB | 2014/02/12 01:00:00 | 2029/02/12 00:59:59 | True | valid | AD/LDAP Servers, EAP, Endpoint Context Servers, SAML, SMTP, Others |
| 3027 | CN=Starfield Services Root Certificate Authority - G2,O=Starfield Technologies, Inc.,L=Scottsdale,ST=Arizona,C=US | 2009/09/02 02:00:00 | 2034/06/28 19:39:16 | True | valid | AD/LDAP Servers, Aruba Services, Endpoint Context Servers, SAML, SMTP, Others |
| 3028 | CN=ISRG Root X1,O=Internet Security Research Group,C=US | 2015/06/04 13:04:38 | 2035/06/04 13:04:38 | True | valid | Others |
| 3054 | CN=Arubalab-Workshop-CA,DC=arubalab,DC=loc | 2016/11/11 14:40:48 | 2026/05/31 16:55:23 | True | valid | AD/LDAP Servers, EAP, Others |

Table - Certificate Trust Lis

## 1.6 Service

The following section details Service settings configured on ClearPass.

### 1.6.1 Summary

The following section details Settings Summary configured on ClearPass.

|  |  |
| --- | --- |
| Service | 42 (default: 6) |
| Service Enabled | 34 (default: 4) |
| Enforcement Policy | 35 (default: 8) |
| Enforcement Profile | 129 (default: 48) |

Table - Service Summary

### 1.6.2 Service

The following section details Service configured on ClearPass.

| Id | Name | Type | Enabled | No | Policy |
| --- | --- | --- | --- | --- | --- |
| 3004 | --- Workshop Admin access --- | TACACS | False | 1 | [Admin Network Login Policy] |
| 3003 | ws\_CPPM Admin Network Login Service | TACACS | True | 2 | ws\_CPPM\_Admin\_policy |
| 3023 | ws\_Instant\_Admin\_access | RADIUS | True | 3 | ws\_Allow\_Admins |
| 3005 | ws\_ArubaOS Switches Device Access Service | TACACS | True | 4 | ws\_AOS-S\_Admin-access |
| 3012 | ws\_Guest Operator Logins | Application | True | 5 | ws\_GuestOperator |
| 3013 | ws\_Onboard\_preauth | Application | True | 6 | ws\_Onboard |
| 3022 | ws\_ArubaOS Switches Device Access (RADIUS) | RADIUS | True | 7 | ws\_AOS-S-Admin-RADIUS |
| 3032 | ws\_Airwave\_Admin\_access | RADIUS | True | 8 | ws\_Airwave\_admin |
| 1 | [Policy Manager Admin Network Login Service] | TACACS | False | 9 | [Admin Network Login Policy] |
| 2 | [AirGroup Authorization Service] | RADIUS | True | 10 | [AirGroup Enforcement Policy] |
| 10 | [Aruba Device Access Service] | TACACS | True | 11 | [Aruba Device Access Policy] |
| 11 | [Guest Operator Logins] | Application | False | 12 | [Guest Operator Logins] |
| 12 | [Insight Operator Logins] | Application | True | 13 | [Insight Operator Logins] |
| 3002 | --- Workshop Wireless Aruba Instant --- | TACACS | False | 14 | [Admin Network Login Policy] |
| 3001 | ws\_ArubaInstant\_802.1X | RADIUS | True | 15 | ws\_wireless\_802.1X |
| 3009 | ws\_Guest MAC Authentication | RADIUS | True | 16 | ws\_Guest MAC Authentication Enforcement Policy |
| 3010 | ws\_Guest User Authentication with MAC Caching | RADIUS | True | 17 | ws\_Guest User Authentication with MAC Caching Enforcement Policy |
| 3029 | ws\_Onguard\_web | WEBAUTH | True | 18 | ws\_Aruba\_Terminate\_Session |
| 3019 | --- Workshop Wired ArubaOS Switch (role-based) --- | TACACS | False | 19 | [Admin Network Login Policy] |
| 3020 | ws\_ArubaOS-Switch-dot1X (role-based) | RADIUS | True | 20 | ws\_ArubaOS-Switch-802.1X-roles |
| 3021 | ws\_ArubaOS-Switch-MAC (role-based) | RADIUS | True | 21 | ws\_ArubaOS-Switch-MAC-roles |
| 3037 | --- Workshop Wired ArubaOS Switch (per user tunneled) --- | TACACS | False | 22 | [Admin Network Login Policy] |
| 3036 | ws\_ArubaOS-Switch-dot1X (per user tunneled node) | RADIUS | True | 23 | ws\_ArubaOS-Switch-802.1X-putn |
| 3038 | ws\_ArubaOS-Switch-MAC (per user tunnel) | RADIUS | True | 24 | ws\_ArubaOS-Switch-MAC-putn |
| 3039 | --- Workshop Wired ArubaOS Switch (downloadable user roles) -- | TACACS | False | 25 | [Admin Network Login Policy] |
| 3040 | ws\_ArubaOS-Switch-dot1X (downloadable user roles) | RADIUS | True | 26 | ws\_ArubaOS-Switch-802.1X-roles-dur |
| 3041 | ws\_ArubaOS-Switch-MAC (downloadable user roles) | RADIUS | True | 27 | ws\_ArubaOS-Switch-MAC-dur |
| 3006 | --- Workshop Wired ArubaOS Switch --- | TACACS | True | 28 | [Admin Network Login Policy] |
| 3007 | ws\_ArubaOS-Switch-dot1X | RADIUS | True | 29 | ws\_ArubaOS-Switch-802.1X |
| 3008 | ws\_ArubaOS-Switch-MAC | RADIUS | True | 30 | ws\_ArubaOS-Switch-MAC |
| 3014 | ws\_Onguard\_wired | WEBAUTH | True | 31 | ws\_Bounce\_client\_wired |
| 3028 | ws\_Onguard\_Dissolvable\_Authorization | Application | True | 32 | ws\_Application\_allow\_all |
| 3018 | ws\_Wired-Guest | WEBAUTH | True | 33 | ws\_Bounce\_client\_wired |
| 3015 | --- Workshop Tunneled Node --- | TACACS | False | 34 | [Admin Network Login Policy] |
| 3016 | ws\_Tunneled\_802.1X | RADIUS | True | 35 | ws\_tunneled\_802.1X |
| 3017 | ws\_Tunneled-node-MAC | RADIUS | True | 36 | ws\_tunneled-MAC |
| 3024 | ws\_Ingress\_Security\_Events | Event | True | 37 | ws\_Ingress\_Security\_Events |
| 3025 | ws\_Release-from-quarantine | Application | True | 38 | ws\_release\_from\_quarantine |
| 3026 | ws\_Onconnect\_Wired | WEBAUTH | True | 39 | ws\_OnConnect |
| 3034 | ws\_ArubaOS Switches Device Access (RADIUS\_MSCHAP) | RADIUS | True | 40 | ws\_AOS-S-Admin-RADIUS |
| 13 | [Device Registration Disconnect] | WEBAUTH | True | 41 | [Device Registration Disconnect] |
| 3045 | ws\_VIA Webauth | RADIUS | True | 42 | [Sample Allow Access Policy] |

Table - Service

The following section details Service configured on ClearPass.

### 1.6.2.1 Service: --- Workshop Admin access ---

|  |  |
| --- | --- |
| Name | --- Workshop Admin access --- |
| Type | TACACS |
| Template | TACACS+ Enforcement |
| Enabled | False |
| Order No | 1 |
| Description |  |
| Monitor Mode | False |
| Auth Sources | [Local User Repository] |
| Auth zSources |  |
| Strip Username | False |
| Enforcement Policy | [Admin Network Login Policy] |
| Rules Match Type |  |

Table - Service: --- Workshop Admin access ---

### 1.6.2.2 Service: ws\_CPPM Admin Network Login Service

|  |  |
| --- | --- |
| Name | ws\_CPPM Admin Network Login Service |
| Type | TACACS |
| Template | TACACS+ Enforcement |
| Enabled | True |
| Order No | 2 |
| Description | Service for access to Policy Manager Admin for network users |
| Monitor Mode | False |
| Auth Sources | AD-arubalab.loc |
| Auth zSources |  |
| Strip Username | False |
| Enforcement Policy | ws\_CPPM\_Admin\_policy |
| Rules Match Type | MATCHES\_ANY |

Table - Service: ws\_CPPM Admin Network Login Service

| Type | Name | Operator | Value |
| --- | --- | --- | --- |
| Connection | NAD-IP-Address | EQUALS | 127.0.0.1 |

Table - Rules Conditions: ws\_CPPM Admin Network Login Service

### 1.6.2.3 Service: ws\_Instant\_Admin\_access

|  |  |
| --- | --- |
| Name | ws\_Instant\_Admin\_access |
| Type | RADIUS |
| Template | RADIUS Enforcement ( Generic ) |
| Enabled | True |
| Order No | 3 |
| Description | Allow Admin Access for Aruba Instant |
| Monitor Mode | False |
| Auth Sources | AD-arubalab.loc-UPN |
| Auth zSources |  |
| Strip Username | False |
| Enforcement Policy | ws\_Allow\_Admins |
| Rules Match Type | MATCHES\_ALL |

Table - Service: ws\_Instant\_Admin\_access

| Type | Name | Operator | Value |
| --- | --- | --- | --- |
| Radius:IETF | NAS-Port-Type | EQUALS | Virtual (5) |
| Radius:IETF | Service-Type | EQUALS | Administrative-User (6) |

Table - Rules Conditions: ws\_Instant\_Admin\_access

### 1.6.2.4 Service: ws\_ArubaOS Switches Device Access Service

|  |  |
| --- | --- |
| Name | ws\_ArubaOS Switches Device Access Service |
| Type | TACACS |
| Template | TACACS+ Enforcement |
| Enabled | True |
| Order No | 4 |
| Description | Service for access to Aruba device |
| Monitor Mode | False |
| Auth Sources | [Local User Repository], AD-arubalab.loc |
| Auth zSources |  |
| Strip Username | False |
| Enforcement Policy | ws\_AOS-S\_Admin-access |
| Rules Match Type |  |

Table - Service: ws\_ArubaOS Switches Device Access Service

### 1.6.2.5 Service: ws\_Guest Operator Logins

|  |  |
| --- | --- |
| Name | ws\_Guest Operator Logins |
| Type | Application |
| Template | Aruba Application Authentication |
| Enabled | True |
| Order No | 5 |
| Description | Authentication service for Guest application |
| Monitor Mode | False |
| Auth Sources | AD-arubalab.loc-deep-nested |
| Auth zSources |  |
| Strip Username | False |
| Enforcement Policy | ws\_GuestOperator |
| Rules Match Type | MATCHES\_ALL |

Table - Service: ws\_Guest Operator Logins

| Type | Name | Operator | Value |
| --- | --- | --- | --- |
| Application | Name | EQUALS | Guest |
| Authentication | Type | NOT\_EQUALS | SSO |

Table - Rules Conditions: ws\_Guest Operator Logins

### 1.6.2.6 Service: ws\_Onboard\_preauth

|  |  |
| --- | --- |
| Name | ws\_Onboard\_preauth |
| Type | Application |
| Template | Aruba Application Authentication |
| Enabled | True |
| Order No | 6 |
| Description | Authentication Service for Applications |
| Monitor Mode | False |
| Auth Sources | AD-arubalab.loc |
| Auth zSources |  |
| Strip Username | False |
| Enforcement Policy | ws\_Onboard |
| Rules Match Type | MATCHES\_ANY |

Table - Service: ws\_Onboard\_preauth

| Type | Name | Operator | Value |
| --- | --- | --- | --- |
| Application | Name | EQUALS | Onboard |

Table - Rules Conditions: ws\_Onboard\_preauth

### 1.6.2.7 Service: ws\_ArubaOS Switches Device Access (RADIUS)

|  |  |
| --- | --- |
| Name | ws\_ArubaOS Switches Device Access (RADIUS) |
| Type | RADIUS |
| Template | RADIUS Enforcement ( Generic ) |
| Enabled | True |
| Order No | 7 |
| Description |  |
| Monitor Mode | False |
| Auth Sources | AD-arubalab.loc |
| Auth zSources |  |
| Strip Username | False |
| Enforcement Policy | ws\_AOS-S-Admin-RADIUS |
| Rules Match Type | MATCHES\_ALL |

Table - Service: ws\_ArubaOS Switches Device Access (RADIUS)

| Type | Name | Operator | Value |
| --- | --- | --- | --- |
| Radius:IETF | NAS-Port-Type | EQUALS | Virtual (5) |
| Radius:IETF | Service-Type | EQUALS | NAS-Prompt-User (7) |

Table - Rules Conditions: ws\_ArubaOS Switches Device Access (RADIUS)

### 1.6.2.8 Service: ws\_Airwave\_Admin\_access

|  |  |
| --- | --- |
| Name | ws\_Airwave\_Admin\_access |
| Type | RADIUS |
| Template | RADIUS Enforcement ( Generic ) |
| Enabled | True |
| Order No | 8 |
| Description | Allow Admin Access for Airwave |
| Monitor Mode | False |
| Auth Sources | AD-arubalab.loc |
| Auth zSources |  |
| Strip Username | False |
| Enforcement Policy | ws\_Airwave\_admin |
| Rules Match Type | MATCHES\_ANY |

Table - Service: ws\_Airwave\_Admin\_access

| Type | Name | Operator | Value |
| --- | --- | --- | --- |
| Radius:IETF | Tunnel-Client-Endpoint | EQUALS | 127.0.0.1 |

Table - Rules Conditions: ws\_Airwave\_Admin\_access

### 1.6.2.9 Service: [Policy Manager Admin Network Login Service]

|  |  |
| --- | --- |
| Name | [Policy Manager Admin Network Login Service] |
| Type | TACACS |
| Template | TACACS+ Enforcement |
| Enabled | False |
| Order No | 9 |
| Description | Service for access to Policy Manager Admin for network users |
| Monitor Mode | False |
| Auth Sources | [Local User Repository], [Admin User Repository] |
| Auth zSources |  |
| Strip Username | False |
| Enforcement Policy | [Admin Network Login Policy] |
| Rules Match Type | MATCHES\_ANY |

Table - Service: [Policy Manager Admin Network Login Service]

| Type | Name | Operator | Value |
| --- | --- | --- | --- |
| Connection | NAD-IP-Address | EQUALS | 127.0.0.1 |

Table - Rules Conditions: [Policy Manager Admin Network Login Service]

### 1.6.2.10 Service: [AirGroup Authorization Service]

|  |  |
| --- | --- |
| Name | [AirGroup Authorization Service] |
| Type | RADIUS |
| Template | RADIUS Enforcement ( Generic ) |
| Enabled | True |
| Order No | 10 |
| Description | Authorization service for AirGroup device access |
| Monitor Mode | False |
| Auth Sources | [Guest Device Repository] |
| Auth zSources |  |
| Strip Username | False |
| Enforcement Policy | [AirGroup Enforcement Policy] |
| Rules Match Type | MATCHES\_ALL |

Table - Service: [AirGroup Authorization Service]

| Type | Name | Operator | Value |
| --- | --- | --- | --- |
| Radius:IETF | Called-Station-Id | EQUALS | AirGroup |
| Radius:IETF | Service-Type | EQUALS | Authorize-Only (17) |

Table - Rules Conditions: [AirGroup Authorization Service]

### 1.6.2.11 Service: [Aruba Device Access Service]

|  |  |
| --- | --- |
| Name | [Aruba Device Access Service] |
| Type | TACACS |
| Template | TACACS+ Enforcement |
| Enabled | True |
| Order No | 11 |
| Description | Service for access to Aruba device |
| Monitor Mode | False |
| Auth Sources | [Local User Repository] |
| Auth zSources |  |
| Strip Username | False |
| Enforcement Policy | [Aruba Device Access Policy] |
| Rules Match Type |  |

Table - Service: [Aruba Device Access Service]

### 1.6.2.12 Service: [Guest Operator Logins]

|  |  |
| --- | --- |
| Name | [Guest Operator Logins] |
| Type | Application |
| Template | Aruba Application Authentication |
| Enabled | False |
| Order No | 12 |
| Description | Authentication service for Guest application |
| Monitor Mode | False |
| Auth Sources | [Local User Repository], [Admin User Repository] |
| Auth zSources |  |
| Strip Username | False |
| Enforcement Policy | [Guest Operator Logins] |
| Rules Match Type | MATCHES\_ALL |

Table - Service: [Guest Operator Logins]

| Type | Name | Operator | Value |
| --- | --- | --- | --- |
| Application | Name | EQUALS | Guest |
| Authentication | Type | NOT\_EQUALS | SSO |

Table - Rules Conditions: [Guest Operator Logins]

### 1.6.2.13 Service: [Insight Operator Logins]

|  |  |
| --- | --- |
| Name | [Insight Operator Logins] |
| Type | Application |
| Template | Aruba Application Authentication |
| Enabled | True |
| Order No | 13 |
| Description | Authentication service for Insight application |
| Monitor Mode | False |
| Auth Sources | [Local User Repository] |
| Auth zSources |  |
| Strip Username | False |
| Enforcement Policy | [Insight Operator Logins] |
| Rules Match Type | MATCHES\_ALL |

Table - Service: [Insight Operator Logins]

| Type | Name | Operator | Value |
| --- | --- | --- | --- |
| Application | Name | EQUALS | Insight |
| Authentication | Type | NOT\_EQUALS | SSO |

Table - Rules Conditions: [Insight Operator Logins]

### 1.6.2.14 Service: --- Workshop Wireless Aruba Instant ---

|  |  |
| --- | --- |
| Name | --- Workshop Wireless Aruba Instant --- |
| Type | TACACS |
| Template | TACACS+ Enforcement |
| Enabled | False |
| Order No | 14 |
| Description |  |
| Monitor Mode | False |
| Auth Sources | [Local User Repository] |
| Auth zSources |  |
| Strip Username | False |
| Enforcement Policy | [Admin Network Login Policy] |
| Rules Match Type |  |

Table - Service: --- Workshop Wireless Aruba Instant ---

### 1.6.2.15 Service: ws\_ArubaInstant\_802.1X

|  |  |
| --- | --- |
| Name | ws\_ArubaInstant\_802.1X |
| Type | RADIUS |
| Template | 802.1X Wireless |
| Enabled | True |
| Order No | 15 |
| Description | 802.1X Wireless Access Service |
| Monitor Mode | False |
| Auth Sources | AD-arubalab.loc |
| Auth zSources | [Endpoints Repository] |
| Strip Username | False |
| Enforcement Policy | ws\_wireless\_802.1X |
| Rules Match Type | MATCHES\_ALL |

Table - Service: ws\_ArubaInstant\_802.1X

| Type | Name | Operator | Value |
| --- | --- | --- | --- |
| Radius:IETF | NAS-Port-Type | EQUALS | Wireless-802.11 (19) |
| Radius:IETF | Service-Type | BELONGS\_TO | Login-User (1), Framed-User (2), Authenticate-Only (8) |
| Radius:Aruba | Aruba-Essid-Name | CONTAINS | corp |

Table - Rules Conditions: ws\_ArubaInstant\_802.1X

### 1.6.2.16 Service: ws\_Guest MAC Authentication

|  |  |
| --- | --- |
| Name | ws\_Guest MAC Authentication |
| Type | RADIUS |
| Template | MAC Authentication |
| Enabled | True |
| Order No | 16 |
| Description | MAC Authentication bypass for captive portal users |
| Monitor Mode | False |
| Auth Sources | [Endpoints Repository] |
| Auth zSources | [Time Source], [Guest User Repository] |
| Strip Username | False |
| Enforcement Policy | ws\_Guest MAC Authentication Enforcement Policy |
| Rules Match Type | MATCHES\_ALL |

Table - Service: ws\_Guest MAC Authentication

| Type | Name | Operator | Value |
| --- | --- | --- | --- |
| Connection | Client-Mac-Address | EQUALS | %{Radius:IETF:User-Name} |
| Radius:Aruba | Aruba-Essid-Name | CONTAINS | -eh |

Table - Rules Conditions: ws\_Guest MAC Authentication

### 1.6.2.17 Service: ws\_Guest User Authentication with MAC Caching

|  |  |
| --- | --- |
| Name | ws\_Guest User Authentication with MAC Caching |
| Type | RADIUS |
| Template | RADIUS Enforcement ( Generic ) |
| Enabled | True |
| Order No | 17 |
| Description | Captive Portal authentication with MAC Caching |
| Monitor Mode | False |
| Auth Sources | [Guest User Repository] |
| Auth zSources | [Endpoints Repository], [Time Source] |
| Strip Username | False |
| Enforcement Policy | ws\_Guest User Authentication with MAC Caching Enforcement Policy |
| Rules Match Type | MATCHES\_ALL |

Table - Service: ws\_Guest User Authentication with MAC Caching

| Type | Name | Operator | Value |
| --- | --- | --- | --- |
| Radius:IETF | Calling-Station-Id | EXISTS |  |
| Connection | Client-Mac-Address | NOT\_EQUALS | %{Radius:IETF:User-Name} |
| Radius:Aruba | Aruba-Essid-Name | EQUALS | guest-1 |

Table - Rules Conditions: ws\_Guest User Authentication with MAC Caching

### 1.6.2.18 Service: ws\_Onguard\_web

|  |  |
| --- | --- |
| Name | ws\_Onguard\_web |
| Type | WEBAUTH |
| Template | Web-based Health Check Only |
| Enabled | True |
| Order No | 18 |
| Description | Web-Based Access - No Authentication; Only Health Check |
| Monitor Mode | False |
| Auth Sources |  |
| Auth zSources |  |
| Strip Username | False |
| Enforcement Policy | ws\_Aruba\_Terminate\_Session |
| Rules Match Type | MATCHES\_ALL |

Table - Service: ws\_Onguard\_web

| Type | Name | Operator | Value |
| --- | --- | --- | --- |
| Host | CheckType | MATCHES\_ALL | Health |
| Connection | Src-IP-Address | EQUALS | 127.0.0.1 |
| Host | AgentType | CONTAINS | WebAgent |

Table - Rules Conditions: ws\_Onguard\_web

### 1.6.2.19 Service: --- Workshop Wired ArubaOS Switch (role-based) ---

|  |  |
| --- | --- |
| Name | --- Workshop Wired ArubaOS Switch (role-based) --- |
| Type | TACACS |
| Template | TACACS+ Enforcement |
| Enabled | False |
| Order No | 19 |
| Description |  |
| Monitor Mode | False |
| Auth Sources | [Local User Repository] |
| Auth zSources |  |
| Strip Username | False |
| Enforcement Policy | [Admin Network Login Policy] |
| Rules Match Type |  |

Table - Service: --- Workshop Wired ArubaOS Switch (role-based) ---

### 1.6.2.20 Service: ws\_ArubaOS-Switch-dot1X (role-based)

|  |  |
| --- | --- |
| Name | ws\_ArubaOS-Switch-dot1X (role-based) |
| Type | RADIUS |
| Template | 802.1X Wired |
| Enabled | True |
| Order No | 20 |
| Description | 802.1X Wired Access Service |
| Monitor Mode | False |
| Auth Sources | AD-arubalab.loc |
| Auth zSources |  |
| Strip Username | True |
| Enforcement Policy | ws\_ArubaOS-Switch-802.1X-roles |
| Rules Match Type | MATCHES\_ALL |

Table - Service: ws\_ArubaOS-Switch-dot1X (role-based)

| Type | Name | Operator | Value |
| --- | --- | --- | --- |
| Radius:IETF | NAS-Port-Type | EQUALS | Ethernet (15) |
| Radius:IETF | Service-Type | BELONGS\_TO | Login-User (1), Framed-User (2), Authenticate-Only (8) |
| Radius:IETF | Connect-Info | BEGINS\_WITH | CONNECT |
| Radius:IETF | NAS-Identifier | CONTAINS | rbac |

Table - Rules Conditions: ws\_ArubaOS-Switch-dot1X (role-based)

### 1.6.2.21 Service: ws\_ArubaOS-Switch-MAC (role-based)

|  |  |
| --- | --- |
| Name | ws\_ArubaOS-Switch-MAC (role-based) |
| Type | RADIUS |
| Template | MAC Authentication |
| Enabled | True |
| Order No | 21 |
| Description | MAC-based Authentication Service for ArubaOS switch |
| Monitor Mode | False |
| Auth Sources | [Endpoints Repository] |
| Auth zSources |  |
| Strip Username | False |
| Enforcement Policy | ws\_ArubaOS-Switch-MAC-roles |
| Rules Match Type | MATCHES\_ALL |

Table - Service: ws\_ArubaOS-Switch-MAC (role-based)

| Type | Name | Operator | Value |
| --- | --- | --- | --- |
| Radius:IETF | NAS-Port-Type | BELONGS\_TO | Ethernet (15), Wireless-802.11 (19) |
| Radius:IETF | Service-Type | BELONGS\_TO | Login-User (1), Call-Check (10) |
| Connection | Client-Mac-Address | EQUALS | %{Radius:IETF:User-Name} |
| Radius:IETF | Connect-Info | BEGINS\_WITH | CONNECT |
| Radius:IETF | NAS-Identifier | CONTAINS | rbac |

Table - Rules Conditions: ws\_ArubaOS-Switch-MAC (role-based)

### 1.6.2.22 Service: --- Workshop Wired ArubaOS Switch (per user tunneled) ---

|  |  |
| --- | --- |
| Name | --- Workshop Wired ArubaOS Switch (per user tunneled) --- |
| Type | TACACS |
| Template | TACACS+ Enforcement |
| Enabled | False |
| Order No | 22 |
| Description |  |
| Monitor Mode | False |
| Auth Sources | [Local User Repository] |
| Auth zSources |  |
| Strip Username | False |
| Enforcement Policy | [Admin Network Login Policy] |
| Rules Match Type |  |

Table - Service: --- Workshop Wired ArubaOS Switch (per user tunneled) ---

### 1.6.2.23 Service: ws\_ArubaOS-Switch-dot1X (per user tunneled node)

|  |  |
| --- | --- |
| Name | ws\_ArubaOS-Switch-dot1X (per user tunneled node) |
| Type | RADIUS |
| Template | 802.1X Wired |
| Enabled | True |
| Order No | 23 |
| Description | 802.1X Wired Access Service (per user tunneled node) |
| Monitor Mode | False |
| Auth Sources | AD-arubalab.loc |
| Auth zSources |  |
| Strip Username | True |
| Enforcement Policy | ws\_ArubaOS-Switch-802.1X-putn |
| Rules Match Type | MATCHES\_ALL |

Table - Service: ws\_ArubaOS-Switch-dot1X (per user tunneled node)

| Type | Name | Operator | Value |
| --- | --- | --- | --- |
| Radius:IETF | NAS-Port-Type | EQUALS | Ethernet (15) |
| Radius:IETF | Service-Type | BELONGS\_TO | Login-User (1), Framed-User (2), Authenticate-Only (8) |
| Radius:IETF | Connect-Info | BEGINS\_WITH | CONNECT |
| Radius:IETF | NAS-Identifier | CONTAINS | putn |

Table - Rules Conditions: ws\_ArubaOS-Switch-dot1X (per user tunneled node)

### 1.6.2.24 Service: ws\_ArubaOS-Switch-MAC (per user tunnel)

|  |  |
| --- | --- |
| Name | ws\_ArubaOS-Switch-MAC (per user tunnel) |
| Type | RADIUS |
| Template | MAC Authentication |
| Enabled | True |
| Order No | 24 |
| Description | MAC-based Authentication Service for ArubaOS switch (per user tunneled) |
| Monitor Mode | False |
| Auth Sources | [Endpoints Repository] |
| Auth zSources |  |
| Strip Username | False |
| Enforcement Policy | ws\_ArubaOS-Switch-MAC-putn |
| Rules Match Type | MATCHES\_ALL |

Table - Service: ws\_ArubaOS-Switch-MAC (per user tunnel)

| Type | Name | Operator | Value |
| --- | --- | --- | --- |
| Radius:IETF | NAS-Port-Type | BELONGS\_TO | Ethernet (15), Wireless-802.11 (19) |
| Radius:IETF | Service-Type | BELONGS\_TO | Login-User (1), Call-Check (10) |
| Connection | Client-Mac-Address | EQUALS | %{Radius:IETF:User-Name} |
| Radius:IETF | Connect-Info | BEGINS\_WITH | CONNECT |
| Radius:IETF | NAS-Identifier | CONTAINS | putn |

Table - Rules Conditions: ws\_ArubaOS-Switch-MAC (per user tunnel)

### 1.6.2.25 Service: --- Workshop Wired ArubaOS Switch (downloadable user roles) --

|  |  |
| --- | --- |
| Name | --- Workshop Wired ArubaOS Switch (downloadable user roles) -- |
| Type | TACACS |
| Template | TACACS+ Enforcement |
| Enabled | False |
| Order No | 25 |
| Description |  |
| Monitor Mode | False |
| Auth Sources | [Local User Repository] |
| Auth zSources |  |
| Strip Username | False |
| Enforcement Policy | [Admin Network Login Policy] |
| Rules Match Type |  |

Table - Service: --- Workshop Wired ArubaOS Switch (downloadable user roles) --

### 1.6.2.26 Service: ws\_ArubaOS-Switch-dot1X (downloadable user roles)

|  |  |
| --- | --- |
| Name | ws\_ArubaOS-Switch-dot1X (downloadable user roles) |
| Type | RADIUS |
| Template | 802.1X Wired |
| Enabled | True |
| Order No | 26 |
| Description | 802.1X Wired Access Service (per user tunneled node) |
| Monitor Mode | False |
| Auth Sources | AD-arubalab.loc |
| Auth zSources |  |
| Strip Username | True |
| Enforcement Policy | ws\_ArubaOS-Switch-802.1X-roles-dur |
| Rules Match Type | MATCHES\_ALL |

Table - Service: ws\_ArubaOS-Switch-dot1X (downloadable user roles)

| Type | Name | Operator | Value |
| --- | --- | --- | --- |
| Radius:IETF | NAS-Port-Type | EQUALS | Ethernet (15) |
| Radius:IETF | Service-Type | BELONGS\_TO | Login-User (1), Framed-User (2), Authenticate-Only (8) |
| Radius:IETF | Connect-Info | BEGINS\_WITH | CONNECT |
| Radius:IETF | NAS-Identifier | CONTAINS | dur |

Table - Rules Conditions: ws\_ArubaOS-Switch-dot1X (downloadable user roles)

### 1.6.2.27 Service: ws\_ArubaOS-Switch-MAC (downloadable user roles)

|  |  |
| --- | --- |
| Name | ws\_ArubaOS-Switch-MAC (downloadable user roles) |
| Type | RADIUS |
| Template | MAC Authentication |
| Enabled | True |
| Order No | 27 |
| Description | MAC-based Authentication Service for ArubaOS switch (downloadable user roles) |
| Monitor Mode | False |
| Auth Sources | [Endpoints Repository] |
| Auth zSources |  |
| Strip Username | False |
| Enforcement Policy | ws\_ArubaOS-Switch-MAC-dur |
| Rules Match Type | MATCHES\_ALL |

Table - Service: ws\_ArubaOS-Switch-MAC (downloadable user roles)

| Type | Name | Operator | Value |
| --- | --- | --- | --- |
| Radius:IETF | NAS-Port-Type | BELONGS\_TO | Ethernet (15), Wireless-802.11 (19) |
| Radius:IETF | Service-Type | BELONGS\_TO | Login-User (1), Call-Check (10) |
| Connection | Client-Mac-Address | EQUALS | %{Radius:IETF:User-Name} |
| Radius:IETF | Connect-Info | BEGINS\_WITH | CONNECT |
| Radius:IETF | NAS-Identifier | CONTAINS | dur |

Table - Rules Conditions: ws\_ArubaOS-Switch-MAC (downloadable user roles)

### 1.6.2.28 Service: --- Workshop Wired ArubaOS Switch ---

|  |  |
| --- | --- |
| Name | --- Workshop Wired ArubaOS Switch --- |
| Type | TACACS |
| Template | TACACS+ Enforcement |
| Enabled | True |
| Order No | 28 |
| Description |  |
| Monitor Mode | False |
| Auth Sources | [Local User Repository] |
| Auth zSources |  |
| Strip Username | False |
| Enforcement Policy | [Admin Network Login Policy] |
| Rules Match Type |  |

Table - Service: --- Workshop Wired ArubaOS Switch ---

### 1.6.2.29 Service: ws\_ArubaOS-Switch-dot1X

|  |  |
| --- | --- |
| Name | ws\_ArubaOS-Switch-dot1X |
| Type | RADIUS |
| Template | 802.1X Wired |
| Enabled | True |
| Order No | 29 |
| Description | 802.1X Wired Access Service |
| Monitor Mode | False |
| Auth Sources | AD-arubalab.loc |
| Auth zSources |  |
| Strip Username | True |
| Enforcement Policy | ws\_ArubaOS-Switch-802.1X |
| Rules Match Type | MATCHES\_ALL |

Table - Service: ws\_ArubaOS-Switch-dot1X

| Type | Name | Operator | Value |
| --- | --- | --- | --- |
| Radius:IETF | NAS-Port-Type | EQUALS | Ethernet (15) |
| Radius:IETF | Service-Type | BELONGS\_TO | Login-User (1), Framed-User (2), Authenticate-Only (8) |
| Radius:IETF | Connect-Info | BEGINS\_WITH | CONNECT |

Table - Rules Conditions: ws\_ArubaOS-Switch-dot1X

### 1.6.2.30 Service: ws\_ArubaOS-Switch-MAC

|  |  |
| --- | --- |
| Name | ws\_ArubaOS-Switch-MAC |
| Type | RADIUS |
| Template | MAC Authentication |
| Enabled | True |
| Order No | 30 |
| Description | MAC-based Authentication Service for ArubaOS switch |
| Monitor Mode | False |
| Auth Sources | [Endpoints Repository] |
| Auth zSources |  |
| Strip Username | False |
| Enforcement Policy | ws\_ArubaOS-Switch-MAC |
| Rules Match Type | MATCHES\_ALL |

Table - Service: ws\_ArubaOS-Switch-MAC

| Type | Name | Operator | Value |
| --- | --- | --- | --- |
| Radius:IETF | NAS-Port-Type | BELONGS\_TO | Ethernet (15), Wireless-802.11 (19) |
| Radius:IETF | Service-Type | BELONGS\_TO | Login-User (1), Call-Check (10) |
| Connection | Client-Mac-Address | EQUALS | %{Radius:IETF:User-Name} |
| Radius:IETF | Connect-Info | BEGINS\_WITH | CONNECT |

Table - Rules Conditions: ws\_ArubaOS-Switch-MAC

### 1.6.2.31 Service: ws\_Onguard\_wired

|  |  |
| --- | --- |
| Name | ws\_Onguard\_wired |
| Type | WEBAUTH |
| Template | Web-based Health Check Only |
| Enabled | True |
| Order No | 31 |
| Description | Web-Based Access - No Authentication; Only Health Check |
| Monitor Mode | False |
| Auth Sources |  |
| Auth zSources |  |
| Strip Username | False |
| Enforcement Policy | ws\_Bounce\_client\_wired |
| Rules Match Type | MATCHES\_ANY |

Table - Service: ws\_Onguard\_wired

| Type | Name | Operator | Value |
| --- | --- | --- | --- |
| Host | CheckType | MATCHES\_ALL | Health |

Table - Rules Conditions: ws\_Onguard\_wired

### 1.6.2.32 Service: ws\_Onguard\_Dissolvable\_Authorization

|  |  |
| --- | --- |
| Name | ws\_Onguard\_Dissolvable\_Authorization |
| Type | Application |
| Template | Aruba Application Authentication |
| Enabled | True |
| Order No | 32 |
| Description | Authentication Service for Applications |
| Monitor Mode | False |
| Auth Sources | AD-arubalab.loc, [Guest User Repository] |
| Auth zSources |  |
| Strip Username | False |
| Enforcement Policy | ws\_Application\_allow\_all |
| Rules Match Type | MATCHES\_ALL |

Table - Service: ws\_Onguard\_Dissolvable\_Authorization

| Type | Name | Operator | Value |
| --- | --- | --- | --- |
| Application | Name | EXISTS |  |
| Application:ClearPass | Page-Name | EQUALS | onguard |

Table - Rules Conditions: ws\_Onguard\_Dissolvable\_Authorization

### 1.6.2.33 Service: ws\_Wired-Guest

|  |  |
| --- | --- |
| Name | ws\_Wired-Guest |
| Type | WEBAUTH |
| Template | Web-based Authentication |
| Enabled | True |
| Order No | 33 |
| Description | Workshop Wired Guest |
| Monitor Mode | False |
| Auth Sources | [Guest User Repository] |
| Auth zSources |  |
| Strip Username | False |
| Enforcement Policy | ws\_Bounce\_client\_wired |
| Rules Match Type | MATCHES\_ANY |

Table - Service: ws\_Wired-Guest

| Type | Name | Operator | Value |
| --- | --- | --- | --- |
| Host | CheckType | MATCHES\_ANY | Authentication |

Table - Rules Conditions: ws\_Wired-Guest

### 1.6.2.34 Service: --- Workshop Tunneled Node ---

|  |  |
| --- | --- |
| Name | --- Workshop Tunneled Node --- |
| Type | TACACS |
| Template | TACACS+ Enforcement |
| Enabled | False |
| Order No | 34 |
| Description |  |
| Monitor Mode | False |
| Auth Sources | [Local User Repository] |
| Auth zSources |  |
| Strip Username | False |
| Enforcement Policy | [Admin Network Login Policy] |
| Rules Match Type |  |

Table - Service: --- Workshop Tunneled Node ---

### 1.6.2.35 Service: ws\_Tunneled\_802.1X

|  |  |
| --- | --- |
| Name | ws\_Tunneled\_802.1X |
| Type | RADIUS |
| Template | 802.1X Wired |
| Enabled | True |
| Order No | 35 |
| Description | 802.1X Wired Access Service |
| Monitor Mode | False |
| Auth Sources | AD-arubalab.loc |
| Auth zSources |  |
| Strip Username | False |
| Enforcement Policy | ws\_tunneled\_802.1X |
| Rules Match Type | MATCHES\_ALL |

Table - Service: ws\_Tunneled\_802.1X

| Type | Name | Operator | Value |
| --- | --- | --- | --- |
| Radius:IETF | NAS-Port-Type | EQUALS | Ethernet (15) |
| Radius:IETF | Service-Type | BELONGS\_TO | Login-User (1), Framed-User (2), Authenticate-Only (8) |
| Radius:IETF | NAS-Identifier | BEGINS\_WITH | tunnel-team |

Table - Rules Conditions: ws\_Tunneled\_802.1X

### 1.6.2.36 Service: ws\_Tunneled-node-MAC

|  |  |
| --- | --- |
| Name | ws\_Tunneled-node-MAC |
| Type | RADIUS |
| Template | MAC Authentication |
| Enabled | True |
| Order No | 36 |
| Description | MAC-based Authentication Service for Tunneled Node |
| Monitor Mode | False |
| Auth Sources | [Endpoints Repository] |
| Auth zSources |  |
| Strip Username | False |
| Enforcement Policy | ws\_tunneled-MAC |
| Rules Match Type | MATCHES\_ALL |

Table - Service: ws\_Tunneled-node-MAC

| Type | Name | Operator | Value |
| --- | --- | --- | --- |
| Radius:IETF | NAS-Port-Type | BELONGS\_TO | Ethernet (15), Wireless-802.11 (19) |
| Radius:IETF | Service-Type | BELONGS\_TO | Login-User (1), Call-Check (10) |
| Connection | Client-Mac-Address | EQUALS | %{Radius:IETF:User-Name} |
| Radius:IETF | NAS-Identifier | BEGINS\_WITH | tunnel-team |

Table - Rules Conditions: ws\_Tunneled-node-MAC

### 1.6.2.37 Service: ws\_Ingress\_Security\_Events

|  |  |
| --- | --- |
| Name | ws\_Ingress\_Security\_Events |
| Type | Event |
| Template | Event-based Enforcement |
| Enabled | True |
| Order No | 37 |
| Description | Service for ingress events based enforcement |
| Monitor Mode | False |
| Auth Sources |  |
| Auth zSources |  |
| Strip Username |  |
| Enforcement Policy | ws\_Ingress\_Security\_Events |
| Rules Match Type |  |

Table - Service: ws\_Ingress\_Security\_Events

### 1.6.2.38 Service: ws\_Release-from-quarantine

|  |  |
| --- | --- |
| Name | ws\_Release-from-quarantine |
| Type | Application |
| Template | Aruba Application Authentication |
| Enabled | True |
| Order No | 38 |
| Description | Authentication Service for Applications |
| Monitor Mode | False |
| Auth Sources | AD-arubalab.loc |
| Auth zSources | [Time Source] |
| Strip Username | False |
| Enforcement Policy | ws\_release\_from\_quarantine |
| Rules Match Type | MATCHES\_ANY |

Table - Service: ws\_Release-from-quarantine

| Type | Name | Operator | Value |
| --- | --- | --- | --- |
| Application | Name | EXISTS |  |

Table - Rules Conditions: ws\_Release-from-quarantine

### 1.6.2.39 Service: ws\_Onconnect\_Wired

|  |  |
| --- | --- |
| Name | ws\_Onconnect\_Wired |
| Type | WEBAUTH |
| Template | ClearPass OnConnect Enforcement |
| Enabled | True |
| Order No | 39 |
| Description | Service for ClearPass OnConnect enforcement |
| Monitor Mode | False |
| Auth Sources |  |
| Auth zSources | [Endpoints Repository], AD-arubalab.loc |
| Strip Username | False |
| Enforcement Policy | ws\_OnConnect |
| Rules Match Type | MATCHES\_ANY |

Table - Service: ws\_Onconnect\_Wired

| Type | Name | Operator | Value |
| --- | --- | --- | --- |
| Host | CheckType | EQUALS | None |

Table - Rules Conditions: ws\_Onconnect\_Wired

### 1.6.2.40 Service: ws\_ArubaOS Switches Device Access (RADIUS\_MSCHAP)

|  |  |
| --- | --- |
| Name | ws\_ArubaOS Switches Device Access (RADIUS\_MSCHAP) |
| Type | RADIUS |
| Template | RADIUS Enforcement ( Generic ) |
| Enabled | True |
| Order No | 40 |
| Description |  |
| Monitor Mode | False |
| Auth Sources | AD-arubalab.loc |
| Auth zSources |  |
| Strip Username | False |
| Enforcement Policy | ws\_AOS-S-Admin-RADIUS |
| Rules Match Type | MATCHES\_ALL |

Table - Service: ws\_ArubaOS Switches Device Access (RADIUS\_MSCHAP)

| Type | Name | Operator | Value |
| --- | --- | --- | --- |
| Radius:IETF | NAS-Port-Type | EQUALS | Wireless-802.11 (19) |
| Radius:IETF | Connect-Info | CONTAINS | CONNECT 11Mbps 802.11b |

Table - Rules Conditions: ws\_ArubaOS Switches Device Access (RADIUS\_MSCHAP)

### 1.6.2.41 Service: [Device Registration Disconnect]

|  |  |
| --- | --- |
| Name | [Device Registration Disconnect] |
| Type | WEBAUTH |
| Template | Web-based Authentication |
| Enabled | True |
| Order No | 41 |
| Description | Service to disconnect all headless devices after they have registered |
| Monitor Mode | False |
| Auth Sources | [Guest Device Repository] |
| Auth zSources |  |
| Strip Username | False |
| Enforcement Policy | [Device Registration Disconnect] |
| Rules Match Type | MATCHES\_ALL |

Table - Service: [Device Registration Disconnect]

| Type | Name | Operator | Value |
| --- | --- | --- | --- |
| Host | CheckType | EQUALS | Authentication |
| Application:ClearPass | Page-Name | BELONGS\_TO | mac\_create,mactrac\_create |

Table - Rules Conditions: [Device Registration Disconnect]

### 1.6.2.42 Service: ws\_VIA Webauth

|  |  |
| --- | --- |
| Name | ws\_VIA Webauth |
| Type | RADIUS |
| Template | RADIUS Enforcement ( Generic ) |
| Enabled | True |
| Order No | 42 |
| Description |  |
| Monitor Mode | False |
| Auth Sources | AD-arubalab.loc |
| Auth zSources |  |
| Strip Username | False |
| Enforcement Policy | [Sample Allow Access Policy] |
| Rules Match Type | MATCHES\_ALL |

Table - Service: ws\_VIA Webauth

| Type | Name | Operator | Value |
| --- | --- | --- | --- |
| Radius:IETF | NAS-Port-Type | EQUALS | Virtual (5) |
| Radius:IETF | Service-Type | EQUALS | Framed-User (2) |

Table - Rules Conditions: ws\_VIA Webauth

### 1.6.3 Enforcement Policy

The following section details Enforcement Policy configured on ClearPass.

| Id | Name | Type | Default | Rule Algo | Rules Count | Ref |
| --- | --- | --- | --- | --- | --- | --- |
| 5 | [Admin Network Login Policy] | TACACS | [TACACS+ Deny Profile] | evaluate-all | 12 | 8 |
| 7 | [AirGroup Enforcement Policy] | RADIUS | [AirGroup Response] | evaluate-all | 4 | 1 |
| 17 | [Aruba Device Access Policy] | TACACS | [ArubaOS Wireless - TACACS+ Read-Only Access] | first-applicable | 2 | 1 |
| 18 | [Guest Operator Logins] | Application | [Deny Application Access Profile] | first-applicable | 2 | 1 |
| 19 | [Insight Operator Logins] | Application | [Deny Application Access Profile] | first-applicable | 1 | 1 |
| 20 | [Device Registration Disconnect] | WEBAUTH | [ArubaOS Wireless - Terminate Session] | first-applicable | 1 | 1 |
| 3001 | [Sample Allow Access Policy] | RADIUS | [Allow Access Profile] | evaluate-all | 1 | 1 |
| 3002 | [Sample Deny Access Policy] | RADIUS | [Deny Access Profile] | evaluate-all | 1 | 0 |
| 3004 | ws\_wireless\_802.1X | RADIUS | [Deny Access Profile] | first-applicable | 9 | 1 |
| 3005 | ws\_CPPM\_Admin\_policy | TACACS | [TACACS+ Deny Profile] | first-applicable | 2 | 1 |
| 3006 | ws\_AOS-S\_Admin-access | TACACS | [TACACS+ Deny Profile] | first-applicable | 2 | 1 |
| 3007 | ws\_ArubaOS-Switch-MAC | RADIUS | ws\_vlan14\_untrust | first-applicable | 8 | 1 |
| 3008 | ws\_ArubaOS-Switch-802.1X | RADIUS | [Deny Access Profile] | first-applicable | 5 | 1 |
| 3009 | ws\_Guest MAC Authentication Enforcement Policy | RADIUS | [Deny Access Profile] | first-applicable | 2 | 1 |
| 3010 | ws\_Guest User Authentication with MAC Caching Enforcement Policy | RADIUS | [Allow Access Profile] | first-applicable | 2 | 1 |
| 3011 | ws\_GuestOperator | Application | [Deny Application Access Profile] | first-applicable | 3 | 1 |
| 3012 | ws\_Onboard | Application | [Deny Application Access Profile] | first-applicable | 2 | 1 |
| 3013 | ws\_Bounce\_client\_wired | WEBAUTH | [ArubaOS Switching - Bounce Switch Port] | first-applicable | 1 | 2 |
| 3014 | ws\_tunneled\_802.1X | RADIUS | [Deny Access Profile] | first-applicable | 4 | 1 |
| 3015 | ws\_tunneled-MAC | RADIUS | [Deny Access Profile] | first-applicable | 2 | 1 |
| 3016 | ws\_HPE-Terminate-Session | WEBAUTH | [ArubaOS Switching - Terminate Session] | first-applicable | 1 | 0 |
| 3017 | ws\_ArubaOS-Switch-802.1X-roles | RADIUS | [Deny Access Profile] | first-applicable | 4 | 1 |
| 3018 | ws\_ArubaOS-Switch-MAC-roles | RADIUS | ws\_hpe\_role\_guest-redirect | first-applicable | 6 | 1 |
| 3019 | ws\_Allow\_Admins | RADIUS | [Deny Access Profile] | first-applicable | 1 | 1 |
| 3020 | ws\_AOS-S-Admin-RADIUS | RADIUS | [Deny Access Profile] | first-applicable | 1 | 2 |
| 3021 | ws\_Ingress\_Security\_Events | Event | ws\_quarantine\_set\_security\_info\_checkpoint | first-applicable | 2 | 1 |
| 3022 | ws\_release\_from\_quarantine | Application | [Deny Application Access Profile] | first-applicable | 3 | 1 |
| 3023 | ws\_OnConnect | WEBAUTH | ws\_snmp\_vlan14\_untrust | first-applicable | 3 | 1 |
| 3024 | ws\_Application\_allow\_all | Application | [Allow Application Access Profile] | first-applicable | 1 | 1 |
| 3025 | ws\_Aruba\_Terminate\_Session | WEBAUTH | [ArubaOS Wireless - Terminate Session] | first-applicable | 1 | 1 |
| 3029 | ws\_Airwave\_admin | RADIUS | [Deny Access Profile] | first-applicable | 1 | 1 |
| 3031 | ws\_ArubaOS-Switch-802.1X-putn | RADIUS | [Deny Access Profile] | first-applicable | 4 | 1 |
| 3032 | ws\_ArubaOS-Switch-MAC-putn | RADIUS | ws\_hpe\_role\_profiler | first-applicable | 5 | 1 |
| 3033 | ws\_ArubaOS-Switch-802.1X-roles-dur | RADIUS | [Deny Access Profile] | first-applicable | 4 | 1 |
| 3034 | ws\_ArubaOS-Switch-MAC-dur | RADIUS | ws\_hpe\_role\_profiler | first-applicable | 5 | 1 |

Table - Enforcement Policy

The following section details Enforcement Policy configured on ClearPass.

### 1.6.3.1 Enforcement Policy: [Admin Network Login Policy]

|  |  |
| --- | --- |
| Id | 5 |
| Name | [Admin Network Login Policy] |
| Type | TACACS |
| Default | [TACACS+ Deny Profile] |
| Rule Algo | evaluate-all |

Table - Enforcement Policy: [Admin Network Login Policy]

| Condition | Enforcement Profiles |
| --- | --- |
| (Role MATCHES\_ANY [TACACS+ Help Desk]) | [TACACS+ Help Desk] |
| (Role MATCHES\_ANY [TACACS+ Network Admin]) | [TACACS+ Network Admin] |
| (Role MATCHES\_ANY [TACACS+ Receptionist]) | [TACACS+ Receptionist] |
| (Role MATCHES\_ANY [TACACS+ Super Admin]) | [TACACS+ Super Admin] |
| (Role MATCHES\_ANY [TACACS+ Read-only Admin]) | [TACACS+ Read-only Admin] |
| (Role MATCHES\_ANY [TACACS+ API Admin]) | [TACACS+ API Admin] |
| (Role\_Name EQUALS Help Desk) | [TACACS+ Help Desk] |
| (Role\_Name EQUALS Network Administrator) | [TACACS+ Network Admin] |
| (Role\_Name EQUALS Receptionist) | [TACACS+ Receptionist] |
| (Role\_Name EQUALS Super Administrator) | [TACACS+ Super Admin] |
| (Role\_Name EQUALS Read-only Administrator) | [TACACS+ Read-only Admin] |
| (Role\_Name EQUALS API Administrator) | [TACACS+ API Admin] |

Table - Rules : [Admin Network Login Policy]

### 1.6.3.2 Enforcement Policy: [AirGroup Enforcement Policy]

|  |  |
| --- | --- |
| Id | 7 |
| Name | [AirGroup Enforcement Policy] |
| Type | RADIUS |
| Default | [AirGroup Response] |
| Rule Algo | evaluate-all |

Table - Enforcement Policy: [AirGroup Enforcement Policy]

| Condition | Enforcement Profiles |
| --- | --- |
| (airgroup\_enable EQUALS 1) AND (airgroup\_shared EQUALS 1) AND (airgroup\_shared\_time MATCHES\_REGEX .) AND (AccountStatus EQUALS 0) | [AirGroup Response], [Handle AirGroup Time Sharing] |
| (airgroup\_enable EQUALS 1) AND (airgroup\_shared EQUALS 1) AND (airgroup\_shared\_time NOT\_MATCHES\_REGEX .) AND (airgroup\_shared\_group MATCHES\_REGEX .) AND (AccountStatus EQUALS 0) AND (Role EQUALS [AirGroup v2]) | [AirGroup Response], [AirGroup Shared Device] |
| (airgroup\_enable EQUALS 1) AND (airgroup\_shared EQUALS 1) AND (airgroup\_shared\_time NOT\_MATCHES\_REGEX .) AND (airgroup\_shared\_group NOT\_MATCHES\_REGEX .) AND (AccountStatus EQUALS 0) | [AirGroup Response], [AirGroup Shared Device] |
| (airgroup\_enable EQUALS 1) AND (airgroup\_shared NOT\_EQUALS 1) AND (AccountStatus EQUALS 0) | [AirGroup Response], [AirGroup Personal Device] |

Table - Rules : [AirGroup Enforcement Policy]

### 1.6.3.3 Enforcement Policy: [Aruba Device Access Policy]

|  |  |
| --- | --- |
| Id | 17 |
| Name | [Aruba Device Access Policy] |
| Type | TACACS |
| Default | [ArubaOS Wireless - TACACS+ Read-Only Access] |
| Rule Algo | first-applicable |

Table - Enforcement Policy: [Aruba Device Access Policy]

| Condition | Enforcement Profiles |
| --- | --- |
| (Role MATCHES\_ANY [Aruba TACACS+ root Admin]) | [ArubaOS Wireless - TACACS+ Root Access] |
| (Role MATCHES\_ANY [Aruba TACACS+ read-only Admin]) | [ArubaOS Wireless - TACACS+ Read-Only Access] |

Table - Rules : [Aruba Device Access Policy]

### 1.6.3.4 Enforcement Policy: [Guest Operator Logins]

|  |  |
| --- | --- |
| Id | 18 |
| Name | [Guest Operator Logins] |
| Type | Application |
| Default | [Deny Application Access Profile] |
| Rule Algo | first-applicable |

Table - Enforcement Policy: [Guest Operator Logins]

| Condition | Enforcement Profiles |
| --- | --- |
| (Role EQUALS [User Authenticated]) AND (Source EQUALS [Local User Repository]) | [Operator Login - Local Users] |
| (Role EQUALS [User Authenticated]) AND (Source EQUALS [Admin User Repository]) | [Operator Login - Admin Users] |

Table - Rules : [Guest Operator Logins]

### 1.6.3.5 Enforcement Policy: [Insight Operator Logins]

|  |  |
| --- | --- |
| Id | 19 |
| Name | [Insight Operator Logins] |
| Type | Application |
| Default | [Deny Application Access Profile] |
| Rule Algo | first-applicable |

Table - Enforcement Policy: [Insight Operator Logins]

| Condition | Enforcement Profiles |
| --- | --- |
| (Role EQUALS [User Authenticated]) AND (Source EQUALS [Local User Repository]) | [Operator Login - Local Users] |

Table - Rules : [Insight Operator Logins]

### 1.6.3.6 Enforcement Policy: [Device Registration Disconnect]

|  |  |
| --- | --- |
| Id | 20 |
| Name | [Device Registration Disconnect] |
| Type | WEBAUTH |
| Default | [ArubaOS Wireless - Terminate Session] |
| Rule Algo | first-applicable |

Table - Enforcement Policy: [Device Registration Disconnect]

| Condition | Enforcement Profiles |
| --- | --- |
| (Source EQUALS [Guest Device Repository]) | [ArubaOS Wireless - Terminate Session], [Aerohive - Terminate Session], [Cisco - Terminate Session], [H3C - Terminate Session], [Juniper Terminate Session], [Motorola - Terminate Session], [Trapeze - Terminate Session], [ArubaOS Switching - Terminate Session], [AOS-CX - Disconnect] |

Table - Rules : [Device Registration Disconnect]

### 1.6.3.7 Enforcement Policy: [Sample Allow Access Policy]

|  |  |
| --- | --- |
| Id | 3001 |
| Name | [Sample Allow Access Policy] |
| Type | RADIUS |
| Default | [Allow Access Profile] |
| Rule Algo | evaluate-all |

Table - Enforcement Policy: [Sample Allow Access Policy]

| Condition | Enforcement Profiles |
| --- | --- |
| (Day-of-Week BELONGS\_TO Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, Sunday) | [Allow Access Profile] |

Table - Rules : [Sample Allow Access Policy]

### 1.6.3.8 Enforcement Policy: [Sample Deny Access Policy]

|  |  |
| --- | --- |
| Id | 3002 |
| Name | [Sample Deny Access Policy] |
| Type | RADIUS |
| Default | [Deny Access Profile] |
| Rule Algo | evaluate-all |

Table - Enforcement Policy: [Sample Deny Access Policy]

| Condition | Enforcement Profiles |
| --- | --- |
| (Day-of-Week BELONGS\_TO Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, Sunday) | [Deny Access Profile] |

Table - Rules : [Sample Deny Access Policy]

### 1.6.3.9 Enforcement Policy: ws\_wireless\_802.1X

|  |  |
| --- | --- |
| Id | 3004 |
| Name | ws\_wireless\_802.1X |
| Type | RADIUS |
| Default | [Deny Access Profile] |
| Rule Algo | first-applicable |

Table - Enforcement Policy: ws\_wireless\_802.1X

| Condition | Enforcement Profiles |
| --- | --- |
| (Compromised EQUALS true) | ws\_role\_quarantine |
| (totalAlerts NOT\_EQUALS 0) AND (totalAlerts EXISTS &nbsp;) | ws\_role\_quarantine |
| (Role EQUALS ws\_Admin) | ws\_role\_admin, ws\_airheads\_security\_update |
| (Role EQUALS ws\_Contractor) AND (Posture NOT\_EQUALS HEALTHY (0)) | ws\_role\_onguard-redirect, ws\_vlan14\_untrust\_aruba, ws\_airheads\_security\_update |
| (Role EQUALS ws\_Contractor) AND (Role EQUALS ws\_Onboarded) | ws\_role\_contractor, ws\_vlan14\_untrust\_aruba, ws\_airheads\_security\_update |
| (Role EQUALS ws\_Employee) AND (Role EQUALS [Machine Authenticated]) | ws\_role\_employee, ws\_vlan11\_corporate\_aruba, ws\_airheads\_security\_update |
| (Role EQUALS ws\_Employee) AND (Role EQUALS ws\_Onboarded) | ws\_role\_BYOD, ws\_vlan13\_guest\_aruba, ws\_airheads\_security\_update |
| (Role MATCHES\_ANY ws\_Contractor<br>ws\_Employee) | ws\_role\_onboard-redirect |
| (Role EQUALS [Machine Authenticated]) | ws\_role\_employee, ws\_vlan11\_corporate\_aruba, ws\_airheads\_security\_update |

Table - Rules : ws\_wireless\_802.1X

### 1.6.3.10 Enforcement Policy: ws\_CPPM\_Admin\_policy

|  |  |
| --- | --- |
| Id | 3005 |
| Name | ws\_CPPM\_Admin\_policy |
| Type | TACACS |
| Default | [TACACS+ Deny Profile] |
| Rule Algo | first-applicable |

Table - Enforcement Policy: ws\_CPPM\_Admin\_policy

| Condition | Enforcement Profiles |
| --- | --- |
| (Role EQUALS ws\_Admin) | [TACACS+ Read-only Admin] |
| (Role EQUALS ws\_Helpdesk) | [TACACS+ Read-only Admin] |

Table - Rules : ws\_CPPM\_Admin\_policy

### 1.6.3.11 Enforcement Policy: ws\_AOS-S\_Admin-access

|  |  |
| --- | --- |
| Id | 3006 |
| Name | ws\_AOS-S\_Admin-access |
| Type | TACACS |
| Default | [TACACS+ Deny Profile] |
| Rule Algo | first-applicable |

Table - Enforcement Policy: ws\_AOS-S\_Admin-access

| Condition | Enforcement Profiles |
| --- | --- |
| (Role EQUALS ws\_Admin) | ws\_AOS-S-mgt-RW |
| (Role EQUALS ws\_Helpdesk) | ws\_AOS-S-mgt-RO |

Table - Rules : ws\_AOS-S\_Admin-access

### 1.6.3.12 Enforcement Policy: ws\_ArubaOS-Switch-MAC

|  |  |
| --- | --- |
| Id | 3007 |
| Name | ws\_ArubaOS-Switch-MAC |
| Type | RADIUS |
| Default | ws\_vlan14\_untrust |
| Rule Algo | first-applicable |

Table - Enforcement Policy: ws\_ArubaOS-Switch-MAC

| Condition | Enforcement Profiles |
| --- | --- |
| (Category EQUALS VoIP Phone) | ws\_vlan\_voice, ws\_dACL\_voice |
| (Device Name EQUALS Raspberry Pi) | ws\_vlan\_untrust, ws\_dACL\_unmanaged\_IoT |
| (Category EQUALS Network Camera) | ws\_vlan\_corporate, ws\_dACL\_camera |
| (Category EQUALS Printer) | ws\_dACL\_internal\_only, ws\_vlan\_corporate |
| (Ownership EQUALS IAP) | ws\_iap\_with\_tagged\_vlans |
| (Device Name EQUALS Aruba AP) | ws\_vlan\_management |
| (Role EQUALS [Guest]) | ws\_dACL\_untrusted, ws\_vlan\_guest |
| (Role EQUALS [User Authenticated]) | ws\_vlan\_untrust, ws\_dACL\_redirect |

Table - Rules : ws\_ArubaOS-Switch-MAC

### 1.6.3.13 Enforcement Policy: ws\_ArubaOS-Switch-802.1X

|  |  |
| --- | --- |
| Id | 3008 |
| Name | ws\_ArubaOS-Switch-802.1X |
| Type | RADIUS |
| Default | [Deny Access Profile] |
| Rule Algo | first-applicable |

Table - Enforcement Policy: ws\_ArubaOS-Switch-802.1X

| Condition | Enforcement Profiles |
| --- | --- |
| (Role EQUALS ws\_Admin) | ws\_vlan10\_management |
| (Role EQUALS ws\_Contractor) | ws\_vlan14\_untrust, ws\_dACL\_untrusted |
| (Role EQUALS ws\_Employee) | ws\_vlan11\_corporate |
| (Role EQUALS [Machine Authenticated]) | ws\_vlan11\_corporate |
| (Username EQUALS ap1x) | ws\_iap\_with\_tagged\_vlans |

Table - Rules : ws\_ArubaOS-Switch-802.1X

### 1.6.3.14 Enforcement Policy: ws\_Guest MAC Authentication Enforcement Policy

|  |  |
| --- | --- |
| Id | 3009 |
| Name | ws\_Guest MAC Authentication Enforcement Policy |
| Type | RADIUS |
| Default | [Deny Access Profile] |
| Rule Algo | first-applicable |

Table - Enforcement Policy: ws\_Guest MAC Authentication Enforcement Policy

| Condition | Enforcement Profiles |
| --- | --- |
| (Role MATCHES\_ALL [MAC Caching]<br>[Guest]<br>[User Authenticated]) | [Allow Access Profile], ws\_Guest Guest Profile |
| (Role MATCHES\_ANY [Guest]<br>[Contractor]<br>[Employee]) | [Allow Access Profile], ws\_Guest Captive Portal Profile |

Table - Rules : ws\_Guest MAC Authentication Enforcement Policy

### 1.6.3.15 Enforcement Policy: ws\_Guest User Authentication with MAC Caching Enforcement Policy

|  |  |
| --- | --- |
| Id | 3010 |
| Name | ws\_Guest User Authentication with MAC Caching Enforcement Policy |
| Type | RADIUS |
| Default | [Allow Access Profile] |
| Rule Algo | first-applicable |

Table - Enforcement Policy: ws\_Guest User Authentication with MAC Caching Enforcement Policy

| Condition | Enforcement Profiles |
| --- | --- |
| (Unique-Device-Count GREATER\_THAN 1) | [Deny Access Profile] |
| (Role EQUALS [Guest]) AND (Day-of-Week BELONGS\_TO Monday,Tuesday,Wednesday,Thursday,Friday,Saturday,Sunday) | ws\_Guest MAC Caching Session Timeout, ws\_Guest MAC Caching Bandwidth Limit, ws\_Guest MAC Caching Session Limit, ws\_Guest Guest MAC Caching, [Update Endpoint Known], ws\_Guest MAC Caching Do Expire, ws\_Guest MAC Caching Expire Post Login, ws\_Guest Guest Profile |

Table - Rules : ws\_Guest User Authentication with MAC Caching Enforcement Policy

### 1.6.3.16 Enforcement Policy: ws\_GuestOperator

|  |  |
| --- | --- |
| Id | 3011 |
| Name | ws\_GuestOperator |
| Type | Application |
| Default | [Deny Application Access Profile] |
| Rule Algo | first-applicable |

Table - Enforcement Policy: ws\_GuestOperator

| Condition | Enforcement Profiles |
| --- | --- |
| (Role EQUALS ws\_Employee) | ws\_Operator\_Device\_Registration |
| (Role EQUALS ws\_Helpdesk) | ws\_Operator\_Receptionist |
| (Role EQUALS ws\_Admin) | ws\_Operator\_Super\_Administrator |

Table - Rules : ws\_GuestOperator

### 1.6.3.17 Enforcement Policy: ws\_Onboard

|  |  |
| --- | --- |
| Id | 3012 |
| Name | ws\_Onboard |
| Type | Application |
| Default | [Deny Application Access Profile] |
| Rule Algo | first-applicable |

Table - Enforcement Policy: ws\_Onboard

| Condition | Enforcement Profiles |
| --- | --- |
| (Role EQUALS ws\_Employee) | [Allow Application Access Profile] |
| (Role EQUALS ws\_Contractor) | [Allow Application Access Profile] |

Table - Rules : ws\_Onboard

### 1.6.3.18 Enforcement Policy: ws\_Bounce\_client\_wired

|  |  |
| --- | --- |
| Id | 3013 |
| Name | ws\_Bounce\_client\_wired |
| Type | WEBAUTH |
| Default | [ArubaOS Switching - Bounce Switch Port] |
| Rule Algo | first-applicable |

Table - Enforcement Policy: ws\_Bounce\_client\_wired

| Condition | Enforcement Profiles |
| --- | --- |
| (Posture EXISTS &nbsp;) | [ArubaOS Switching - Terminate Session] |

Table - Rules : ws\_Bounce\_client\_wired

### 1.6.3.19 Enforcement Policy: ws\_tunneled\_802.1X

|  |  |
| --- | --- |
| Id | 3014 |
| Name | ws\_tunneled\_802.1X |
| Type | RADIUS |
| Default | [Deny Access Profile] |
| Rule Algo | first-applicable |

Table - Enforcement Policy: ws\_tunneled\_802.1X

| Condition | Enforcement Profiles |
| --- | --- |
| (Role EQUALS ws\_Admin) | ws\_role\_admin, ws\_vlan203\_tunneled\_aruba |
| (Role EQUALS ws\_Contractor) AND (Role EQUALS ws\_Onboarded) | ws\_role\_contractor, ws\_vlan203\_tunneled\_aruba |
| (Role EQUALS ws\_Employee) | ws\_role\_employee, ws\_vlan203\_tunneled\_aruba |
| (Role EQUALS [Machine Authenticated]) | ws\_role\_employee, ws\_vlan203\_tunneled\_aruba |

Table - Rules : ws\_tunneled\_802.1X

### 1.6.3.20 Enforcement Policy: ws\_tunneled-MAC

|  |  |
| --- | --- |
| Id | 3015 |
| Name | ws\_tunneled-MAC |
| Type | RADIUS |
| Default | [Deny Access Profile] |
| Rule Algo | first-applicable |

Table - Enforcement Policy: ws\_tunneled-MAC

| Condition | Enforcement Profiles |
| --- | --- |
| (Category EQUALS VoIP Phone) | ws\_role\_voice, ws\_vlan203\_tunneled\_aruba |
| (Category EQUALS Computer) | ws\_vlan203\_tunneled\_aruba, ws\_role\_voice |

Table - Rules : ws\_tunneled-MAC

### 1.6.3.21 Enforcement Policy: ws\_HPE-Terminate-Session

|  |  |
| --- | --- |
| Id | 3016 |
| Name | ws\_HPE-Terminate-Session |
| Type | WEBAUTH |
| Default | [ArubaOS Switching - Terminate Session] |
| Rule Algo | first-applicable |

Table - Enforcement Policy: ws\_HPE-Terminate-Session

| Condition | Enforcement Profiles |
| --- | --- |
| (Role EQUALS [User Authenticated]) | [ArubaOS Switching - Terminate Session] |

Table - Rules : ws\_HPE-Terminate-Session

### 1.6.3.22 Enforcement Policy: ws\_ArubaOS-Switch-802.1X-roles

|  |  |
| --- | --- |
| Id | 3017 |
| Name | ws\_ArubaOS-Switch-802.1X-roles |
| Type | RADIUS |
| Default | [Deny Access Profile] |
| Rule Algo | first-applicable |

Table - Enforcement Policy: ws\_ArubaOS-Switch-802.1X-roles

| Condition | Enforcement Profiles |
| --- | --- |
| (Role EQUALS ws\_Admin) | ws\_hpe\_role\_admin |
| (Role EQUALS ws\_Contractor) | ws\_hpe\_role\_contractor |
| (Role EQUALS ws\_Employee) | ws\_hpe\_role\_employee |
| (Role EQUALS [Machine Authenticated]) | ws\_hpe\_role\_employee |

Table - Rules : ws\_ArubaOS-Switch-802.1X-roles

### 1.6.3.23 Enforcement Policy: ws\_ArubaOS-Switch-MAC-roles

|  |  |
| --- | --- |
| Id | 3018 |
| Name | ws\_ArubaOS-Switch-MAC-roles |
| Type | RADIUS |
| Default | ws\_hpe\_role\_guest-redirect |
| Rule Algo | first-applicable |

Table - Enforcement Policy: ws\_ArubaOS-Switch-MAC-roles

| Condition | Enforcement Profiles |
| --- | --- |
| (Category EQUALS VoIP Phone) | ws\_hpe\_role\_voice |
| (Category EQUALS Network Camera) | ws\_hpe\_role\_camera |
| (Role EQUALS [Guest]) | ws\_hpe\_role\_guest |
| (Role EQUALS [User Authenticated]) | ws\_hpe\_role\_guest-redirect |
| (Role EQUALS ws\_Contractor) | ws\_hpe\_role\_contractor |
| (Role EQUALS ws\_Employee) | ws\_hpe\_role\_employee |

Table - Rules : ws\_ArubaOS-Switch-MAC-roles

### 1.6.3.24 Enforcement Policy: ws\_Allow\_Admins

|  |  |
| --- | --- |
| Id | 3019 |
| Name | ws\_Allow\_Admins |
| Type | RADIUS |
| Default | [Deny Access Profile] |
| Rule Algo | first-applicable |

Table - Enforcement Policy: ws\_Allow\_Admins

| Condition | Enforcement Profiles |
| --- | --- |
| (Role EQUALS ws\_Admin) | [Allow Access Profile] |

Table - Rules : ws\_Allow\_Admins

### 1.6.3.25 Enforcement Policy: ws\_AOS-S-Admin-RADIUS

|  |  |
| --- | --- |
| Id | 3020 |
| Name | ws\_AOS-S-Admin-RADIUS |
| Type | RADIUS |
| Default | [Deny Access Profile] |
| Rule Algo | first-applicable |

Table - Enforcement Policy: ws\_AOS-S-Admin-RADIUS

| Condition | Enforcement Profiles |
| --- | --- |
| (Role EQUALS ws\_Admin) | ws\_AOS-SW-Admin-priv |

Table - Rules : ws\_AOS-S-Admin-RADIUS

### 1.6.3.26 Enforcement Policy: ws\_Ingress\_Security\_Events

|  |  |
| --- | --- |
| Id | 3021 |
| Name | ws\_Ingress\_Security\_Events |
| Type | Event |
| Default | ws\_quarantine\_set\_security\_info\_checkpoint |
| Rule Algo | first-applicable |

Table - Enforcement Policy: ws\_Ingress\_Security\_Events

| Condition | Enforcement Profiles |
| --- | --- |
| (ConfidenceLevel EXISTS &nbsp;) | ws\_quarantine\_set\_security\_info\_checkpoint |
| (application-name EXISTS &nbsp;) | ws\_quarantine\_set\_security\_info\_juniper\_srx, [ArubaOS Wireless - Terminate Session] |

Table - Rules : ws\_Ingress\_Security\_Events

### 1.6.3.27 Enforcement Policy: ws\_release\_from\_quarantine

|  |  |
| --- | --- |
| Id | 3022 |
| Name | ws\_release\_from\_quarantine |
| Type | Application |
| Default | [Deny Application Access Profile] |
| Rule Algo | first-applicable |

Table - Enforcement Policy: ws\_release\_from\_quarantine

| Condition | Enforcement Profiles |
| --- | --- |
| (Threat Release Timeout NOT\_EXISTS &nbsp;) | [Allow Application Access Profile], ws\_quarantine\_reset\_and\_set\_timestamp, [ArubaOS Wireless - Terminate Session] |
| (Now DT GREATER\_THAN %{Endpoint:Threat Release Timeout}) | [Allow Application Access Profile], ws\_quarantine\_reset\_and\_set\_timestamp, [ArubaOS Wireless - Terminate Session] |
| (Role EQUALS [User Authenticated]) | ws\_quarantine\_release\_error |

Table - Rules : ws\_release\_from\_quarantine

### 1.6.3.28 Enforcement Policy: ws\_OnConnect

|  |  |
| --- | --- |
| Id | 3023 |
| Name | ws\_OnConnect |
| Type | WEBAUTH |
| Default | ws\_snmp\_vlan14\_untrust |
| Rule Algo | first-applicable |

Table - Enforcement Policy: ws\_OnConnect

| Condition | Enforcement Profiles |
| --- | --- |
| (Category EQUALS VoIP Phone) | ws\_snmp\_vlan12\_voice, ws\_snmp\_bounce\_port |
| (Full-Username EXISTS &nbsp;) | ws\_snmp\_vlan11\_corporate, ws\_snmp\_vlan31, ws\_snmp\_bounce\_port |
| (Role EQUALS [User Authenticated]) | ws\_snmp\_vlan14\_untrust, ws\_snmp\_bounce\_port |

Table - Rules : ws\_OnConnect

### 1.6.3.29 Enforcement Policy: ws\_Application\_allow\_all

|  |  |
| --- | --- |
| Id | 3024 |
| Name | ws\_Application\_allow\_all |
| Type | Application |
| Default | [Allow Application Access Profile] |
| Rule Algo | first-applicable |

Table - Enforcement Policy: ws\_Application\_allow\_all

| Condition | Enforcement Profiles |
| --- | --- |
| (Role EQUALS [User Authenticated]) | [Allow Application Access Profile] |

Table - Rules : ws\_Application\_allow\_all

### 1.6.3.30 Enforcement Policy: ws\_Aruba\_Terminate\_Session

|  |  |
| --- | --- |
| Id | 3025 |
| Name | ws\_Aruba\_Terminate\_Session |
| Type | WEBAUTH |
| Default | [ArubaOS Wireless - Terminate Session] |
| Rule Algo | first-applicable |

Table - Enforcement Policy: ws\_Aruba\_Terminate\_Session

| Condition | Enforcement Profiles |
| --- | --- |
| (Role EQUALS [User Authenticated]) | [ArubaOS Wireless - Terminate Session] |

Table - Rules : ws\_Aruba\_Terminate\_Session

### 1.6.3.31 Enforcement Policy: ws\_Airwave\_admin

|  |  |
| --- | --- |
| Id | 3029 |
| Name | ws\_Airwave\_admin |
| Type | RADIUS |
| Default | [Deny Access Profile] |
| Rule Algo | first-applicable |

Table - Enforcement Policy: ws\_Airwave\_admin

| Condition | Enforcement Profiles |
| --- | --- |
| (Role EQUALS ws\_Admin) | ws\_Airwave\_admin |

Table - Rules : ws\_Airwave\_admin

### 1.6.3.32 Enforcement Policy: ws\_ArubaOS-Switch-802.1X-putn

|  |  |
| --- | --- |
| Id | 3031 |
| Name | ws\_ArubaOS-Switch-802.1X-putn |
| Type | RADIUS |
| Default | [Deny Access Profile] |
| Rule Algo | first-applicable |

Table - Enforcement Policy: ws\_ArubaOS-Switch-802.1X-putn

| Condition | Enforcement Profiles |
| --- | --- |
| (Role EQUALS ws\_Admin) | ws\_hpe\_role\_admin |
| (Role EQUALS ws\_Contractor) | ws\_hpe\_role\_contractor-tun |
| (Role EQUALS ws\_Employee) | ws\_hpe\_role\_employee |
| (Role EQUALS [Machine Authenticated]) | ws\_hpe\_role\_employee |

Table - Rules : ws\_ArubaOS-Switch-802.1X-putn

### 1.6.3.33 Enforcement Policy: ws\_ArubaOS-Switch-MAC-putn

|  |  |
| --- | --- |
| Id | 3032 |
| Name | ws\_ArubaOS-Switch-MAC-putn |
| Type | RADIUS |
| Default | ws\_hpe\_role\_profiler |
| Rule Algo | first-applicable |

Table - Enforcement Policy: ws\_ArubaOS-Switch-MAC-putn

| Condition | Enforcement Profiles |
| --- | --- |
| (Category EQUALS VoIP Phone) | ws\_hpe\_role\_voice |
| (Category EQUALS Network Camera) | ws\_hpe\_role\_camera |
| (Device Name EQUALS Raspberry Pi) | radius\_rapi |
| (Role EQUALS [Guest]) | ws\_hpe\_role\_guest-tun |
| (Role EQUALS [User Authenticated]) | ws\_hpe\_role\_contractor |

Table - Rules : ws\_ArubaOS-Switch-MAC-putn

### 1.6.3.34 Enforcement Policy: ws\_ArubaOS-Switch-802.1X-roles-dur

|  |  |
| --- | --- |
| Id | 3033 |
| Name | ws\_ArubaOS-Switch-802.1X-roles-dur |
| Type | RADIUS |
| Default | [Deny Access Profile] |
| Rule Algo | first-applicable |

Table - Enforcement Policy: ws\_ArubaOS-Switch-802.1X-roles-dur

| Condition | Enforcement Profiles |
| --- | --- |
| (Role EQUALS ws\_Admin) | ws\_hpe\_role\_admin-tun |
| (Role EQUALS ws\_Contractor) | ws\_hpe\_role\_contractor-tun |
| (Role EQUALS ws\_Employee) | ws\_dur\_employee |
| (Role EQUALS [Machine Authenticated]) | ws\_dur\_employee |

Table - Rules : ws\_ArubaOS-Switch-802.1X-roles-dur

### 1.6.3.35 Enforcement Policy: ws\_ArubaOS-Switch-MAC-dur

|  |  |
| --- | --- |
| Id | 3034 |
| Name | ws\_ArubaOS-Switch-MAC-dur |
| Type | RADIUS |
| Default | ws\_hpe\_role\_profiler |
| Rule Algo | first-applicable |

Table - Enforcement Policy: ws\_ArubaOS-Switch-MAC-dur

| Condition | Enforcement Profiles |
| --- | --- |
| (Category EQUALS VoIP Phone) | ws\_dur\_voice |
| (Category EQUALS Network Camera) | ws\_dur\_camera |
| (Device Name EQUALS Raspberry Pi) | ws\_hpe\_role\_iot-tun |
| (Role EQUALS [Guest]) | ws\_hpe\_role\_guest-tun |
| (Role EQUALS [User Authenticated]) | ws\_dur\_redirect |

Table - Rules : ws\_ArubaOS-Switch-MAC-dur

### 1.6.4 Enforcement Profile

The following section details Enforcement Profile configured on ClearPass.

| Id | Name | Type | Description | Action | Attribute | Ref |
| --- | --- | --- | --- | --- | --- | --- |
| 1 | [Allow Access Profile] | RADIUS | System-defined profile to allow network access | Accept | 1 | 3 |
| 2 | [Deny Access Profile] | RADIUS | System-defined profile to deny network access | Reject | 1 | 2 |
| 3 | [Drop Access Profile] | RADIUS | System-defined profile to drop the request | Drop | 1 | 0 |
| 12 | [TACACS+ Deny Profile] | TACACS | System-defined profile to deny network access | Accept | 1 | 0 |
| 13 | [TACACS+ Super Admin] | TACACS | Super admin access for Policy Manager Admin | Accept | 2 | 1 |
| 15 | [TACACS+ Network Admin] | TACACS | Network admin access for Policy Manager Admin | Accept | 1 | 1 |
| 16 | [TACACS+ Help Desk] | TACACS | Help desk access for Policy Manager Admin | Accept | 1 | 1 |
| 17 | [TACACS+ Receptionist] | TACACS | Receptionist access for Policy Manager Admin | Accept | 1 | 1 |
| 18 | [TACACS+ Read-only Admin] | TACACS | Read-only admin access for Policy Manager Admin | Accept | 1 | 2 |
| 19 | [TACACS+ API Admin] | TACACS | API admin access for Policy Manager Admin | Accept | 1 | 1 |
| 20 | [ArubaOS Wireless - TACACS+ Root Access] | TACACS | System-defined profile for TACACS+ root access on ArubaOS Mobility Controllers, Aruba Instant APs & Mobility Access Switches. | Accept | 1 | 1 |
| 21 | [ArubaOS Wireless - TACACS+ Read-Only Access] | TACACS | System-defined profile for TACACS+ read-only access on ArubaOS Mobility Controllers, Aruba Instant APs & Mobility Access Switches. | Accept | 1 | 1 |
| 31 | [Deny Application Access Profile] | Application | System-defined profile to deny access to application | Reject | 1 | 0 |
| 32 | [Allow Application Access Profile] | Application | System-defined profile to allow access to application | Accept | 1 | 3 |
| 33 | [Handle AirGroup Time Sharing] | HTTP | System-defined profile to send time-based sharing policy to the AirGroup notification service |  | 2 | 1 |
| 40 | [AirGroup Response] | RADIUS | System-defined profile for any AirGroup request | Accept | 3 | 1 |
| 41 | [AirGroup Personal Device] | RADIUS | System-defined profile for an AirGroup personal device request | Accept | 3 | 1 |
| 42 | [AirGroup Shared Device] | RADIUS | System-defined profile for an AirGroup shared device request | Accept | 5 | 1 |
| 43 | [Return Device Sponsor Name - RADIUS User-Name] | RADIUS | Returns a device's owner (sponsor name) as the IETF User-Name | Accept | 1 | 0 |
| 44 | [Registered Device MPSK] | RADIUS | Returns a device's assigned MPSK that was generated automatically during Device Registration | Accept | 1 | 0 |
| 51 | [Update Endpoint Known] | Post\_Authentication | System-defined profile to change Endpoint's status to Known |  | 1 | 1 |
| 61 | [Operator Login - Local Users] | Application | Enforcement profile for Guest operator logins | Accept | 1 | 2 |
| 62 | [Operator Login - Admin Users] | Application | Enforcement profile for Guest admin logins | Accept | 1 | 1 |
| 101 | [Cisco - Terminate Session] | RADIUS\_DynAuthZ | System-defined profile to disconnect user (Cisco) |  | 2 | 1 |
| 102 | [Cisco - Disable Host-Port] | RADIUS\_DynAuthZ | System-defined profile to disable host port (Cisco) |  | 2 | 0 |
| 103 | [Cisco - Bounce-Host-Port] | RADIUS\_DynAuthZ | System-defined profile to bounce host port (Cisco) |  | 2 | 0 |
| 104 | [Cisco - Reauthenticate-Session] | RADIUS\_DynAuthZ | System-defined profile to re-authenticate session (Cisco) |  | 2 | 0 |
| 105 | [ArubaOS Switching - Terminate Session] | RADIUS\_DynAuthZ | System-defined profile to disconnect the user on ArubaOS Switching, HP ProCurve and HP UWW products. |  | 5 | 3 |
| 106 | [ArubaOS Wireless - Terminate Session] | RADIUS\_DynAuthZ | System-defined profile to disconnect the user on ArubaOS Mobility Controllers, Aruba Instant APs & Mobility Access Switches. |  | 1 | 4 |
| 107 | [Juniper Terminate Session] | RADIUS\_DynAuthZ | System-defined profile to disconnect user (Juniper) |  | 2 | 1 |
| 108 | [Trapeze - Terminate Session] | RADIUS\_DynAuthZ | System-defined profile to disconnect user (Trapeze) |  | 3 | 1 |
| 109 | [Aerohive - Terminate Session] | RADIUS\_DynAuthZ | System-defined profile to disconnect user (Aerohive) |  | 3 | 1 |
| 110 | [Motorola - Terminate Session] | RADIUS\_DynAuthZ | System-defined profile to disconnect user (Motorola) |  | 3 | 1 |
| 111 | [ArubaOS Wireless - Bounce Switch Port] | RADIUS\_DynAuthZ | System-defined profile to bounce the switch port on ArubaOS Mobility Controllers, Multi-Port APs & Mobility Access Switches. |  | 2 | 0 |
| 112 | [ArubaOS Switching - Bounce Switch Port] | RADIUS\_DynAuthZ | System-defined profile to bounce the switch port on ArubaOS Switching products. |  | 6 | 0 |
| 113 | [H3C - Terminate Session] | RADIUS\_DynAuthZ | System-defined profile to disconnect the user on H3C products (including HPE FlexNetwork / Comware). |  | 2 | 1 |
| 114 | [H3C - Bounce Switch Port] | RADIUS\_DynAuthZ | System-defined profile to bounce the switch port on H3C products (including HPE FlexNetwork / Comware). |  | 2 | 0 |
| 115 | [H3C - Disable Switch Port] | RADIUS\_DynAuthZ | System-defined profile to disable the switch port on H3C products (including HPE FlexNetwork / Comware). |  | 2 | 0 |
| 116 | [Tellabs - Bounce Host Port] | RADIUS\_DynAuthZ | System-defined profile to bounce host port (Tellabs) |  | 3 | 0 |
| 117 | [Tellabs - Disable Host Port] | RADIUS\_DynAuthZ | System-defined profile to disable host port (Tellabs) |  | 3 | 0 |
| 118 | [Tellabs - Reauthenticate Session] | RADIUS\_DynAuthZ | System-defined profile to re-authenticate session (Tellabs) |  | 2 | 0 |
| 119 | [Tellabs - Terminate Session] | RADIUS\_DynAuthZ | System-defined profile to disconnect user (Tellabs) |  | 2 | 0 |
| 120 | [Cisco ASA - Terminate Session] | RADIUS\_DynAuthZ | System-defined profile to disconnect user (Cisco ASA) |  | 3 | 0 |
| 121 | [AOS-CX - Disconnect] | RADIUS\_DynAuthZ | System-defined profile to disconnect a device on AOS-CX switches. |  | 5 | 1 |
| 122 | [AOS-CX - Bounce Switch Port] | RADIUS\_DynAuthZ | System-defined profile to bounce the switch port on AOS-CX switches. |  | 6 | 0 |
| 123 | [Meraki - Terminate Session] | RADIUS\_DynAuthZ | System-defined profile to disconnect user (Meraki) |  | 3 | 0 |
| 124 | [Arista Wireless - Terminate Session] | RADIUS\_DynAuthZ | System-defined profile to disconnect user (Arista Wireless) |  | 2 | 0 |
| 125 | [Arista Wired - Terminate Session] | RADIUS\_DynAuthZ | System-defined profile to disconnect user (Arista Wired) |  | 5 | 0 |
| 3001 | ws\_role\_employee | RADIUS | Aruba Employee Role | Accept | 1 | 2 |
| 3002 | ws\_role\_voice | RADIUS | Aruba Voice Role | Accept | 1 | 1 |
| 3003 | ws\_role\_BYOD | RADIUS | Aruba BYOD Role | Accept | 1 | 1 |
| 3004 | ws\_role\_admin | RADIUS | Aruba Admin Role | Accept | 1 | 2 |
| 3005 | ws\_role\_contractor | RADIUS | Aruba Contractor Role | Accept | 1 | 2 |
| 3006 | ws\_vlan11\_corporate | RADIUS | Return the corporate VLAN11 | Accept | 5 | 1 |
| 3007 | ws\_vlan12\_voice | RADIUS | Return the voice VLAN12 | Accept | 5 | 0 |
| 3008 | ws\_vlan13\_guest | RADIUS | Return the guest VLAN13 | Accept | 5 | 0 |
| 3009 | ws\_vlan14\_untrust | RADIUS | Return the untrusted VLAN14 | Accept | 5 | 1 |
| 3010 | ws\_vlan10\_management | RADIUS | Return the management VLAN10 | Accept | 5 | 1 |
| 3011 | ws\_vlan10\_management\_aruba | RADIUS | Return the management VLAN10 | Accept | 1 | 0 |
| 3012 | ws\_vlan11\_corporate\_aruba | RADIUS | Return the corporate VLAN11 | Accept | 1 | 1 |
| 3013 | ws\_vlan13\_guest\_aruba | RADIUS | Return the guest VLAN13 | Accept | 1 | 1 |
| 3014 | ws\_vlan14\_untrust\_aruba | RADIUS | Return the untrusted VLAN14 | Accept | 1 | 1 |
| 3015 | ws\_vlan12\_voice\_aruba | RADIUS | Return the voice VLAN12 | Accept | 1 | 0 |
| 3016 | ws\_AOS-S-mgt-RW | TACACS | ArubaOS Switches Admin access Read-Write | Accept | 1 | 1 |
| 3017 | ws\_AOS-S-mgt-RO | TACACS | ArubaOS Switches Admin access Read-Only | Accept | 1 | 1 |
| 3018 | ws\_Guest Guest Profile | RADIUS | Role/VLAN enforcement for Guest | Accept | 2 | 2 |
| 3019 | ws\_Guest Captive Portal Profile | RADIUS | Captive Portal Role/VLAN enforcement | Accept | 1 | 1 |
| 3020 | ws\_Guest MAC Caching Session Timeout | RADIUS |  | Accept | 1 | 1 |
| 3021 | ws\_Guest MAC Caching Do Expire | Post\_Authentication | Enforcement profile for User do expire functionality |  | 1 | 1 |
| 3022 | ws\_Guest MAC Caching Expire Post Login | Post\_Authentication | Enforcement profile for User expire post login functionality |  | 1 | 1 |
| 3023 | ws\_Guest MAC Caching Bandwidth Limit | Post\_Authentication | System-defined profile to set User bandwidth limits |  | 4 | 1 |
| 3024 | ws\_Guest MAC Caching Session Limit | Post\_Authentication | System-defined profile to set concurrent User session count |  | 2 | 1 |
| 3025 | ws\_Guest Guest MAC Caching | Post\_Authentication | Endpoint attribute updates for Guest |  | 3 | 1 |
| 3026 | ws\_Operator\_Receptionist | Application | ClearPass Guest Receptionist Operator Profile | Accept | 1 | 1 |
| 3027 | ws\_Operator\_Device\_Registration | Application | ClearPass Guest Device Registration Operator Profile | Accept | 1 | 1 |
| 3028 | ws\_role\_onboard-redirect | RADIUS | Return the onboard-redirect role | Accept | 1 | 1 |
| 3029 | ws\_role\_guest-redirect | RADIUS | Return the guest-redirect role | Accept | 1 | 0 |
| 3030 | ws\_vlan203\_tunneled\_aruba | RADIUS | Return the tunneled client VLAN203 | Accept | 1 | 2 |
| 3031 | ws\_dACL\_untrusted | RADIUS | Deny access to internal servers | Accept | 3 | 2 |
| 3032 | ws\_dACL\_redirect | RADIUS | Captive portal Redirect | Accept | 4 | 1 |
| 3034 | ws\_dACL\_voice | RADIUS | Voice only | Accept | 4 | 1 |
| 3035 | ws\_hpe\_role\_admin | RADIUS | HPE Admin Role | Accept | 1 | 2 |
| 3036 | ws\_hpe\_role\_guest-redirect | RADIUS | Return the guest-redirect role | Accept | 1 | 1 |
| 3037 | ws\_hpe\_role\_contractor | RADIUS | HPE Contractor Role | Accept | 1 | 3 |
| 3038 | ws\_hpe\_role\_employee | RADIUS | HPE Employee Role | Accept | 1 | 3 |
| 3039 | ws\_hpe\_role\_voice | RADIUS | HPE Voice Role | Accept | 1 | 2 |
| 3040 | ws\_hpe\_role\_guest | RADIUS | Return the guest role | Accept | 1 | 1 |
| 3041 | ws\_AOS-SW-Admin-priv | RADIUS |  | Accept | 1 | 1 |
| 3042 | ws\_airheads\_security\_update | Post\_Authentication | Update the security system with user information. |  | 4 | 1 |
| 3044 | ws\_quarantine\_set\_security\_info\_juniper\_srx | Post\_Authentication | Update Endpoint with Security Information |  | 4 | 1 |
| 3045 | ws\_role\_quarantine | RADIUS | Aruba Quarantine Role | Accept | 1 | 1 |
| 3046 | ws\_clear\_comprimized | Post\_Authentication | Clear the compromized attribute in the endpoint |  | 1 | 0 |
| 3047 | ws\_snmp\_vlan31 | SNMP |  |  | 1 | 1 |
| 3048 | ws\_snmp\_bounce\_port | SNMP |  |  | 1 | 1 |
| 3049 | ws\_quarantine\_release\_error | Application | Return an error message that quarantine release is only allowed once a day. | Reject | 1 | 1 |
| 3050 | ws\_quarantine\_reset\_and\_set\_timestamp | Post\_Authentication | Set the timestamp of now + 1 day on the Endpoint; and clear the Compromised flag. |  | 2 | 1 |
| 3051 | ws\_snmp\_vlan39 | SNMP |  |  | 1 | 0 |
| 3052 | ws\_snmp\_vlan11\_corporate | SNMP |  |  | 1 | 1 |
| 3053 | ws\_snmp\_vlan14\_untrust | SNMP |  |  | 1 | 1 |
| 3054 | ws\_snmp\_vlan12\_voice | SNMP |  |  | 1 | 1 |
| 3055 | ws\_role\_onguard-redirect | RADIUS | Return the onguard-redirect role | Accept | 1 | 1 |
| 3059 | ws\_Airwave\_admin | RADIUS | Airwave Admin Role | Accept | 1 | 1 |
| 3060 | ws\_iap\_with\_tagged\_vlans | RADIUS | Return untagged Management VLAN, and tagged VLANs Corporate, Voice, Guest, Untrusted | Accept | 7 | 2 |
| 3061 | ws\_vlan90\_management | RADIUS | Return the management VLAN90 | Accept | 5 | 0 |
| 3062 | ws\_vlan94\_untrust | RADIUS | Return the untrusted VLAN94 | Accept | 5 | 0 |
| 3063 | ws\_vlan\_voice | RADIUS | Return the Voice VLAN named VLAN | Accept | 5 | 1 |
| 3065 | ws\_dACL\_internal\_only | RADIUS | Only internal access | Accept | 3 | 1 |
| 3066 | ws\_vlan\_corporate | RADIUS | Return the Corporate VLAN named VLAN | Accept | 5 | 1 |
| 3067 | ws\_vlan\_untrust | RADIUS | Return the Untrusted VLAN named VLAN | Accept | 5 | 1 |
| 3068 | ws\_vlan\_guest | RADIUS | Return the GuestVLAN named VLAN | Accept | 5 | 1 |
| 3069 | ws\_vlan\_management | RADIUS | Return the Management VLAN named VLAN | Accept | 5 | 1 |
| 3070 | ws\_dACL\_camera | RADIUS | Only internal access | Accept | 3 | 1 |
| 3071 | ws\_dACL\_unmanaged\_IoT | RADIUS | Deny access to internal servers | Accept | 4 | 1 |
| 3072 | ws\_iap1x\_with\_tagged\_vlans | RADIUS | Return untagged Management VLAN, and tagged VLANs Corporate, Voice, Guest, Untrusted | Accept | 7 | 0 |
| 3074 | ws\_hpe\_role\_employee-tun | RADIUS | HPE Employee Role [tunneled] | Accept | 1 | 0 |
| 3075 | ws\_hpe\_role\_admin-tun | RADIUS | HPE Admin Role | Accept | 1 | 1 |
| 3076 | ws\_hpe\_role\_voice-tun | RADIUS | HPE Voice Role tunneled | Accept | 1 | 0 |
| 3077 | ws\_hpe\_role\_camera | RADIUS | HPE camera Role | Accept | 1 | 2 |
| 3078 | ws\_hpe\_role\_iot-tun | RADIUS | HPE IOT Role (Internet only) | Accept | 1 | 1 |
| 3079 | ws\_hpe\_role\_profiler | RADIUS | Return the profiler role | Accept | 1 | 0 |
| 3080 | ws\_hpe\_role\_contractor-tun | RADIUS | HPE Contractor Role [tunneled] | Accept | 1 | 2 |
| 3081 | ws\_hpe\_role\_guest-tun | RADIUS | Return the guest-tun role | Accept | 1 | 2 |
| 3082 | ws\_dur\_employee | Aruba\_DUR | ArubaOS Switch employee downloadable role |  | 1 | 1 |
| 3084 | ws\_dur\_voice | Aruba\_DUR | ArubaOS Switch voice downloadable role |  | 1 | 1 |
| 3085 | ws\_dur\_camera | Aruba\_DUR | ArubaOS Switch camera downloadable role |  | 1 | 1 |
| 3087 | ws\_dur\_redirect | Aruba\_DUR | ArubaOS Switch clearpass-redirect downloadable role |  | 1 | 1 |
| 3088 | radius\_rapi | RADIUS |  | Accept | 1 | 1 |
| 3090 | ws\_Operator\_Super\_Administrator | Application | ClearPass Guest Super Administrator Operator Profile | Accept | 1 | 1 |
| 3091 | ws\_quarantine\_set\_security\_info\_checkpoint | Post\_Authentication | Update Endpoint with Security Information |  | 4 | 1 |

Table - Enforcement Profile

The following section details Enforcement Profiles configured on ClearPass.

### 1.6.4.1 Enforcement Profiles: [Allow Access Profile]

|  |  |
| --- | --- |
| Id | 1 |
| Name | [Allow Access Profile] |
| Type | RADIUS |
| Action | Accept |

Table - Enforcement profile: [Allow Access Profile]

### 1.6.4.2 Enforcement Profiles: [Deny Access Profile]

|  |  |
| --- | --- |
| Id | 2 |
| Name | [Deny Access Profile] |
| Type | RADIUS |
| Action | Reject |

Table - Enforcement profile: [Deny Access Profile]

### 1.6.4.3 Enforcement Profiles: [Drop Access Profile]

|  |  |
| --- | --- |
| Id | 3 |
| Name | [Drop Access Profile] |
| Type | RADIUS |
| Action | Drop |

Table - Enforcement profile: [Drop Access Profile]

### 1.6.4.4 Enforcement Profiles: [TACACS+ Deny Profile]

|  |  |
| --- | --- |
| Id | 12 |
| Name | [TACACS+ Deny Profile] |
| Type | TACACS |
| Action | Accept |

Table - Enforcement profile: [TACACS+ Deny Profile]

### 1.6.4.5 Enforcement Profiles: [TACACS+ Super Admin]

|  |  |
| --- | --- |
| Id | 13 |
| Name | [TACACS+ Super Admin] |
| Type | TACACS |
| Action | Accept |

Table - Enforcement profile: [TACACS+ Super Admin]

| Type | Name | Value |
| --- | --- | --- |
| cpass:HTTP | AdminPrivilege | Super Administrator |
| cpass:CLI | AdminPrivilege | Super Administrator |

Table - Atttributes : [TACACS+ Super Admin]

| Privilege Level | Services | Authorize Attribute Status |
| --- | --- | --- |
| 1 | cpass:HTTP, cpass:CLI | ADD |

Table - Tacacs Services Params: [TACACS+ Super Admin]

### 1.6.4.6 Enforcement Profiles: [TACACS+ Network Admin]

|  |  |
| --- | --- |
| Id | 15 |
| Name | [TACACS+ Network Admin] |
| Type | TACACS |
| Action | Accept |

Table - Enforcement profile: [TACACS+ Network Admin]

| Type | Name | Value |
| --- | --- | --- |
| cpass:HTTP | AdminPrivilege | Network Administrator |

Table - Atttributes : [TACACS+ Network Admin]

| Privilege Level | Services | Authorize Attribute Status |
| --- | --- | --- |
| 1 | cpass:HTTP | ADD |

Table - Tacacs Services Params: [TACACS+ Network Admin]

### 1.6.4.7 Enforcement Profiles: [TACACS+ Help Desk]

|  |  |
| --- | --- |
| Id | 16 |
| Name | [TACACS+ Help Desk] |
| Type | TACACS |
| Action | Accept |

Table - Enforcement profile: [TACACS+ Help Desk]

| Type | Name | Value |
| --- | --- | --- |
| cpass:HTTP | AdminPrivilege | Help Desk |

Table - Atttributes : [TACACS+ Help Desk]

| Privilege Level | Services | Authorize Attribute Status |
| --- | --- | --- |
| 1 | cpass:HTTP | ADD |

Table - Tacacs Services Params: [TACACS+ Help Desk]

### 1.6.4.8 Enforcement Profiles: [TACACS+ Receptionist]

|  |  |
| --- | --- |
| Id | 17 |
| Name | [TACACS+ Receptionist] |
| Type | TACACS |
| Action | Accept |

Table - Enforcement profile: [TACACS+ Receptionist]

| Type | Name | Value |
| --- | --- | --- |
| cpass:HTTP | AdminPrivilege | Receptionist |

Table - Atttributes : [TACACS+ Receptionist]

| Privilege Level | Services | Authorize Attribute Status |
| --- | --- | --- |
| 1 | cpass:HTTP | ADD |

Table - Tacacs Services Params: [TACACS+ Receptionist]

### 1.6.4.9 Enforcement Profiles: [TACACS+ Read-only Admin]

|  |  |
| --- | --- |
| Id | 18 |
| Name | [TACACS+ Read-only Admin] |
| Type | TACACS |
| Action | Accept |

Table - Enforcement profile: [TACACS+ Read-only Admin]

| Type | Name | Value |
| --- | --- | --- |
| cpass:HTTP | AdminPrivilege | Read-only Administrator |

Table - Atttributes : [TACACS+ Read-only Admin]

| Privilege Level | Services | Authorize Attribute Status |
| --- | --- | --- |
| 1 | cpass:HTTP | ADD |

Table - Tacacs Services Params: [TACACS+ Read-only Admin]

### 1.6.4.10 Enforcement Profiles: [TACACS+ API Admin]

|  |  |
| --- | --- |
| Id | 19 |
| Name | [TACACS+ API Admin] |
| Type | TACACS |
| Action | Accept |

Table - Enforcement profile: [TACACS+ API Admin]

| Type | Name | Value |
| --- | --- | --- |
| cpass:HTTP | AdminPrivilege | API Administrator |

Table - Atttributes : [TACACS+ API Admin]

| Privilege Level | Services | Authorize Attribute Status |
| --- | --- | --- |
| 1 | cpass:HTTP | ADD |

Table - Tacacs Services Params: [TACACS+ API Admin]

### 1.6.4.11 Enforcement Profiles: [ArubaOS Wireless - TACACS+ Root Access]

|  |  |
| --- | --- |
| Id | 20 |
| Name | [ArubaOS Wireless - TACACS+ Root Access] |
| Type | TACACS |
| Action | Accept |

Table - Enforcement profile: [ArubaOS Wireless - TACACS+ Root Access]

| Type | Name | Value |
| --- | --- | --- |
| Aruba:Common | Aruba-Admin-Role | root |

Table - Atttributes : [ArubaOS Wireless - TACACS+ Root Access]

| Privilege Level | Services | Authorize Attribute Status |
| --- | --- | --- |
| 15 | Aruba:Common | ADD |

Table - Tacacs Services Params: [ArubaOS Wireless - TACACS+ Root Access]

### 1.6.4.12 Enforcement Profiles: [ArubaOS Wireless - TACACS+ Read-Only Access]

|  |  |
| --- | --- |
| Id | 21 |
| Name | [ArubaOS Wireless - TACACS+ Read-Only Access] |
| Type | TACACS |
| Action | Accept |

Table - Enforcement profile: [ArubaOS Wireless - TACACS+ Read-Only Access]

| Type | Name | Value |
| --- | --- | --- |
| Aruba:Common | Aruba-Admin-Role | read-only |

Table - Atttributes : [ArubaOS Wireless - TACACS+ Read-Only Access]

| Privilege Level | Services | Authorize Attribute Status |
| --- | --- | --- |
| 15 | Aruba:Common | ADD |

Table - Tacacs Services Params: [ArubaOS Wireless - TACACS+ Read-Only Access]

### 1.6.4.13 Enforcement Profiles: [Deny Application Access Profile]

|  |  |
| --- | --- |
| Id | 31 |
| Name | [Deny Application Access Profile] |
| Type | Application |
| Action | Reject |

Table - Enforcement profile: [Deny Application Access Profile]

### 1.6.4.14 Enforcement Profiles: [Allow Application Access Profile]

|  |  |
| --- | --- |
| Id | 32 |
| Name | [Allow Application Access Profile] |
| Type | Application |
| Action | Accept |

Table - Enforcement profile: [Allow Application Access Profile]

### 1.6.4.15 Enforcement Profiles: [Handle AirGroup Time Sharing]

|  |  |
| --- | --- |
| Id | 33 |
| Name | [Handle AirGroup Time Sharing] |
| Type | HTTP |

Table - Enforcement profile: [Handle AirGroup Time Sharing]

| Type | Name | Value |
| --- | --- | --- |
|  | Target Server | localhost |
|  | Action | Handle AirGroup Time Sharing |

Table - Atttributes : [Handle AirGroup Time Sharing]

### 1.6.4.16 Enforcement Profiles: [AirGroup Response]

|  |  |
| --- | --- |
| Id | 40 |
| Name | [AirGroup Response] |
| Type | RADIUS |
| Action | Accept |

Table - Enforcement profile: [AirGroup Response]

| Type | Name | Value |
| --- | --- | --- |
| Radius:IETF | Called-Station-Id | AirGroup |
| Radius:IETF | Calling-Station-Id | %{Connection:Client-Mac-Address-NoDelim} |
| Radius:Aruba | Aruba-AirGroup-Version | AirGroup-v2 (2) |

Table - Atttributes : [AirGroup Response]

### 1.6.4.17 Enforcement Profiles: [AirGroup Personal Device]

|  |  |
| --- | --- |
| Id | 41 |
| Name | [AirGroup Personal Device] |
| Type | RADIUS |
| Action | Accept |

Table - Enforcement profile: [AirGroup Personal Device]

| Type | Name | Value |
| --- | --- | --- |
| Radius:Aruba | Aruba-AirGroup-Device-Type | Personal-Device (1) |
| Radius:Aruba | Aruba-AirGroup-User-Name | %{Authorization:[Guest Device Repository]:SponsorName} |
| Radius:Aruba | Aruba-AirGroup-Shared-User | %{GuestUser:airgroup\_shared\_user} |

Table - Atttributes : [AirGroup Personal Device]

### 1.6.4.18 Enforcement Profiles: [AirGroup Shared Device]

|  |  |
| --- | --- |
| Id | 42 |
| Name | [AirGroup Shared Device] |
| Type | RADIUS |
| Action | Accept |

Table - Enforcement profile: [AirGroup Shared Device]

| Type | Name | Value |
| --- | --- | --- |
| Radius:Aruba | Aruba-AirGroup-Device-Type | Shared-Device (2) |
| Radius:Aruba | Aruba-AirGroup-Shared-User | %{GuestUser:airgroup\_shared\_user} |
| Radius:Aruba | Aruba-AirGroup-Shared-Role | %{GuestUser:airgroup\_shared\_role} |
| Radius:Aruba | Aruba-Location-Id | %{GuestUser:airgroup\_shared\_location} |
| Radius:Aruba | Aruba-AirGroup-Shared-Group | %{GuestUser:airgroup\_shared\_group} |

Table - Atttributes : [AirGroup Shared Device]

### 1.6.4.19 Enforcement Profiles: [Return Device Sponsor Name - RADIUS User-Name]

|  |  |
| --- | --- |
| Id | 43 |
| Name | [Return Device Sponsor Name - RADIUS User-Name] |
| Type | RADIUS |
| Action | Accept |

Table - Enforcement profile: [Return Device Sponsor Name - RADIUS User-Name]

| Type | Name | Value |
| --- | --- | --- |
| Radius:IETF | User-Name | %{Authorization:[Guest Device Repository]:SponsorName} |

Table - Atttributes : [Return Device Sponsor Name - RADIUS User-Name]

### 1.6.4.20 Enforcement Profiles: [Registered Device MPSK]

|  |  |
| --- | --- |
| Id | 44 |
| Name | [Registered Device MPSK] |
| Type | RADIUS |
| Action | Accept |

Table - Enforcement profile: [Registered Device MPSK]

| Type | Name | Value |
| --- | --- | --- |
| Radius:Aruba | Aruba-MPSK-Passphrase | Device's Assigned MPSK |

Table - Atttributes : [Registered Device MPSK]

### 1.6.4.21 Enforcement Profiles: [Update Endpoint Known]

|  |  |
| --- | --- |
| Id | 51 |
| Name | [Update Endpoint Known] |
| Type | Post\_Authentication |

Table - Enforcement profile: [Update Endpoint Known]

| Type | Name | Value |
| --- | --- | --- |
| Status-Update | Endpoint | Known |

Table - Atttributes : [Update Endpoint Known]

### 1.6.4.22 Enforcement Profiles: [Operator Login - Local Users]

|  |  |
| --- | --- |
| Id | 61 |
| Name | [Operator Login - Local Users] |
| Type | Application |
| Action | Accept |

Table - Enforcement profile: [Operator Login - Local Users]

| Type | Name | Value |
| --- | --- | --- |
|  | admin\_privileges | %{Authorization:[Local User Repository]:Role\_Name} |

Table - Atttributes : [Operator Login - Local Users]

### 1.6.4.23 Enforcement Profiles: [Operator Login - Admin Users]

|  |  |
| --- | --- |
| Id | 62 |
| Name | [Operator Login - Admin Users] |
| Type | Application |
| Action | Accept |

Table - Enforcement profile: [Operator Login - Admin Users]

| Type | Name | Value |
| --- | --- | --- |
|  | admin\_privileges | %{Authorization:[Admin User Repository]:Role\_Name} |

Table - Atttributes : [Operator Login - Admin Users]

### 1.6.4.24 Enforcement Profiles: [Cisco - Terminate Session]

|  |  |
| --- | --- |
| Id | 101 |
| Name | [Cisco - Terminate Session] |
| Type | RADIUS\_DynAuthZ |
| RADIUS Dyn Template | Cisco - Terminate Session |

Table - Enforcement profile: [Cisco - Terminate Session]

| Type | Name | Value |
| --- | --- | --- |
| Radius:IETF | Calling-Station-Id | %{Radius:IETF:Calling-Station-Id} |
| Radius:IETF | Service-Type | 1 |

Table - Atttributes : [Cisco - Terminate Session]

### 1.6.4.25 Enforcement Profiles: [Cisco - Disable Host-Port]

|  |  |
| --- | --- |
| Id | 102 |
| Name | [Cisco - Disable Host-Port] |
| Type | RADIUS\_DynAuthZ |
| RADIUS Dyn Template | Cisco - Disable Switch Port |

Table - Enforcement profile: [Cisco - Disable Host-Port]

| Type | Name | Value |
| --- | --- | --- |
| Radius:IETF | Calling-Station-Id | %{Radius:IETF:Calling-Station-Id} |
| Radius:Cisco | Cisco-AVPair | subscriber:command=disable-host-port |

Table - Atttributes : [Cisco - Disable Host-Port]

### 1.6.4.26 Enforcement Profiles: [Cisco - Bounce-Host-Port]

|  |  |
| --- | --- |
| Id | 103 |
| Name | [Cisco - Bounce-Host-Port] |
| Type | RADIUS\_DynAuthZ |
| RADIUS Dyn Template | Cisco - Bounce Switch Port |

Table - Enforcement profile: [Cisco - Bounce-Host-Port]

| Type | Name | Value |
| --- | --- | --- |
| Radius:IETF | Calling-Station-Id | %{Radius:IETF:Calling-Station-Id} |
| Radius:Cisco | Cisco-AVPair | subscriber:command=bounce-host-port |

Table - Atttributes : [Cisco - Bounce-Host-Port]

### 1.6.4.27 Enforcement Profiles: [Cisco - Reauthenticate-Session]

|  |  |
| --- | --- |
| Id | 104 |
| Name | [Cisco - Reauthenticate-Session] |
| Type | RADIUS\_DynAuthZ |
| RADIUS Dyn Template | Cisco - Reauthenticate Session |

Table - Enforcement profile: [Cisco - Reauthenticate-Session]

| Type | Name | Value |
| --- | --- | --- |
| Radius:IETF | Calling-Station-Id | %{Radius:IETF:Calling-Station-Id} |
| Radius:Cisco | Cisco-AVPair | subscriber:command=reauthenticate |

Table - Atttributes : [Cisco - Reauthenticate-Session]

### 1.6.4.28 Enforcement Profiles: [ArubaOS Switching - Terminate Session]

|  |  |
| --- | --- |
| Id | 105 |
| Name | [ArubaOS Switching - Terminate Session] |
| Type | RADIUS\_DynAuthZ |
| RADIUS Dyn Template | ArubaOS Switching - Terminate Session |

Table - Enforcement profile: [ArubaOS Switching - Terminate Session]

| Type | Name | Value |
| --- | --- | --- |
| Radius:IETF | User-Name | %{Radius:IETF:User-Name} |
| Radius:IETF | Calling-Station-Id | %{Radius:IETF:Calling-Station-Id} |
| Radius:IETF | NAS-Port | %{Radius:IETF:NAS-Port} |
| Radius:IETF | NAS-IP-Address | %{Radius:IETF:NAS-IP-Address} |
| Radius:IETF | Event-Timestamp | %{Radius:IETF:Event-Timestamp} |

Table - Atttributes : [ArubaOS Switching - Terminate Session]

### 1.6.4.29 Enforcement Profiles: [ArubaOS Wireless - Terminate Session]

|  |  |
| --- | --- |
| Id | 106 |
| Name | [ArubaOS Wireless - Terminate Session] |
| Type | RADIUS\_DynAuthZ |
| RADIUS Dyn Template | ArubaOS Wireless - Terminate Session |

Table - Enforcement profile: [ArubaOS Wireless - Terminate Session]

| Type | Name | Value |
| --- | --- | --- |
| Radius:IETF | Calling-Station-Id | %{Radius:IETF:Calling-Station-Id} |

Table - Atttributes : [ArubaOS Wireless - Terminate Session]

### 1.6.4.30 Enforcement Profiles: [Juniper Terminate Session]

|  |  |
| --- | --- |
| Id | 107 |
| Name | [Juniper Terminate Session] |
| Type | RADIUS\_DynAuthZ |
| RADIUS Dyn Template | Juniper - Terminate Session |

Table - Enforcement profile: [Juniper Terminate Session]

| Type | Name | Value |
| --- | --- | --- |
| Radius:IETF | Calling-Station-Id | %{Radius:IETF:Calling-Station-Id} |
| Radius:IETF | Acct-Session-Id | %{Radius:IETF:Acct-Session-Id} |

Table - Atttributes : [Juniper Terminate Session]

### 1.6.4.31 Enforcement Profiles: [Trapeze - Terminate Session]

|  |  |
| --- | --- |
| Id | 108 |
| Name | [Trapeze - Terminate Session] |
| Type | RADIUS\_DynAuthZ |
| RADIUS Dyn Template | Trapeze - Terminate Session |

Table - Enforcement profile: [Trapeze - Terminate Session]

| Type | Name | Value |
| --- | --- | --- |
| Radius:IETF | User-Name | %{Radius:IETF:User-Name} |
| Radius:IETF | Calling-Station-Id | %{Radius:IETF:Calling-Station-Id} |
| Radius:IETF | NAS-IP-Address | %{Radius:IETF:NAS-IP-Address} |

Table - Atttributes : [Trapeze - Terminate Session]

### 1.6.4.32 Enforcement Profiles: [Aerohive - Terminate Session]

|  |  |
| --- | --- |
| Id | 109 |
| Name | [Aerohive - Terminate Session] |
| Type | RADIUS\_DynAuthZ |
| RADIUS Dyn Template | Aerohive - Terminate Session |

Table - Enforcement profile: [Aerohive - Terminate Session]

| Type | Name | Value |
| --- | --- | --- |
| Radius:IETF | User-Name | %{Radius:IETF:User-Name} |
| Radius:IETF | Calling-Station-Id | %{Radius:IETF:Calling-Station-Id} |
| Radius:IETF | NAS-IP-Address | %{Radius:IETF:NAS-IP-Address} |

Table - Atttributes : [Aerohive - Terminate Session]

### 1.6.4.33 Enforcement Profiles: [Motorola - Terminate Session]

|  |  |
| --- | --- |
| Id | 110 |
| Name | [Motorola - Terminate Session] |
| Type | RADIUS\_DynAuthZ |
| RADIUS Dyn Template | Motorola - Terminate Session |

Table - Enforcement profile: [Motorola - Terminate Session]

| Type | Name | Value |
| --- | --- | --- |
| Radius:IETF | User-Name | %{Radius:IETF:User-Name} |
| Radius:IETF | Calling-Station-Id | %{Radius:IETF:Calling-Station-Id} |
| Radius:IETF | NAS-IP-Address | %{Radius:IETF:NAS-IP-Address} |

Table - Atttributes : [Motorola - Terminate Session]

### 1.6.4.34 Enforcement Profiles: [ArubaOS Wireless - Bounce Switch Port]

|  |  |
| --- | --- |
| Id | 111 |
| Name | [ArubaOS Wireless - Bounce Switch Port] |
| Type | RADIUS\_DynAuthZ |
| RADIUS Dyn Template | ArubaOS Wireless - Bounce Switch Port |

Table - Enforcement profile: [ArubaOS Wireless - Bounce Switch Port]

| Type | Name | Value |
| --- | --- | --- |
| Radius:IETF | Calling-Station-Id | %{Radius:IETF:Calling-Station-Id} |
| Radius:Aruba | Aruba-Port-Bounce-Host | 12 |

Table - Atttributes : [ArubaOS Wireless - Bounce Switch Port]

### 1.6.4.35 Enforcement Profiles: [ArubaOS Switching - Bounce Switch Port]

|  |  |
| --- | --- |
| Id | 112 |
| Name | [ArubaOS Switching - Bounce Switch Port] |
| Type | RADIUS\_DynAuthZ |
| RADIUS Dyn Template | ArubaOS Switching - Bounce Switch Port |

Table - Enforcement profile: [ArubaOS Switching - Bounce Switch Port]

| Type | Name | Value |
| --- | --- | --- |
| Radius:IETF | User-Name | %{Radius:IETF:User-Name} |
| Radius:IETF | Calling-Station-Id | %{Radius:IETF:Calling-Station-Id} |
| Radius:IETF | NAS-Port | %{Radius:IETF:NAS-Port} |
| Radius:IETF | NAS-IP-Address | %{Radius:IETF:NAS-IP-Address} |
| Radius:IETF | Event-Timestamp | %{Radius:IETF:Event-Timestamp} |
| Radius:Hewlett-Packard-Enterprise | HPE-Port-Bounce-Host | 12 |

Table - Atttributes : [ArubaOS Switching - Bounce Switch Port]

### 1.6.4.36 Enforcement Profiles: [H3C - Terminate Session]

|  |  |
| --- | --- |
| Id | 113 |
| Name | [H3C - Terminate Session] |
| Type | RADIUS\_DynAuthZ |
| RADIUS Dyn Template | H3C - Terminate Session |

Table - Enforcement profile: [H3C - Terminate Session]

| Type | Name | Value |
| --- | --- | --- |
| Radius:IETF | User-Name | %{Radius:IETF:User-Name} |
| Radius:IETF | Calling-Station-Id | %{Radius:IETF:Calling-Station-Id} |

Table - Atttributes : [H3C - Terminate Session]

### 1.6.4.37 Enforcement Profiles: [H3C - Bounce Switch Port]

|  |  |
| --- | --- |
| Id | 114 |
| Name | [H3C - Bounce Switch Port] |
| Type | RADIUS\_DynAuthZ |
| RADIUS Dyn Template | H3C - Bounce Switch Port |

Table - Enforcement profile: [H3C - Bounce Switch Port]

| Type | Name | Value |
| --- | --- | --- |
| Radius:IETF | Calling-Station-Id | %{Radius:IETF:Calling-Station-Id} |
| Radius:H3C | H3C-AVPair | subscriber:command=bounce-host-port |

Table - Atttributes : [H3C - Bounce Switch Port]

### 1.6.4.38 Enforcement Profiles: [H3C - Disable Switch Port]

|  |  |
| --- | --- |
| Id | 115 |
| Name | [H3C - Disable Switch Port] |
| Type | RADIUS\_DynAuthZ |
| RADIUS Dyn Template | H3C - Disable Switch Port |

Table - Enforcement profile: [H3C - Disable Switch Port]

| Type | Name | Value |
| --- | --- | --- |
| Radius:IETF | Calling-Station-Id | %{Radius:IETF:Calling-Station-Id} |
| Radius:H3C | H3C-AVPair | subscriber:command=disable-host-port |

Table - Atttributes : [H3C - Disable Switch Port]

### 1.6.4.39 Enforcement Profiles: [Tellabs - Bounce Host Port]

|  |  |
| --- | --- |
| Id | 116 |
| Name | [Tellabs - Bounce Host Port] |
| Type | RADIUS\_DynAuthZ |
| RADIUS Dyn Template | Tellabs - Bounce Switch Port |

Table - Enforcement profile: [Tellabs - Bounce Host Port]

| Type | Name | Value |
| --- | --- | --- |
| Radius:IETF | Calling-Station-Id | %{Radius:IETF:Calling-Station-Id} |
| Radius:Tellabs | Tellabs-AVPair | subscriber:command=bounce-host-port |
| Radius:IETF | Acct-Terminate-Cause | 6 |

Table - Atttributes : [Tellabs - Bounce Host Port]

### 1.6.4.40 Enforcement Profiles: [Tellabs - Disable Host Port]

|  |  |
| --- | --- |
| Id | 117 |
| Name | [Tellabs - Disable Host Port] |
| Type | RADIUS\_DynAuthZ |
| RADIUS Dyn Template | Tellabs - Disable Switch Port |

Table - Enforcement profile: [Tellabs - Disable Host Port]

| Type | Name | Value |
| --- | --- | --- |
| Radius:IETF | Calling-Station-Id | %{Radius:IETF:Calling-Station-Id} |
| Radius:Tellabs | Tellabs-AVPair | subscriber:command=disable-host-port |
| Radius:IETF | Acct-Terminate-Cause | 6 |

Table - Atttributes : [Tellabs - Disable Host Port]

### 1.6.4.41 Enforcement Profiles: [Tellabs - Reauthenticate Session]

|  |  |
| --- | --- |
| Id | 118 |
| Name | [Tellabs - Reauthenticate Session] |
| Type | RADIUS\_DynAuthZ |
| RADIUS Dyn Template | Tellabs - Reauthenticate Session |

Table - Enforcement profile: [Tellabs - Reauthenticate Session]

| Type | Name | Value |
| --- | --- | --- |
| Radius:IETF | Calling-Station-Id | %{Radius:IETF:Calling-Station-Id} |
| Radius:Tellabs | Tellabs-AVPair | subscriber:command=reauthenticate |

Table - Atttributes : [Tellabs - Reauthenticate Session]

### 1.6.4.42 Enforcement Profiles: [Tellabs - Terminate Session]

|  |  |
| --- | --- |
| Id | 119 |
| Name | [Tellabs - Terminate Session] |
| Type | RADIUS\_DynAuthZ |
| RADIUS Dyn Template | Tellabs - Terminate Session |

Table - Enforcement profile: [Tellabs - Terminate Session]

| Type | Name | Value |
| --- | --- | --- |
| Radius:IETF | Calling-Station-Id | %{Radius:IETF:Calling-Station-Id} |
| Radius:IETF | Acct-Terminate-Cause | 6 |

Table - Atttributes : [Tellabs - Terminate Session]

### 1.6.4.43 Enforcement Profiles: [Cisco ASA - Terminate Session]

|  |  |
| --- | --- |
| Id | 120 |
| Name | [Cisco ASA - Terminate Session] |
| Type | RADIUS\_DynAuthZ |
| RADIUS Dyn Template | Cisco ASA - Terminate Session |

Table - Enforcement profile: [Cisco ASA - Terminate Session]

| Type | Name | Value |
| --- | --- | --- |
| Radius:IETF | Calling-Station-Id | %{Radius:IETF:Calling-Station-Id} |
| Radius:IETF | Service-Type | 1 |
| Radius:Cisco | Cisco-AVPair | %{Radius:Cisco:Cisco-AVPair} |

Table - Atttributes : [Cisco ASA - Terminate Session]

### 1.6.4.44 Enforcement Profiles: [AOS-CX - Disconnect]

|  |  |
| --- | --- |
| Id | 121 |
| Name | [AOS-CX - Disconnect] |
| Type | RADIUS\_DynAuthZ |
| RADIUS Dyn Template | AOS-CX - Disconnect |

Table - Enforcement profile: [AOS-CX - Disconnect]

| Type | Name | Value |
| --- | --- | --- |
| Radius:IETF | Calling-Station-Id | %{Radius:IETF:Calling-Station-Id} |
| Radius:IETF | NAS-Port | %{Radius:IETF:NAS-Port} |
| Radius:IETF | NAS-Identifier | %{Radius:IETF:NAS-Identifier} |
| Radius:IETF | User-Name | %{Radius:IETF:User-Name} |
| Radius:IETF | Event-Timestamp | %{Radius:IETF:Event-Timestamp} |

Table - Atttributes : [AOS-CX - Disconnect]

### 1.6.4.45 Enforcement Profiles: [AOS-CX - Bounce Switch Port]

|  |  |
| --- | --- |
| Id | 122 |
| Name | [AOS-CX - Bounce Switch Port] |
| Type | RADIUS\_DynAuthZ |
| RADIUS Dyn Template | AOS-CX - Bounce Switch Port |

Table - Enforcement profile: [AOS-CX - Bounce Switch Port]

| Type | Name | Value |
| --- | --- | --- |
| Radius:IETF | Calling-Station-Id | %{Radius:IETF:Calling-Station-Id} |
| Radius:IETF | NAS-Port | %{Radius:IETF:NAS-Port} |
| Radius:IETF | NAS-Identifier | %{Radius:IETF:NAS-Identifier} |
| Radius:IETF | User-Name | %{Radius:IETF:User-Name} |
| Radius:IETF | Event-Timestamp | %{Radius:IETF:Event-Timestamp} |
| Radius:Aruba | Aruba-Port-Bounce-Host | 12 |

Table - Atttributes : [AOS-CX - Bounce Switch Port]

### 1.6.4.46 Enforcement Profiles: [Meraki - Terminate Session]

|  |  |
| --- | --- |
| Id | 123 |
| Name | [Meraki - Terminate Session] |
| Type | RADIUS\_DynAuthZ |
| RADIUS Dyn Template | Meraki - Terminate Session |

Table - Enforcement profile: [Meraki - Terminate Session]

| Type | Name | Value |
| --- | --- | --- |
| Radius:IETF | Calling-Station-Id | %{Radius:IETF:Calling-Station-Id} |
| Radius:IETF | Acct-Session-Id | %{Radius:IETF:Acct-Session-Id} |
| Radius:IETF | Event-Timestamp | %{Radius:IETF:Event-Timestamp} |

Table - Atttributes : [Meraki - Terminate Session]

### 1.6.4.47 Enforcement Profiles: [Arista Wireless - Terminate Session]

|  |  |
| --- | --- |
| Id | 124 |
| Name | [Arista Wireless - Terminate Session] |
| Type | RADIUS\_DynAuthZ |
| RADIUS Dyn Template | Arista Wireless - Terminate Session |

Table - Enforcement profile: [Arista Wireless - Terminate Session]

| Type | Name | Value |
| --- | --- | --- |
| Radius:IETF | NAS-IP-Address | %{Radius:IETF:NAS-IP-Address} |
| Radius:IETF | Calling-Station-Id | %{Radius:IETF:Calling-Station-Id} |

Table - Atttributes : [Arista Wireless - Terminate Session]

### 1.6.4.48 Enforcement Profiles: [Arista Wired - Terminate Session]

|  |  |
| --- | --- |
| Id | 125 |
| Name | [Arista Wired - Terminate Session] |
| Type | RADIUS\_DynAuthZ |
| RADIUS Dyn Template | Arista Wired - Terminate Session |

Table - Enforcement profile: [Arista Wired - Terminate Session]

| Type | Name | Value |
| --- | --- | --- |
| Radius:IETF | User-Name | %{Radius:IETF:User-Name} |
| Radius:IETF | NAS-Port-Id | %{Radius:IETF:NAS-Port-Id} |
| Radius:IETF | Calling-Station-Id | %{Radius:IETF:Calling-Station-Id} |
| Radius:IETF | Acct-Session-Id | %{Radius:IETF:Acct-Session-Id} |
| Radius:IETF | NAS-IP-Address | %{Radius:IETF:NAS-IP-Address} |

Table - Atttributes : [Arista Wired - Terminate Session]

### 1.6.4.49 Enforcement Profiles: ws\_role\_employee

|  |  |
| --- | --- |
| Id | 3001 |
| Name | ws\_role\_employee |
| Type | RADIUS |
| Action | Accept |

Table - Enforcement profile: ws\_role\_employee

| Type | Name | Value |
| --- | --- | --- |
| Radius:Aruba | Aruba-User-Role | employee |

Table - Atttributes : ws\_role\_employee

### 1.6.4.50 Enforcement Profiles: ws\_role\_voice

|  |  |
| --- | --- |
| Id | 3002 |
| Name | ws\_role\_voice |
| Type | RADIUS |
| Action | Accept |

Table - Enforcement profile: ws\_role\_voice

| Type | Name | Value |
| --- | --- | --- |
| Radius:Aruba | Aruba-User-Role | voice |

Table - Atttributes : ws\_role\_voice

### 1.6.4.51 Enforcement Profiles: ws\_role\_BYOD

|  |  |
| --- | --- |
| Id | 3003 |
| Name | ws\_role\_BYOD |
| Type | RADIUS |
| Action | Accept |

Table - Enforcement profile: ws\_role\_BYOD

| Type | Name | Value |
| --- | --- | --- |
| Radius:Aruba | Aruba-User-Role | BYOD |

Table - Atttributes : ws\_role\_BYOD

### 1.6.4.52 Enforcement Profiles: ws\_role\_admin

|  |  |
| --- | --- |
| Id | 3004 |
| Name | ws\_role\_admin |
| Type | RADIUS |
| Action | Accept |

Table - Enforcement profile: ws\_role\_admin

| Type | Name | Value |
| --- | --- | --- |
| Radius:Aruba | Aruba-User-Role | admin |

Table - Atttributes : ws\_role\_admin

### 1.6.4.53 Enforcement Profiles: ws\_role\_contractor

|  |  |
| --- | --- |
| Id | 3005 |
| Name | ws\_role\_contractor |
| Type | RADIUS |
| Action | Accept |

Table - Enforcement profile: ws\_role\_contractor

| Type | Name | Value |
| --- | --- | --- |
| Radius:Aruba | Aruba-User-Role | contractor |

Table - Atttributes : ws\_role\_contractor

### 1.6.4.54 Enforcement Profiles: ws\_vlan11\_corporate

|  |  |
| --- | --- |
| Id | 3006 |
| Name | ws\_vlan11\_corporate |
| Type | RADIUS |
| Action | Accept |

Table - Enforcement profile: ws\_vlan11\_corporate

| Type | Name | Value |
| --- | --- | --- |
| Radius:IETF | Session-Timeout | 10800 |
| Radius:IETF | Termination-Action | RADIUS-Request (1) |
| Radius:IETF | Tunnel-Type | VLAN (13) |
| Radius:IETF | Tunnel-Medium-Type | IEEE-802 (6) |
| Radius:IETF | Tunnel-Private-Group-Id | 11 |

Table - Atttributes : ws\_vlan11\_corporate

### 1.6.4.55 Enforcement Profiles: ws\_vlan12\_voice

|  |  |
| --- | --- |
| Id | 3007 |
| Name | ws\_vlan12\_voice |
| Type | RADIUS |
| Action | Accept |

Table - Enforcement profile: ws\_vlan12\_voice

| Type | Name | Value |
| --- | --- | --- |
| Radius:IETF | Session-Timeout | 10800 |
| Radius:IETF | Termination-Action | RADIUS-Request (1) |
| Radius:IETF | Tunnel-Type | VLAN (13) |
| Radius:IETF | Tunnel-Medium-Type | IEEE-802 (6) |
| Radius:IETF | Tunnel-Private-Group-Id | 12 |

Table - Atttributes : ws\_vlan12\_voice

### 1.6.4.56 Enforcement Profiles: ws\_vlan13\_guest

|  |  |
| --- | --- |
| Id | 3008 |
| Name | ws\_vlan13\_guest |
| Type | RADIUS |
| Action | Accept |

Table - Enforcement profile: ws\_vlan13\_guest

| Type | Name | Value |
| --- | --- | --- |
| Radius:IETF | Session-Timeout | 10800 |
| Radius:IETF | Termination-Action | RADIUS-Request (1) |
| Radius:IETF | Tunnel-Type | VLAN (13) |
| Radius:IETF | Tunnel-Medium-Type | IEEE-802 (6) |
| Radius:IETF | Tunnel-Private-Group-Id | 13 |

Table - Atttributes : ws\_vlan13\_guest

### 1.6.4.57 Enforcement Profiles: ws\_vlan14\_untrust

|  |  |
| --- | --- |
| Id | 3009 |
| Name | ws\_vlan14\_untrust |
| Type | RADIUS |
| Action | Accept |

Table - Enforcement profile: ws\_vlan14\_untrust

| Type | Name | Value |
| --- | --- | --- |
| Radius:IETF | Session-Timeout | 10800 |
| Radius:IETF | Termination-Action | RADIUS-Request (1) |
| Radius:IETF | Tunnel-Type | VLAN (13) |
| Radius:IETF | Tunnel-Medium-Type | IEEE-802 (6) |
| Radius:IETF | Tunnel-Private-Group-Id | 14 |

Table - Atttributes : ws\_vlan14\_untrust

### 1.6.4.58 Enforcement Profiles: ws\_vlan10\_management

|  |  |
| --- | --- |
| Id | 3010 |
| Name | ws\_vlan10\_management |
| Type | RADIUS |
| Action | Accept |

Table - Enforcement profile: ws\_vlan10\_management

| Type | Name | Value |
| --- | --- | --- |
| Radius:IETF | Session-Timeout | 10800 |
| Radius:IETF | Termination-Action | RADIUS-Request (1) |
| Radius:IETF | Tunnel-Type | VLAN (13) |
| Radius:IETF | Tunnel-Medium-Type | IEEE-802 (6) |
| Radius:IETF | Tunnel-Private-Group-Id | 10 |

Table - Atttributes : ws\_vlan10\_management

### 1.6.4.59 Enforcement Profiles: ws\_vlan10\_management\_aruba

|  |  |
| --- | --- |
| Id | 3011 |
| Name | ws\_vlan10\_management\_aruba |
| Type | RADIUS |
| Action | Accept |

Table - Enforcement profile: ws\_vlan10\_management\_aruba

| Type | Name | Value |
| --- | --- | --- |
| Radius:Aruba | Aruba-User-Vlan | 10 |

Table - Atttributes : ws\_vlan10\_management\_aruba

### 1.6.4.60 Enforcement Profiles: ws\_vlan11\_corporate\_aruba

|  |  |
| --- | --- |
| Id | 3012 |
| Name | ws\_vlan11\_corporate\_aruba |
| Type | RADIUS |
| Action | Accept |

Table - Enforcement profile: ws\_vlan11\_corporate\_aruba

| Type | Name | Value |
| --- | --- | --- |
| Radius:Aruba | Aruba-User-Vlan | 11 |

Table - Atttributes : ws\_vlan11\_corporate\_aruba

### 1.6.4.61 Enforcement Profiles: ws\_vlan13\_guest\_aruba

|  |  |
| --- | --- |
| Id | 3013 |
| Name | ws\_vlan13\_guest\_aruba |
| Type | RADIUS |
| Action | Accept |

Table - Enforcement profile: ws\_vlan13\_guest\_aruba

| Type | Name | Value |
| --- | --- | --- |
| Radius:Aruba | Aruba-User-Vlan | 13 |

Table - Atttributes : ws\_vlan13\_guest\_aruba

### 1.6.4.62 Enforcement Profiles: ws\_vlan14\_untrust\_aruba

|  |  |
| --- | --- |
| Id | 3014 |
| Name | ws\_vlan14\_untrust\_aruba |
| Type | RADIUS |
| Action | Accept |

Table - Enforcement profile: ws\_vlan14\_untrust\_aruba

| Type | Name | Value |
| --- | --- | --- |
| Radius:Aruba | Aruba-User-Vlan | 14 |

Table - Atttributes : ws\_vlan14\_untrust\_aruba

### 1.6.4.63 Enforcement Profiles: ws\_vlan12\_voice\_aruba

|  |  |
| --- | --- |
| Id | 3015 |
| Name | ws\_vlan12\_voice\_aruba |
| Type | RADIUS |
| Action | Accept |

Table - Enforcement profile: ws\_vlan12\_voice\_aruba

| Type | Name | Value |
| --- | --- | --- |
| Radius:Aruba | Aruba-User-Vlan | 12 |

Table - Atttributes : ws\_vlan12\_voice\_aruba

### 1.6.4.64 Enforcement Profiles: ws\_AOS-S-mgt-RW

|  |  |
| --- | --- |
| Id | 3016 |
| Name | ws\_AOS-S-mgt-RW |
| Type | TACACS |
| Action | Accept |

Table - Enforcement profile: ws\_AOS-S-mgt-RW

| Privilege Level | Services | Authorize Attribute Status |
| --- | --- | --- |
| 15 | Shell | ADD |

Table - Tacacs Services Params: ws\_AOS-S-mgt-RW

### 1.6.4.65 Enforcement Profiles: ws\_AOS-S-mgt-RO

|  |  |
| --- | --- |
| Id | 3017 |
| Name | ws\_AOS-S-mgt-RO |
| Type | TACACS |
| Action | Accept |

Table - Enforcement profile: ws\_AOS-S-mgt-RO

| Privilege Level | Services | Authorize Attribute Status |
| --- | --- | --- |
| 14 | Shell | ADD |

Table - Tacacs Services Params: ws\_AOS-S-mgt-RO

### 1.6.4.66 Enforcement Profiles: ws\_Guest Guest Profile

|  |  |
| --- | --- |
| Id | 3018 |
| Name | ws\_Guest Guest Profile |
| Type | RADIUS |
| Action | Accept |

Table - Enforcement profile: ws\_Guest Guest Profile

| Type | Name | Value |
| --- | --- | --- |
| Radius:Aruba | Aruba-User-Role | guest-1 |
| Radius:IETF | User-Name | %{Endpoint:Username} |

Table - Atttributes : ws\_Guest Guest Profile

### 1.6.4.67 Enforcement Profiles: ws\_Guest Captive Portal Profile

|  |  |
| --- | --- |
| Id | 3019 |
| Name | ws\_Guest Captive Portal Profile |
| Type | RADIUS |
| Action | Accept |

Table - Enforcement profile: ws\_Guest Captive Portal Profile

| Type | Name | Value |
| --- | --- | --- |
| Radius:Aruba | Aruba-User-Role | guest-register |

Table - Atttributes : ws\_Guest Captive Portal Profile

### 1.6.4.68 Enforcement Profiles: ws\_Guest MAC Caching Session Timeout

|  |  |
| --- | --- |
| Id | 3020 |
| Name | ws\_Guest MAC Caching Session Timeout |
| Type | RADIUS |
| Action | Accept |

Table - Enforcement profile: ws\_Guest MAC Caching Session Timeout

| Type | Name | Value |
| --- | --- | --- |
| Radius:IETF | Session-Timeout | %{Authorization:[Guest User Repository]:RemainingExpiration} |

Table - Atttributes : ws\_Guest MAC Caching Session Timeout

### 1.6.4.69 Enforcement Profiles: ws\_Guest MAC Caching Do Expire

|  |  |
| --- | --- |
| Id | 3021 |
| Name | ws\_Guest MAC Caching Do Expire |
| Type | Post\_Authentication |

Table - Enforcement profile: ws\_Guest MAC Caching Do Expire

| Type | Name | Value |
| --- | --- | --- |
| Expiry-Check | Expiry-Action | %{GuestUser:do\_expire} |

Table - Atttributes : ws\_Guest MAC Caching Do Expire

### 1.6.4.70 Enforcement Profiles: ws\_Guest MAC Caching Expire Post Login

|  |  |
| --- | --- |
| Id | 3022 |
| Name | ws\_Guest MAC Caching Expire Post Login |
| Type | Post\_Authentication |

Table - Enforcement profile: ws\_Guest MAC Caching Expire Post Login

| Type | Name | Value |
| --- | --- | --- |
| Expire-Time-Update | GuestUser | %{GuestUser:expire\_postlogin} |

Table - Atttributes : ws\_Guest MAC Caching Expire Post Login

### 1.6.4.71 Enforcement Profiles: ws\_Guest MAC Caching Bandwidth Limit

|  |  |
| --- | --- |
| Id | 3023 |
| Name | ws\_Guest MAC Caching Bandwidth Limit |
| Type | Post\_Authentication |

Table - Enforcement profile: ws\_Guest MAC Caching Bandwidth Limit

| Type | Name | Value |
| --- | --- | --- |
| Bandwidth-Check | Allowed-Limit | 50 |
| Bandwidth-Check | Limit-Units | MB |
| Bandwidth-Check | Check-Type | Today |
| Post-Auth-Check | Action | Disconnect |

Table - Atttributes : ws\_Guest MAC Caching Bandwidth Limit

### 1.6.4.72 Enforcement Profiles: ws\_Guest MAC Caching Session Limit

|  |  |
| --- | --- |
| Id | 3024 |
| Name | ws\_Guest MAC Caching Session Limit |
| Type | Post\_Authentication |

Table - Enforcement profile: ws\_Guest MAC Caching Session Limit

| Type | Name | Value |
| --- | --- | --- |
| Session-Check | Active-Session-Count | %{GuestUser:simultaneous\_use} |
| Post-Auth-Check | Action | Disconnect and Block Access |

Table - Atttributes : ws\_Guest MAC Caching Session Limit

### 1.6.4.73 Enforcement Profiles: ws\_Guest Guest MAC Caching

|  |  |
| --- | --- |
| Id | 3025 |
| Name | ws\_Guest Guest MAC Caching |
| Type | Post\_Authentication |

Table - Enforcement profile: ws\_Guest Guest MAC Caching

| Type | Name | Value |
| --- | --- | --- |
| Endpoint | Username | %{Authentication:Username} |
| Endpoint | Guest Role ID | %{GuestUser:Role ID} |
| Endpoint | MAC-Auth Expiry | %{Authorization:[Guest User Repository]:ExpireTime} |

Table - Atttributes : ws\_Guest Guest MAC Caching

### 1.6.4.74 Enforcement Profiles: ws\_Operator\_Receptionist

|  |  |
| --- | --- |
| Id | 3026 |
| Name | ws\_Operator\_Receptionist |
| Type | Application |
| Action | Accept |

Table - Enforcement profile: ws\_Operator\_Receptionist

| Type | Name | Value |
| --- | --- | --- |
|  | admin\_privileges | Receptionist |

Table - Atttributes : ws\_Operator\_Receptionist

### 1.6.4.75 Enforcement Profiles: ws\_Operator\_Device\_Registration

|  |  |
| --- | --- |
| Id | 3027 |
| Name | ws\_Operator\_Device\_Registration |
| Type | Application |
| Action | Accept |

Table - Enforcement profile: ws\_Operator\_Device\_Registration

| Type | Name | Value |
| --- | --- | --- |
|  | admin\_privileges | Device Registration |

Table - Atttributes : ws\_Operator\_Device\_Registration

### 1.6.4.76 Enforcement Profiles: ws\_role\_onboard-redirect

|  |  |
| --- | --- |
| Id | 3028 |
| Name | ws\_role\_onboard-redirect |
| Type | RADIUS |
| Action | Accept |

Table - Enforcement profile: ws\_role\_onboard-redirect

| Type | Name | Value |
| --- | --- | --- |
| Radius:Aruba | Aruba-User-Role | onboard-redirect |

Table - Atttributes : ws\_role\_onboard-redirect

### 1.6.4.77 Enforcement Profiles: ws\_role\_guest-redirect

|  |  |
| --- | --- |
| Id | 3029 |
| Name | ws\_role\_guest-redirect |
| Type | RADIUS |
| Action | Accept |

Table - Enforcement profile: ws\_role\_guest-redirect

| Type | Name | Value |
| --- | --- | --- |
| Radius:Aruba | Aruba-User-Role | guest-redirect |

Table - Atttributes : ws\_role\_guest-redirect

### 1.6.4.78 Enforcement Profiles: ws\_vlan203\_tunneled\_aruba

|  |  |
| --- | --- |
| Id | 3030 |
| Name | ws\_vlan203\_tunneled\_aruba |
| Type | RADIUS |
| Action | Accept |

Table - Enforcement profile: ws\_vlan203\_tunneled\_aruba

| Type | Name | Value |
| --- | --- | --- |
| Radius:Aruba | Aruba-User-Vlan | 203 |

Table - Atttributes : ws\_vlan203\_tunneled\_aruba

### 1.6.4.79 Enforcement Profiles: ws\_dACL\_untrusted

|  |  |
| --- | --- |
| Id | 3031 |
| Name | ws\_dACL\_untrusted |
| Type | RADIUS |
| Action | Accept |

Table - Enforcement profile: ws\_dACL\_untrusted

| Type | Name | Value |
| --- | --- | --- |
| Radius:IETF | NAS-Filter-Rule | permit in udp from any to any 53,67 |
| Radius:IETF | NAS-Filter-Rule | deny in ip from any to 10.1.254.0/24 |
| Radius:IETF | NAS-Filter-Rule | permit in ip from any to any |

Table - Atttributes : ws\_dACL\_untrusted

### 1.6.4.80 Enforcement Profiles: ws\_dACL\_redirect

|  |  |
| --- | --- |
| Id | 3032 |
| Name | ws\_dACL\_redirect |
| Type | RADIUS |
| Action | Accept |

Table - Enforcement profile: ws\_dACL\_redirect

| Type | Name | Value |
| --- | --- | --- |
| Radius:IETF | NAS-Filter-Rule | permit in udp from any to any 53,67 |
| Radius:Hewlett-Packard-Enterprise | HPE-Captive-Portal-URL | https://cppm.arubalab.com/guest/wired-guest.php |
| Radius:IETF | NAS-Filter-Rule | permit in tcp from any to 10.1.254.21 80, 443 |
| Radius:IETF | NAS-Filter-Rule | deny in tcp from any to any 80 cpy |

Table - Atttributes : ws\_dACL\_redirect

### 1.6.4.81 Enforcement Profiles: ws\_dACL\_voice

|  |  |
| --- | --- |
| Id | 3034 |
| Name | ws\_dACL\_voice |
| Type | RADIUS |
| Action | Accept |

Table - Enforcement profile: ws\_dACL\_voice

| Type | Name | Value |
| --- | --- | --- |
| Radius:IETF | NAS-Filter-Rule | permit in udp from any to any 53,67 |
| Radius:IETF | NAS-Filter-Rule | permit in ip from any to 10.1.254.28 |
| Radius:IETF | NAS-Filter-Rule | permit in ip from any to 10.1.254.21 |
| Radius:IETF | NAS-Filter-Rule | deny in ip from any to any any |

Table - Atttributes : ws\_dACL\_voice

### 1.6.4.82 Enforcement Profiles: ws\_hpe\_role\_admin

|  |  |
| --- | --- |
| Id | 3035 |
| Name | ws\_hpe\_role\_admin |
| Type | RADIUS |
| Action | Accept |

Table - Enforcement profile: ws\_hpe\_role\_admin

| Type | Name | Value |
| --- | --- | --- |
| Radius:Hewlett-Packard-Enterprise | HPE-User-Role | admin |

Table - Atttributes : ws\_hpe\_role\_admin

### 1.6.4.83 Enforcement Profiles: ws\_hpe\_role\_guest-redirect

|  |  |
| --- | --- |
| Id | 3036 |
| Name | ws\_hpe\_role\_guest-redirect |
| Type | RADIUS |
| Action | Accept |

Table - Enforcement profile: ws\_hpe\_role\_guest-redirect

| Type | Name | Value |
| --- | --- | --- |
| Radius:Hewlett-Packard-Enterprise | HPE-User-Role | guest-redirect |

Table - Atttributes : ws\_hpe\_role\_guest-redirect

### 1.6.4.84 Enforcement Profiles: ws\_hpe\_role\_contractor

|  |  |
| --- | --- |
| Id | 3037 |
| Name | ws\_hpe\_role\_contractor |
| Type | RADIUS |
| Action | Accept |

Table - Enforcement profile: ws\_hpe\_role\_contractor

| Type | Name | Value |
| --- | --- | --- |
| Radius:Hewlett-Packard-Enterprise | HPE-User-Role | contractor |

Table - Atttributes : ws\_hpe\_role\_contractor

### 1.6.4.85 Enforcement Profiles: ws\_hpe\_role\_employee

|  |  |
| --- | --- |
| Id | 3038 |
| Name | ws\_hpe\_role\_employee |
| Type | RADIUS |
| Action | Accept |

Table - Enforcement profile: ws\_hpe\_role\_employee

| Type | Name | Value |
| --- | --- | --- |
| Radius:Hewlett-Packard-Enterprise | HPE-User-Role | employee |

Table - Atttributes : ws\_hpe\_role\_employee

### 1.6.4.86 Enforcement Profiles: ws\_hpe\_role\_voice

|  |  |
| --- | --- |
| Id | 3039 |
| Name | ws\_hpe\_role\_voice |
| Type | RADIUS |
| Action | Accept |

Table - Enforcement profile: ws\_hpe\_role\_voice

| Type | Name | Value |
| --- | --- | --- |
| Radius:Hewlett-Packard-Enterprise | HPE-User-Role | voice |

Table - Atttributes : ws\_hpe\_role\_voice

### 1.6.4.87 Enforcement Profiles: ws\_hpe\_role\_guest

|  |  |
| --- | --- |
| Id | 3040 |
| Name | ws\_hpe\_role\_guest |
| Type | RADIUS |
| Action | Accept |

Table - Enforcement profile: ws\_hpe\_role\_guest

| Type | Name | Value |
| --- | --- | --- |
| Radius:Hewlett-Packard-Enterprise | HPE-User-Role | guest |

Table - Atttributes : ws\_hpe\_role\_guest

### 1.6.4.88 Enforcement Profiles: ws\_AOS-SW-Admin-priv

|  |  |
| --- | --- |
| Id | 3041 |
| Name | ws\_AOS-SW-Admin-priv |
| Type | RADIUS |
| Action | Accept |

Table - Enforcement profile: ws\_AOS-SW-Admin-priv

| Type | Name | Value |
| --- | --- | --- |
| Radius:IETF | Service-Type | Administrative-User (6) |

Table - Atttributes : ws\_AOS-SW-Admin-priv

### 1.6.4.89 Enforcement Profiles: ws\_airheads\_security\_update

|  |  |
| --- | --- |
| Id | 3042 |
| Name | ws\_airheads\_security\_update |
| Type | Post\_Authentication |

Table - Enforcement profile: ws\_airheads\_security\_update

| Type | Name | Value |
| --- | --- | --- |
| Session-Notify | Server Type | Generic HTTP |
| Session-Notify | Server IP | ubuntu.arubalab.loc |
| Session-Notify | Login Action | Arubalab Login |
| Session-Notify | Logout Action | Arubalab Logout |

Table - Atttributes : ws\_airheads\_security\_update

### 1.6.4.90 Enforcement Profiles: ws\_quarantine\_set\_security\_info\_juniper\_srx

|  |  |
| --- | --- |
| Id | 3044 |
| Name | ws\_quarantine\_set\_security\_info\_juniper\_srx |
| Type | Post\_Authentication |

Table - Enforcement profile: ws\_quarantine\_set\_security\_info\_juniper\_srx

| Type | Name | Value |
| --- | --- | --- |
| Endpoint | Compromised | true |
| Endpoint | Threat Detection Time | %{Event:Juniper-SRX-TS:time} |
| Endpoint | Threat Name | %{Event:Juniper-SRX-TS:application-name} |
| Endpoint | Threat Category | %{Event:Juniper-SRX-TS:message-type} |

Table - Atttributes : ws\_quarantine\_set\_security\_info\_juniper\_srx

### 1.6.4.91 Enforcement Profiles: ws\_role\_quarantine

|  |  |
| --- | --- |
| Id | 3045 |
| Name | ws\_role\_quarantine |
| Type | RADIUS |
| Action | Accept |

Table - Enforcement profile: ws\_role\_quarantine

| Type | Name | Value |
| --- | --- | --- |
| Radius:Aruba | Aruba-User-Role | quarantine |

Table - Atttributes : ws\_role\_quarantine

### 1.6.4.92 Enforcement Profiles: ws\_clear\_comprimized

|  |  |
| --- | --- |
| Id | 3046 |
| Name | ws\_clear\_comprimized |
| Type | Post\_Authentication |

Table - Enforcement profile: ws\_clear\_comprimized

| Type | Name | Value |
| --- | --- | --- |
| Endpoint | Compromised | false |

Table - Atttributes : ws\_clear\_comprimized

### 1.6.4.93 Enforcement Profiles: ws\_snmp\_vlan31

|  |  |
| --- | --- |
| Id | 3047 |
| Name | ws\_snmp\_vlan31 |
| Type | SNMP |

Table - Enforcement profile: ws\_snmp\_vlan31

| Type | Name | Value |
| --- | --- | --- |
|  | VLAN ID | 31 |

Table - Atttributes : ws\_snmp\_vlan31

### 1.6.4.94 Enforcement Profiles: ws\_snmp\_bounce\_port

|  |  |
| --- | --- |
| Id | 3048 |
| Name | ws\_snmp\_bounce\_port |
| Type | SNMP |

Table - Enforcement profile: ws\_snmp\_bounce\_port

| Type | Name | Value |
| --- | --- | --- |
|  | Reset Connection (after the settings are applied) | Enabled |

Table - Atttributes : ws\_snmp\_bounce\_port

### 1.6.4.95 Enforcement Profiles: ws\_quarantine\_release\_error

|  |  |
| --- | --- |
| Id | 3049 |
| Name | ws\_quarantine\_release\_error |
| Type | Application |
| Action | Reject |

Table - Enforcement profile: ws\_quarantine\_release\_error

| Type | Name | Value |
| --- | --- | --- |
|  | ClearPass:Error-Message | Sorry, you can only release yourself once a day! Contact the helpdesk. |

Table - Atttributes : ws\_quarantine\_release\_error

### 1.6.4.96 Enforcement Profiles: ws\_quarantine\_reset\_and\_set\_timestamp

|  |  |
| --- | --- |
| Id | 3050 |
| Name | ws\_quarantine\_reset\_and\_set\_timestamp |
| Type | Post\_Authentication |

Table - Enforcement profile: ws\_quarantine\_reset\_and\_set\_timestamp

| Type | Name | Value |
| --- | --- | --- |
| Endpoint | Threat Release Timeout | %{Authorization:[Time Source]:One Day DT} |
| Endpoint | Compromised | false |

Table - Atttributes : ws\_quarantine\_reset\_and\_set\_timestamp

### 1.6.4.97 Enforcement Profiles: ws\_snmp\_vlan39

|  |  |
| --- | --- |
| Id | 3051 |
| Name | ws\_snmp\_vlan39 |
| Type | SNMP |

Table - Enforcement profile: ws\_snmp\_vlan39

| Type | Name | Value |
| --- | --- | --- |
|  | VLAN ID | 39 |

Table - Atttributes : ws\_snmp\_vlan39

### 1.6.4.98 Enforcement Profiles: ws\_snmp\_vlan11\_corporate

|  |  |
| --- | --- |
| Id | 3052 |
| Name | ws\_snmp\_vlan11\_corporate |
| Type | SNMP |

Table - Enforcement profile: ws\_snmp\_vlan11\_corporate

| Type | Name | Value |
| --- | --- | --- |
|  | VLAN ID | 11 |

Table - Atttributes : ws\_snmp\_vlan11\_corporate

### 1.6.4.99 Enforcement Profiles: ws\_snmp\_vlan14\_untrust

|  |  |
| --- | --- |
| Id | 3053 |
| Name | ws\_snmp\_vlan14\_untrust |
| Type | SNMP |

Table - Enforcement profile: ws\_snmp\_vlan14\_untrust

| Type | Name | Value |
| --- | --- | --- |
|  | VLAN ID | 14 |

Table - Atttributes : ws\_snmp\_vlan14\_untrust

### 1.6.4.100 Enforcement Profiles: ws\_snmp\_vlan12\_voice

|  |  |
| --- | --- |
| Id | 3054 |
| Name | ws\_snmp\_vlan12\_voice |
| Type | SNMP |

Table - Enforcement profile: ws\_snmp\_vlan12\_voice

| Type | Name | Value |
| --- | --- | --- |
|  | VLAN ID | 12 |

Table - Atttributes : ws\_snmp\_vlan12\_voice

### 1.6.4.101 Enforcement Profiles: ws\_role\_onguard-redirect

|  |  |
| --- | --- |
| Id | 3055 |
| Name | ws\_role\_onguard-redirect |
| Type | RADIUS |
| Action | Accept |

Table - Enforcement profile: ws\_role\_onguard-redirect

| Type | Name | Value |
| --- | --- | --- |
| Radius:Aruba | Aruba-User-Role | onguard-redirect |

Table - Atttributes : ws\_role\_onguard-redirect

### 1.6.4.102 Enforcement Profiles: ws\_Airwave\_admin

|  |  |
| --- | --- |
| Id | 3059 |
| Name | ws\_Airwave\_admin |
| Type | RADIUS |
| Action | Accept |

Table - Enforcement profile: ws\_Airwave\_admin

| Type | Name | Value |
| --- | --- | --- |
| Radius:Aruba | Aruba-Admin-Role | Admin |

Table - Atttributes : ws\_Airwave\_admin

### 1.6.4.103 Enforcement Profiles: ws\_iap\_with\_tagged\_vlans

|  |  |
| --- | --- |
| Id | 3060 |
| Name | ws\_iap\_with\_tagged\_vlans |
| Type | RADIUS |
| Action | Accept |

Table - Enforcement profile: ws\_iap\_with\_tagged\_vlans

| Type | Name | Value |
| --- | --- | --- |
| Radius:Hewlett-Packard-Enterprise | HPE-Egress-VLAN-Name | 2Management VLAN |
| Radius:Hewlett-Packard-Enterprise | HPE-Egress-VLAN-Name | 1Corporate VLAN |
| Radius:Hewlett-Packard-Enterprise | HPE-Egress-VLAN-Name | 1Voice VLAN |
| Radius:Hewlett-Packard-Enterprise | HPE-Egress-VLAN-Name | 1Guest VLAN |
| Radius:Hewlett-Packard-Enterprise | HPE-Egress-VLAN-Name | 1Untrusted VLAN |
| Radius:Hewlett-Packard-Enterprise | HPE-Port-MA-Port-Mode | Port-Based (1) |
| Radius:Hewlett-Packard-Enterprise | HPE-Port-Dot1x-Client-Limit | 0 |

Table - Atttributes : ws\_iap\_with\_tagged\_vlans

### 1.6.4.104 Enforcement Profiles: ws\_vlan90\_management

|  |  |
| --- | --- |
| Id | 3061 |
| Name | ws\_vlan90\_management |
| Type | RADIUS |
| Action | Accept |

Table - Enforcement profile: ws\_vlan90\_management

| Type | Name | Value |
| --- | --- | --- |
| Radius:IETF | Session-Timeout | 10800 |
| Radius:IETF | Termination-Action | RADIUS-Request (1) |
| Radius:IETF | Tunnel-Type | VLAN (13) |
| Radius:IETF | Tunnel-Medium-Type | IEEE-802 (6) |
| Radius:IETF | Tunnel-Private-Group-Id | 90 |

Table - Atttributes : ws\_vlan90\_management

### 1.6.4.105 Enforcement Profiles: ws\_vlan94\_untrust

|  |  |
| --- | --- |
| Id | 3062 |
| Name | ws\_vlan94\_untrust |
| Type | RADIUS |
| Action | Accept |

Table - Enforcement profile: ws\_vlan94\_untrust

| Type | Name | Value |
| --- | --- | --- |
| Radius:IETF | Session-Timeout | 10800 |
| Radius:IETF | Termination-Action | RADIUS-Request (1) |
| Radius:IETF | Tunnel-Type | VLAN (13) |
| Radius:IETF | Tunnel-Medium-Type | IEEE-802 (6) |
| Radius:IETF | Tunnel-Private-Group-Id | 94 |

Table - Atttributes : ws\_vlan94\_untrust

### 1.6.4.106 Enforcement Profiles: ws\_vlan\_voice

|  |  |
| --- | --- |
| Id | 3063 |
| Name | ws\_vlan\_voice |
| Type | RADIUS |
| Action | Accept |

Table - Enforcement profile: ws\_vlan\_voice

| Type | Name | Value |
| --- | --- | --- |
| Radius:IETF | Session-Timeout | 10800 |
| Radius:IETF | Termination-Action | RADIUS-Request (1) |
| Radius:IETF | Tunnel-Type | VLAN (13) |
| Radius:IETF | Tunnel-Medium-Type | IEEE-802 (6) |
| Radius:IETF | Tunnel-Private-Group-Id | Voice VLAN |

Table - Atttributes : ws\_vlan\_voice

### 1.6.4.107 Enforcement Profiles: ws\_dACL\_internal\_only

|  |  |
| --- | --- |
| Id | 3065 |
| Name | ws\_dACL\_internal\_only |
| Type | RADIUS |
| Action | Accept |

Table - Enforcement profile: ws\_dACL\_internal\_only

| Type | Name | Value |
| --- | --- | --- |
| Radius:IETF | NAS-Filter-Rule | permit in udp from any to any 53,67 |
| Radius:IETF | NAS-Filter-Rule | permit in ip from any to 10.1.254.0/24 |
| Radius:IETF | NAS-Filter-Rule | deny in ip from any to any |

Table - Atttributes : ws\_dACL\_internal\_only

### 1.6.4.108 Enforcement Profiles: ws\_vlan\_corporate

|  |  |
| --- | --- |
| Id | 3066 |
| Name | ws\_vlan\_corporate |
| Type | RADIUS |
| Action | Accept |

Table - Enforcement profile: ws\_vlan\_corporate

| Type | Name | Value |
| --- | --- | --- |
| Radius:IETF | Session-Timeout | 600 |
| Radius:IETF | Termination-Action | RADIUS-Request (1) |
| Radius:IETF | Tunnel-Type | VLAN (13) |
| Radius:IETF | Tunnel-Medium-Type | IEEE-802 (6) |
| Radius:IETF | Tunnel-Private-Group-Id | Corporate VLAN |

Table - Atttributes : ws\_vlan\_corporate

### 1.6.4.109 Enforcement Profiles: ws\_vlan\_untrust

|  |  |
| --- | --- |
| Id | 3067 |
| Name | ws\_vlan\_untrust |
| Type | RADIUS |
| Action | Accept |

Table - Enforcement profile: ws\_vlan\_untrust

| Type | Name | Value |
| --- | --- | --- |
| Radius:IETF | Session-Timeout | 10800 |
| Radius:IETF | Termination-Action | RADIUS-Request (1) |
| Radius:IETF | Tunnel-Type | VLAN (13) |
| Radius:IETF | Tunnel-Medium-Type | IEEE-802 (6) |
| Radius:IETF | Tunnel-Private-Group-Id | Untrusted VLAN |

Table - Atttributes : ws\_vlan\_untrust

### 1.6.4.110 Enforcement Profiles: ws\_vlan\_guest

|  |  |
| --- | --- |
| Id | 3068 |
| Name | ws\_vlan\_guest |
| Type | RADIUS |
| Action | Accept |

Table - Enforcement profile: ws\_vlan\_guest

| Type | Name | Value |
| --- | --- | --- |
| Radius:IETF | Session-Timeout | 10800 |
| Radius:IETF | Termination-Action | RADIUS-Request (1) |
| Radius:IETF | Tunnel-Type | VLAN (13) |
| Radius:IETF | Tunnel-Medium-Type | IEEE-802 (6) |
| Radius:IETF | Tunnel-Private-Group-Id | Guest VLAN |

Table - Atttributes : ws\_vlan\_guest

### 1.6.4.111 Enforcement Profiles: ws\_vlan\_management

|  |  |
| --- | --- |
| Id | 3069 |
| Name | ws\_vlan\_management |
| Type | RADIUS |
| Action | Accept |

Table - Enforcement profile: ws\_vlan\_management

| Type | Name | Value |
| --- | --- | --- |
| Radius:IETF | Session-Timeout | 10800 |
| Radius:IETF | Termination-Action | RADIUS-Request (1) |
| Radius:IETF | Tunnel-Type | VLAN (13) |
| Radius:IETF | Tunnel-Medium-Type | IEEE-802 (6) |
| Radius:IETF | Tunnel-Private-Group-Id | Management VLAN |

Table - Atttributes : ws\_vlan\_management

### 1.6.4.112 Enforcement Profiles: ws\_dACL\_camera

|  |  |
| --- | --- |
| Id | 3070 |
| Name | ws\_dACL\_camera |
| Type | RADIUS |
| Action | Accept |

Table - Enforcement profile: ws\_dACL\_camera

| Type | Name | Value |
| --- | --- | --- |
| Radius:IETF | NAS-Filter-Rule | permit in udp from any to any 53,67 |
| Radius:IETF | NAS-Filter-Rule | permit in ip from any to 10.1.254.0/24 |
| Radius:IETF | NAS-Filter-Rule | deny in ip from any to any |

Table - Atttributes : ws\_dACL\_camera

### 1.6.4.113 Enforcement Profiles: ws\_dACL\_unmanaged\_IoT

|  |  |
| --- | --- |
| Id | 3071 |
| Name | ws\_dACL\_unmanaged\_IoT |
| Type | RADIUS |
| Action | Accept |

Table - Enforcement profile: ws\_dACL\_unmanaged\_IoT

| Type | Name | Value |
| --- | --- | --- |
| Radius:IETF | NAS-Filter-Rule | permit in udp from any to any 53,67 |
| Radius:IETF | NAS-Filter-Rule | permit in ip from any to 10.1.254.21 |
| Radius:IETF | NAS-Filter-Rule | deny in ip from any to 10.1.254.0/24 |
| Radius:IETF | NAS-Filter-Rule | permit in ip from any to any |

Table - Atttributes : ws\_dACL\_unmanaged\_IoT

### 1.6.4.114 Enforcement Profiles: ws\_iap1x\_with\_tagged\_vlans

|  |  |
| --- | --- |
| Id | 3072 |
| Name | ws\_iap1x\_with\_tagged\_vlans |
| Type | RADIUS |
| Action | Accept |

Table - Enforcement profile: ws\_iap1x\_with\_tagged\_vlans

| Type | Name | Value |
| --- | --- | --- |
| Radius:Hewlett-Packard-Enterprise | HPE-Egress-VLAN-Name | 2Management VLAN |
| Radius:Hewlett-Packard-Enterprise | HPE-Egress-VLAN-Name | 1Corporate VLAN |
| Radius:Hewlett-Packard-Enterprise | HPE-Egress-VLAN-Name | 1Voice VLAN |
| Radius:Hewlett-Packard-Enterprise | HPE-Egress-VLAN-Name | 1Guest VLAN |
| Radius:Hewlett-Packard-Enterprise | HPE-Egress-VLAN-Name | 1Untrusted VLAN |
| Radius:Hewlett-Packard-Enterprise | HPE-Port-Dot1x-Port-Mode | Port-Based (1) |
| Radius:Hewlett-Packard-Enterprise | HPE-Port-Macauth-Client-Limit | 0 |

Table - Atttributes : ws\_iap1x\_with\_tagged\_vlans

### 1.6.4.115 Enforcement Profiles: ws\_hpe\_role\_employee-tun

|  |  |
| --- | --- |
| Id | 3074 |
| Name | ws\_hpe\_role\_employee-tun |
| Type | RADIUS |
| Action | Accept |

Table - Enforcement profile: ws\_hpe\_role\_employee-tun

| Type | Name | Value |
| --- | --- | --- |
| Radius:Hewlett-Packard-Enterprise | HPE-User-Role | employee-tun |

Table - Atttributes : ws\_hpe\_role\_employee-tun

### 1.6.4.116 Enforcement Profiles: ws\_hpe\_role\_admin-tun

|  |  |
| --- | --- |
| Id | 3075 |
| Name | ws\_hpe\_role\_admin-tun |
| Type | RADIUS |
| Action | Accept |

Table - Enforcement profile: ws\_hpe\_role\_admin-tun

| Type | Name | Value |
| --- | --- | --- |
| Radius:Hewlett-Packard-Enterprise | HPE-User-Role | admin-tun |

Table - Atttributes : ws\_hpe\_role\_admin-tun

### 1.6.4.117 Enforcement Profiles: ws\_hpe\_role\_voice-tun

|  |  |
| --- | --- |
| Id | 3076 |
| Name | ws\_hpe\_role\_voice-tun |
| Type | RADIUS |
| Action | Accept |

Table - Enforcement profile: ws\_hpe\_role\_voice-tun

| Type | Name | Value |
| --- | --- | --- |
| Radius:Hewlett-Packard-Enterprise | HPE-User-Role | voice-tun |

Table - Atttributes : ws\_hpe\_role\_voice-tun

### 1.6.4.118 Enforcement Profiles: ws\_hpe\_role\_camera

|  |  |
| --- | --- |
| Id | 3077 |
| Name | ws\_hpe\_role\_camera |
| Type | RADIUS |
| Action | Accept |

Table - Enforcement profile: ws\_hpe\_role\_camera

| Type | Name | Value |
| --- | --- | --- |
| Radius:Hewlett-Packard-Enterprise | HPE-User-Role | camera |

Table - Atttributes : ws\_hpe\_role\_camera

### 1.6.4.119 Enforcement Profiles: ws\_hpe\_role\_iot-tun

|  |  |
| --- | --- |
| Id | 3078 |
| Name | ws\_hpe\_role\_iot-tun |
| Type | RADIUS |
| Action | Accept |

Table - Enforcement profile: ws\_hpe\_role\_iot-tun

| Type | Name | Value |
| --- | --- | --- |
| Radius:Hewlett-Packard-Enterprise | HPE-User-Role | iot-tun |

Table - Atttributes : ws\_hpe\_role\_iot-tun

### 1.6.4.120 Enforcement Profiles: ws\_hpe\_role\_profiler

|  |  |
| --- | --- |
| Id | 3079 |
| Name | ws\_hpe\_role\_profiler |
| Type | RADIUS |
| Action | Accept |

Table - Enforcement profile: ws\_hpe\_role\_profiler

| Type | Name | Value |
| --- | --- | --- |
| Radius:Hewlett-Packard-Enterprise | HPE-User-Role | profiler |

Table - Atttributes : ws\_hpe\_role\_profiler

### 1.6.4.121 Enforcement Profiles: ws\_hpe\_role\_contractor-tun

|  |  |
| --- | --- |
| Id | 3080 |
| Name | ws\_hpe\_role\_contractor-tun |
| Type | RADIUS |
| Action | Accept |

Table - Enforcement profile: ws\_hpe\_role\_contractor-tun

| Type | Name | Value |
| --- | --- | --- |
| Radius:Hewlett-Packard-Enterprise | HPE-User-Role | contractor-tun |

Table - Atttributes : ws\_hpe\_role\_contractor-tun

### 1.6.4.122 Enforcement Profiles: ws\_hpe\_role\_guest-tun

|  |  |
| --- | --- |
| Id | 3081 |
| Name | ws\_hpe\_role\_guest-tun |
| Type | RADIUS |
| Action | Accept |

Table - Enforcement profile: ws\_hpe\_role\_guest-tun

| Type | Name | Value |
| --- | --- | --- |
| Radius:Hewlett-Packard-Enterprise | HPE-User-Role | guest-tun |

Table - Atttributes : ws\_hpe\_role\_guest-tun

### 1.6.4.123 Enforcement Profiles: ws\_dur\_employee

|  |  |
| --- | --- |
| Id | 3082 |
| Name | ws\_dur\_employee |
| Type | Aruba\_DUR |

Table - Enforcement profile: ws\_dur\_employee

| Type | Name | Value |
| --- | --- | --- |
| Radius:Hewlett-Packard-Enterprise | HPE-CPPM-Role | class ipv4 "employee-class-dur"<br>10 match ip 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255<br>exit<br>policy user "employee-policy-dur"<br>10 class ipv4 "employee-class-dur" action permit<br>exit<br>aaa authorization user-role name "employee-tun-dur"<br>policy "employee-policy-dur"<br>vlan-id 11<br>exit<br> |

Table - Atttributes : ws\_dur\_employee

### 1.6.4.124 Enforcement Profiles: ws\_dur\_voice

|  |  |
| --- | --- |
| Id | 3084 |
| Name | ws\_dur\_voice |
| Type | Aruba\_DUR |

Table - Enforcement profile: ws\_dur\_voice

### 1.6.4.125 Enforcement Profiles: ws\_dur\_camera

|  |  |
| --- | --- |
| Id | 3085 |
| Name | ws\_dur\_camera |
| Type | Aruba\_DUR |

Table - Enforcement profile: ws\_dur\_camera

| Type | Name | Value |
| --- | --- | --- |
| Radius:Hewlett-Packard-Enterprise | HPE-CPPM-Role | class ipv4 "class-dhcp-dns"<br> 10 match udp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 eq 67<br> 20 match udp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 eq 53<br> exit<br>class ipv4 "class-ipcam"<br> 10 match ip 0.0.0.0 255.255.255.255 10.1.254.24 0.0.0.0<br> 20 match ip 0.0.0.0 255.255.255.255 10.1.254.20 0.0.0.0<br> exit<br>class ipv4 "class-internal"<br> 10 match ip 0.0.0.0 255.255.255.255 10.1.0.0 0.0.255.255<br> exit<br>policy user "pol-ipcam"<br> 10 class ipv4 "class-dhcp-dns" action permit<br> 20 class ipv4 "class-ipcam" action permit<br> 30 class ipv4 "class-internal" action deny<br> exit<br>aaa authorization user-role name "camera-dur"<br>policy "pol-ipcam"<br>vlan-id 14<br>exit<br> |

Table - Atttributes : ws\_dur\_camera

### 1.6.4.126 Enforcement Profiles: ws\_dur\_redirect

|  |  |
| --- | --- |
| Id | 3087 |
| Name | ws\_dur\_redirect |
| Type | Aruba\_DUR |

Table - Enforcement profile: ws\_dur\_redirect

| Type | Name | Value |
| --- | --- | --- |
| Radius:Hewlett-Packard-Enterprise | HPE-CPPM-Role | class ipv4 "dhcp-dns"<br>10 match udp any any eq 67 <br>20 match udp any any eq 53 <br>exit<br>class ipv4 "internal"<br>10 match ip any 10.1.0.0/16 <br>exit<br>class ipv4 "class-clearpass"<br>10 match tcp any host 10.1.254.21 eq 443 <br>exit<br>class ipv4 "http"<br>10 match tcp any any eq 80 <br>exit<br>aaa authentication captive-portal profile "clearpass-redirect" url https://cppm.arubalab.com/guest/wired-guest.php<br>policy user "guest-redirect"<br>10 class ipv4 "dhcp-dns" action permit<br>20 class ipv4 "class-clearpass" action permit<br>30 class ipv4 "http" action redirect captive-portal<br>40 class ipv4 "internal" action deny<br>exit<br>aaa authorization user-role name "cp-redirect-dur"<br>captive-portal-profile "clearpass-redirect"<br>policy "guest-redirect"<br>vlan-id 13<br>exit<br> |

Table - Atttributes : ws\_dur\_redirect

### 1.6.4.127 Enforcement Profiles: radius\_rapi

|  |  |
| --- | --- |
| Id | 3088 |
| Name | radius\_rapi |
| Type | RADIUS |
| Action | Accept |

Table - Enforcement profile: radius\_rapi

| Type | Name | Value |
| --- | --- | --- |
| Radius:Aruba | Aruba-User-Role | raspberry-pi |

Table - Atttributes : radius\_rapi

### 1.6.4.128 Enforcement Profiles: ws\_Operator\_Super\_Administrator

|  |  |
| --- | --- |
| Id | 3090 |
| Name | ws\_Operator\_Super\_Administrator |
| Type | Application |
| Action | Accept |

Table - Enforcement profile: ws\_Operator\_Super\_Administrator

| Type | Name | Value |
| --- | --- | --- |
|  | admin\_privileges | Super Administrator |

Table - Atttributes : ws\_Operator\_Super\_Administrator

### 1.6.4.129 Enforcement Profiles: ws\_quarantine\_set\_security\_info\_checkpoint

|  |  |
| --- | --- |
| Id | 3091 |
| Name | ws\_quarantine\_set\_security\_info\_checkpoint |
| Type | Post\_Authentication |

Table - Enforcement profile: ws\_quarantine\_set\_security\_info\_checkpoint

| Type | Name | Value |
| --- | --- | --- |
| Endpoint | Compromised | true |
| Endpoint | Threat Detection Time | %{Event:CheckPoint-Log:time} |
| Endpoint | Threat Name | %{Event:CheckPoint-Log:Protectionname} |
| Endpoint | Threat Category | %{Event:CheckPoint-Log:product} |

Table - Atttributes : ws\_quarantine\_set\_security\_info\_checkpoint

## 1.7 Network Device

The following section details Network Device settings configured on ClearPass.

### 1.7.1 Summary

The following section provides a summary of Network Device settings.

|  |  |
| --- | --- |
| Network Device | 9 |
| Network Device Group | 2 |

Table - Network Device Summary

### 1.7.2 Network Device

The following section details Network Device configured on ClearPass.

| Id | Name | Description | IP Address | Vendor | CoA |
| --- | --- | --- | --- | --- | --- |
| 3001 | sw-workshop-01 |  | 10.1.10.1 | Hewlett-Packard-Enterprise | True |
| 3002 | instant-1 |  | 10.1.10.2 | Aruba | True |
| 3003 | controller |  | 10.1.254.0/24 | Aruba | True |
| 3004 | lab-iap |  | 10.1.3.2 | Aruba | True |
| 3005 | sw-workshop-03 |  | 10.1.30.254 | Hewlett-Packard-Enterprise | True |
| 3006 | sw-workshop-09 |  | 10.1.90.254 | Hewlett-Packard-Enterprise | True |
| 3008 | sw-workshop |  | 10.1.254.1 | Hewlett-Packard-Enterprise | True |
| 3010 | instant-10 |  | 10.1.10.5 | Aruba | True |
| 3012 | iap-192.2 |  | 192.168.2.0/24 | Aruba | True |

Table - Network Device

### 1.7.3 Network Device Group

The following section details Network Device Group configured on ClearPass.

| Id | Name | Description | Group Format | Value |
| --- | --- | --- | --- | --- |
| 3001 | team1 |  | list | 10.1.10.1 |
| 3002 | team3 |  | list | 10.1.30.254 |

Table - Network Device Group