**Creating an XML Request**

You can create XML requests to add, delete, authenticate, blacklist, or query a user. This section provides XML request formats that you can use for each authentication tasks.

|  |  |
| --- | --- |
|   | The XML API functionalities such as addition, deletion, role change, querying, authentication, and blacklisting has been extended to support IPv6 users in addition to IPv4 users. The XML API server is configured using only the IPv4 address. |
|   |   |

**Adding a User**

This XML requests uses the user\_add command to create a new user entry in the controllers user table. If the user entry is already present in the user table, the command will modify the entry with the values defined in the XML request.

xml=<aruba command="**user\_add**">

 <ipaddr>IP-address\_of\_the\_user</ipaddr>

 <macaddr>MAC-address\_of\_the\_user</macaddr>

 <name>User\_Name</name>

 <role>Role\_Name<role>

 <session\_timeout>Session\_timeout</session\_timeout>

 <key>Shared\_Key</key>

 <authentication>MD5|SHA-1|cleartext</authentication> #select any one

 <version>1.0</version>

</aruba>

The following options are mandatory when you execute the user\_add command:

|  |  |  |
| --- | --- | --- |
|  | ⚫ | IP Address |

|  |  |  |
| --- | --- | --- |
|  | ⚫ | Version |

**Deleting a User**

This XML requests uses the user\_delete command to delete an existing user from the controllers user table. If the user entry contains multiple attributes these must be specified in the XML request

xml=<aruba command="**user\_delete**">

 <ipaddr>IP-address\_of\_the\_user</ipaddr>

 <macaddr>MAC-address\_of\_the\_user</macaddr>

 <name>User\_Name</name>

 <key>Shared\_Key</key>

 <authentication>MD5|SHA-1|cleartext</authentication> #select any one

 <version>1.0</version>

</aruba>

The following options are mandatory when you execute the user\_add command:

|  |  |  |
| --- | --- | --- |
|  | ⚫ | IP Address |

|  |  |  |
| --- | --- | --- |
|  | ⚫ | Version |

**Authenticating a User**

This XML requests uses the user\_authenticate command to authenticate and derive a new for the user.

xml=<aruba command="**user\_authenticate**">

 <ipaddr>IP-address\_of\_the\_user</ipaddr>

 <macaddr>MAC-address\_of\_the\_user</macaddr>

 <name>User\_Name</name>

 <password>Password\_for\_the\_user</password>

 <key>Shared\_Key</key>

 <authentication>MD5|SHA-1|cleartext</authentication> #select any one

 <version>1.0</version>

</aruba>

The following options are mandatory when you execute the user\_authenticate command:

|  |  |  |
| --- | --- | --- |
|  | ⚫ | IP Address |

|  |  |  |
| --- | --- | --- |
|  | ⚫ | Version |

|  |  |  |
| --- | --- | --- |
|  | ⚫ | Name |

|  |  |  |
| --- | --- | --- |
|  | ⚫ | Password |

**Blacklisting a User**

This XML requests uses the user\_blacklist command to blacklist a user from connecting to your network.

xml=<aruba command="**user\_blacklist**">

 <ipaddr>IP-address\_of\_the\_user</ipaddr>

 <macaddr>MAC-address\_of\_the\_user</macaddr>

 <name>User\_Name</name>

 <key>Shared\_Key</key>

 <authentication>MD5|SHA-1|cleartext</authentication> #select any one

 <version>1.0</version>

</aruba>

The following options are mandatory when you execute the user\_blacklist command:

|  |  |  |
| --- | --- | --- |
|  | ⚫ | IP Address |

|  |  |  |
| --- | --- | --- |
|  | ⚫ | Version |

**Querying for User Status**

This XML requests uses the user\_query command to get the status and details of a user connected to your network.

xml=<aruba command="**user\_query**">

 <ipaddr>IP-address\_of\_the\_user</ipaddr>

 <macaddr>MAC-address\_of\_the\_user</macaddr>

 <name>User\_Name</name>

 <key>Shared\_Key</key>

 <authentication>MD5|SHA-1|cleartext</authentication> #select any one

 <version>1.0</version>

</aruba>

The following options are mandatory when you execute the user\_blacklist command:

|  |  |  |
| --- | --- | --- |
|  | ⚫ | IP Address |

|  |  |  |
| --- | --- | --- |
|  | ⚫ | Version |

**XML Response**

For every successful XML request the controller will return the processed information as an XML response. There are two types of responses: Default response and Query response.

**Default Response Format**

The format of a default XML response from the controller is:

<aruba>

 <result>Error | Ok</result>

 <code>response\_code</code>

 <reason>response\_message</reason>

</aruba>

In which,

|  |  |  |
| --- | --- | --- |
|  | ⚫ | Result specifies if the XML result was successful or failure. If the request was successful, the result tag will contain the **Ok**string. If the request was a failure, the result tag will contain the **Error** string. |

|  |  |  |
| --- | --- | --- |
|  | ⚫ | Code is an integer number that represents the error in the request. This tag is populated only if there is an error in the request. |

|  |  |  |
| --- | --- | --- |
|  | ⚫ | Reason is message that contain descriptive information about error. |

**Response Codes**

The following response codes are returned if the XML request return an the Error string.

| **Table 1:***XML Response Codes* |
| --- |
| **Code** | **Reason message** | **Description** |
| 1 | unknown user The user specified in the XML request does not exist or is incorrect. | Returned by the user\_authenticate,user\_delete, user\_blacklist, anduser\_query commands. |
| 2 | **unknown role**The specified role in the XML request does not exist in thecontroller. | Returned by the user\_add command. |
| 3 | unknown external agent  | Returned by all commands. |
| 4 | authentication failed The username and the key does not match. | Returned by commands that contain the shared\_key in XML request. |
| 5 | invalid command The XML request contains a command not supported byArubaOS XML API interface. | — |
| 6 | invalid message authentication method The authentication method specified in the XML request is not supported by the ArubaOS XML API interface. | Returned by commands that contain the authentication method in the XML request. |
| 7 | invalid message digest  | Returned by commands that contain the shared\_key in the XML request. |
| 8 | missing message authentication The authentication method is not specified in the XML request. | Returned by all commands that require the authentication method in the XML request. |
| 9 | **missing or invalid version number**The XML request does not contain the version number or the version number is incorrect. | Returned by all commands. |
| 10 | internal error  |   |
| 11 | client not authorized The shared key in the XML request does not match or the XML API server is not defined in the appropriate AAA profile. | Returned by all commands that require shared key to be specified in the XML request. |
| 12 | Cant use VLAN IP  | — |
| 13 | Invalid IP The XML request contains invalid IP address of the user or client. | Returned by all commands that required IP address to be specified in the XML request. |
| 14 | Cant use Switch IP The XML request contains the controllers IP address instead of the client IP address. | Returned by all commands that required IP address to be specified in the XML request.  |
| 15 | missing MAC address The XML request does not contain the MAC address of the user or client. | Returned by all commands that required MAC address to be specified in the XML request. |
| 16 | Unsupported command for this user | Returned when the requested operation is invalid for the specified user. |
| 17 | Socket failed or timed out waiting for operation to complete | Returned when the status of the requested operation is unavailable; usually signifies a socket communication failure or timeout. |

**Query Command Response Format**

The response of the XML request with the user\_query command contains detailed information about the status of the user or client. The format of the response of a query command is:

<aruba>

 <result>Result</result>

 <code>Code</code>

 <reason>Reason</reason>

 <role>Role</role>

 <type>Type</type>

 <auth\_status>Auth\_status</auth\_status>

 <auth\_server>Auth\_server</auth\_server>

 <auth\_method>Auth\_method</auth\_method>

 <location>Location</location>

 <age>Age</age>

 <essid>Essid</essid>

 <bssid>Bssid</bssid>

 <phy\_type>Phy\_type</phytype>

 <vlan>Vlan</vlan>

</aruba>

In which, the result, code and reason values are similar to the default response. The following responses, however, are returned only in the result code returns the **OK** string.

| **Table 2:***Query Response Code* |
| --- |
| **Response Code** | **Description** |
| Role | Displays the current role of the authenticated user |
| Type | Displays is the user or client is **wired** or **wireless**. |
| Auth\_status | Displays the authentication status of the user or client. Available values are:**authenticated** or **unauthenticated**. |
| Auth\_server | Displays the name of the authentication server used for authenticating the user. This information is available only if the user is authenticated by the controller. |
| Auth\_method | Displays the authentication mechanism used to authenticate the user. This information is available only if the user is authenticated by the controller. |
| Location | Displays the current location of the user / clients. For wireless clients, the location is displayed in the B.F.L format. For wired clients, the location is displayed in the slot/port format. |
| Age | Displays the age of user in the controller. The age is displayed in DD:HH:MM format (Day:Hours:Minutes). |
| ESSID | Displays the ESSID to which the user is associated. |
| BSSID | Displays the BSSID of the AP to which the user is associated. |
| Phy Type | Displays the physical connection type. One of a, b, or g. |
| Vlan | Displays the VLAN ID of the user. |

**Using the XML API Server**

To use the XML API:

|  |  |  |
| --- | --- | --- |
|  | 1. | Configure an external XML API server |

|  |  |  |
| --- | --- | --- |
|  | 2. | Associate the XML API server to an appropriate AAA profile |

|  |  |  |
| --- | --- | --- |
|  | 3. | Configure a user role to direct un-authenticated users to the external captive portal server |

|  |  |  |
| --- | --- | --- |
|  | 4. | Configure Captive Portal profile and associate that to an initial role (example logon) |

|  |  |  |
| --- | --- | --- |
|  | 5. | Create an XML request with the appropriate API call |

|  |  |  |
| --- | --- | --- |
|  | 6. | Process XML response appropriately |

|  |  |
| --- | --- |
|   | The default logon role of a client or user must have captive-portal enabled. |

**Configuring the XML API Server**

Configure an external XML API server in your AAA infrastructure. In this example, **10.11.12.13** is your server. The XML API interface on the controller will receive requests from this server.

|  |  |  |
| --- | --- | --- |
|  | ⚫ | Define the XML API server and specify the key for verifying requests from your server |

(host) (config) #aaa xml-api server 10.11.12.13

(host) (XML API Server "10.11.12.13") #key $abcd$1234$

|  |  |  |
| --- | --- | --- |
|  | ⚫ | Verify the XML API server configuration |

(host) (config) #show aaa xml-api server

XML API Server List

-------------------

Name References Profile Status

---- ---------- --------------

10.11.12.13 1 <====== Reference Count is incremented for each usage.

Total:1

**Associating the XML API Server to a AAA profile**

After you define the XML API server profile associate it to the appropriate AAA profile. If the XML API server is not correctly configured in the appropriate profile, the controller will respond with the client not authorized error message. You can add XML API server references to the following AAA profile depending on your requirement:

|  |  |  |
| --- | --- | --- |
|  | ⚫ | For wireless users—Associate the XML API server to the AAA profile of the virtual AP profile. |

(host) (config) #aaa profile wirelessusers

(host) (AAA Profile "wirelessusers") #xml-api-server 10.11.12.13

(host) (XML API Server "10.11.12.13") #key Aruba123

(host) (config) #show aaa profile wirelessusers

AAA Profile "wirelessusers"

---------------------------

Parameter Value

--------- -----

Initial role logon

MAC Authentication Profile N/A

MAC Authentication Default Role guest

MAC Authentication Server Group default

802.1X Authentication Profile N/A

802.1X Authentication Default Role guest

802.1X Authentication Server Group N/A

RADIUS Accounting Server Group N/A

XML API server 10.11.12.13

RFC 3576 server N/A

User derivation rules N/A

Wired to Wireless Roaming Enabled

SIP authentication role N/A

(host) (config) #wlan virtual-ap wireless-vap

(host) (Virtual AP profile "wireless-vap") #aaa-profile wirelessusers

(host) (config) #show wlan virtual-ap wireless-vap

Virtual AP profile "wireless-vap"

---------------------------------

Parameter Value

--------- -----

Virtual AP enable Enabled

Allowed band all

AAA Profile wirelessusers

802.11K Profile default

SSID Profile default

VLAN N/A

Forward mode tunnel

Deny time range N/A

Mobile IP Enabled

HA Discovery on-association Disabled

DoS Prevention Disabled

Station Blacklisting Enabled

Blacklist Time 3600 sec

Dynamic Multicast Optimization (DMO) Disabled

Dynamic Multicast Optimization (DMO) Threshold 6

Authentication Failure Blacklist Time 3600 sec

Multi Association Disabled

Strict Compliance Disabled

VLAN Mobility Disabled

Remote-AP Operation standard

Drop Broadcast and Multicast Disabled

Convert Broadcast ARP requests to unicast Disabled

Band Steering Disabled

WMM Traffic Management Profile N/A

|  |  |  |
| --- | --- | --- |
|  | ⚫ | For wired users—Associate the XML API server to the AAA profile of the appropriate wired profile. |

(host) (config) #aaa profile wiredusers

(host) (AAA Profile "wiredusers") #xml-api-server 10.11.12.13

(host) (AAA Profile "wiredusers") #!

(host) (config) #aaa authentication wired

(host) (Wired Authentication Profile) #profile wiredusers

(host) (Wired Authentication Profile) #show aaa authentication wired

Wired Authentication Profile

----------------------------

Parameter Value

--------- -----

AAA Profile wiredusers

|  |  |  |
| --- | --- | --- |
|  | ⚫ | Unknown wired users—Associate the XML API server to the default-xml-api AAA profile. |

|  |  |
| --- | --- |
|   | The default-xml-api AAA profile is used only to add or authenticate new users. |

The following example illustrates using the default-xml-api AAA profile.

(host) (config) #aaa profile default-xml-api

(host) (AAA Profile "default-xml-api") #xml-api-server 10.11.12.13

(host) (config) #show aaa profile default-xml-api

AAA Profile "default-xml-api" (Predefined (changed))

----------------------------------------------------

Parameter Value

--------- -----

Initial role logon

MAC Authentication Profile N/A

MAC Authentication Default Role guest

MAC Authentication Server Group default

802.1X Authentication Profile N/A

802.1X Authentication Default Role guest

802.1X Authentication Server Group N/A

RADIUS Accounting Server Group N/A

XML API server 10.11.12.13

RFC 3576 server N/A

User derivation rules N/A

Wired to Wireless Roaming Enabled

SIP authentication role N/A

Your controller is now ready to receive API calls from your XML API server.

**Set up Captive Portal profile**

Set up a Captive Portal profile with a login page that will redirect users to the external Captive Portal server.

(host) (config-role) #aaa authentication captive-portal captive-portal-auth

(host) (Captive Portal Authentication Profile "captive-portal-auth") #default-role authenticated

(host) (Captive Portal Authentication Profile "captive-portal-auth") #login-page https://10.11.12.13/cgi-bin/login.pl

(host) (Captive Portal Authentication Profile "captive-portal-auth") #switch-in-redirection-url

**Associating the Captive Portal Profile to an Initial Role**

(host) (Captive Portal Authentication Profile "captive-portal-auth") #user-role logon

(host) (config-role) #captive-portal captive-portal-auth

(host)(config-role) #session-acl captiveportal

You can either create a new ACL or append specific rules to an exisiting ACLs. To create session ACL for the logon role do the following:

(host) (config-role) #netdestination xCP *#an alias for the external Captive Portal server*

(host) (config-dest) #host 10.11.12.13 *#IP address of the external Captive Portal server*

(host) (config-dest) #ip access-list session captiveportal *#append or add rules to session ACL*

(host) (config-sess-captiveportal)#user alias xCP svc-https permit

(host) (config-sess-captiveportal)#user alias xCP svc-http permit

**Creating an XML API Request**

You can now create an XML request with an appropriate authentication command and send it to the controller via HTTPS post. The format of the URL to send the XML request is:

https://<controller-ip/auth/command.xml

|  |  |  |
| --- | --- | --- |
|  | ⚫ | controller-ip is the IP address of the controller that will receive the authentication request |

|  |  |  |
| --- | --- | --- |
|  | ⚫ | command.xml is the XML request that contains the details of authentication. |

The format of the XML API request is:

xml=<aruba command="<authentication\_command>">

 <options>Value</options>

 ...

 <options>Value</options>

</aruba>

You can specify any of the following commands in the XML request:

| **Table 1:***XML API Authentication Command* |
| --- |
| **Authentication Command** | **Description** |
| user\_add | This command adds the user to the controllers user table. |
| user\_delete | This command deletes the user from the controller |
| user\_authenticate | This command will authentication the user based on the authentication rules defined in the controllers configuration. |
| user\_blacklist | This command will block a user from connection to your network. |
| user\_query | This command will display the current status of the user connected to your network. |

The authentication command requires certain mandatory options to successfully execute the authentication tasks. The list of all available options are:

| **Table 2:***Authentication Command Options* |
| --- |
| **Options** | **Description** | **Range / Defaults** |
| ipaddr | IP address of the user in A.B.C.D format. | — |
| macaddr | MAC address of the user aa:bb:cc:dd:ee:ff format. | Enter MAC address with colon. |
| user | Name of the user. | 64 character string |
| role | Role name assigned after authenticating. | 64 character string |
| password | The password of the user used for authentication. | — |
| session\_timeout | Session time-out in seconds. User will be disconnected after this time. | — |
| authentication | Authentication method used to authenticate the message and the sender. You can use any of MD5, SHA-1 or clear text methods of authentication. This option is ignored if shared secret is not configured. It is, however, mandatory if it is configured. | — |
| key | This is the encoded SHA1/MD5 hash of shared secret or plaintext shared secret.This option is ignored if shared secret is not configured on the switch.The actual MD5/SHA-1 hash is 16/20 bytes and consists of binary data. It must be encoded as an ASCII based HEX string before sending. It must be present when the controller is configured with an xml-api key for the server. Encoded hash length is 32/40 bytes for MD5/SHA-1. |   |
| version  | The version of the XML API interface available in thecontroller. This field is mandatory is all requests. | Current version 1.0 |

**Monitoring External Captive Portal Usage Statistics**

To check the external captive portal authentication statistics use the show aaa xml-api statistics command. This command displays the number of times an authentication command was executed per client. The command also displays the number of times an authentication event occurred and the number of new authentication events that occurred since the last status check.

(host) # show aaa xml-api statistics

ECP Statistics

--------------

Statistics 10.10.10.249

---------- ----------

user\_authenticate 1 (0)

user\_add 1 (0)

user\_delete 1 (0)

user\_blacklist 2 (0)

unknown user 2 (0)

unknown role 0 (0)

unknown external agent 0 (0)

authentication failed 0 (0)

invalid command 0 (0)

invalid message authentication method 0 (0)

invalid message digest 0 (0)

Packets received from unknown clients : 0 (0)

Packets received with unknown request : 0 (0)

Requests Received/Success/Failed