AAA Service v2.2

Created Mar 27, 2024 at 07:03 PM

Resource: access_tokens

Access token handling

```
http://{device}/api/mgmt.aaa/2.2/token
```

JSON

```
{
}
```

Property Name	Type	Description	Notes
access_tokens	*<object>*	Access token handling	

Links

access_tokens: request

Request a new access token

```
POST http://{device}/api/mgmt.aaa/2.2/token
```

Request Body

Provide a request body with the following structure:

JSON

```
{
  "generate_refresh_token": boolean,
  "refresh_token": refresh_token_assertion,
  "state": string,
  "user_credentials": user_credentials_assertion
}
```

Property Name	Type	Description	Notes
access_tokens.links.request.request	*<object>*	Access token request details	
access_tokens.links.request.request.generate_refresh_token	*<boolean>*	If True, a refresh token will also be returned	Optional;
access_tokens.links.request.request.refresh_token	*<refresh_token_assertion>*	A refresh token assertion	
access_tokens.links.request.request.state	*<string>*	Optional opaque value to pass back with the token	Optional;
access_tokens.links.request.request.user_credentials	*<user_credentials_assertion>*	A username/password assertion	
access_tokens.links.request.request.oneOf[0]	*<object>*		Required properties: [user_credentials];
access_tokens.links.request.request.oneOf[0].<prop>	*<any>*		Optional;
access_tokens.links.request.request.oneOf[1]	*<object>*		Required properties: [refresh_token];
access_tokens.links.request.request.oneOf[1].generate_refresh_token	*<boolean>*		Optional; Values: False;
access_tokens.links.request.request.oneOf[1].<prop>	*<any>*		Optional;

Response Body

On success, the server returns a response body with the following structure:

JSON

```
{
  "access_token": string,
  "expires_at": integer,
  "refresh_token": string,
  "state": string,
  "token_type": string
}
```

Property Name	Type	Description	Notes
access_tokens.links.request.response	*<object>*	Granted access token details	Required properties: [access_token, expires_at, token_type];
access_tokens.links.request.response.access_token	*<string>*	The new access token	
access_tokens.links.request.response.expires_at	*<integer>*	The Unix epoch time when the access token will expire	
access_tokens.links.request.response.refresh_token	*<string>*	The new refresh token, if requested. This token must be stored securely.	Optional;
access_tokens.links.request.response.state	*<string>*	The value of the state field in the request, if present	Optional;
access_tokens.links.request.response.token_type	*<string>*	The type of token issued	Values: bearer;

Resource: account_policy

Global account settings

http://{device}/api/mgmt.aaa/2.2/account_policy

JSON

```
{
  "login_policy": {
    "count": integer,
    "wait_time": integer
  },
  "password_policy": {
    "change_frequency": integer,
    "dictionary_check": boolean,
    "difference": integer,
    "digits": integer,
    "expiration": {
      "inactive": {
        "enabled": boolean,
        "value": integer
      },
      "time": {
        "enabled": boolean,
        "value": integer
      },
      "warn": integer
    },
    "lower_case": integer,
    "minimum_length": integer,
    "permit_empty_passwords": boolean,
    "repeat": integer,
    "reuse_interval": integer,
    "symbols": integer,
    "upper_case": integer
  }
}
```

Property Name	Type	Description	Notes
account_policy	*<object>*	Global account settings	Required properties: [login_policy, password_policy];
account_policy.login_policy	*<object>*	Settings related to login attempts	Required properties: [count, wait_time];
account_policy.login_policy.count	*<integer>*	Maximum failed login attempts before temporary account lock. 0 disables this check.	Minimum 0;
account_policy.login_policy.wait_time	*<integer>*	Length in minutes for temporary account lock. N/A when count is 0.	Minimum 0;
account_policy.password_policy	*<object>*	Password complexity and expiration settings	Required properties: [permit_empty_passwords, minimum_length, lower_case, upper_case, digits, symbols, repeat, difference, dictionary_check, change_frequency, reuse_interval, expiration];
account_policy.password_policy.change_frequency	*<integer>*	Minimum number of days a user must wait between password changes. 0 disables this check.	Minimum 0;
account_policy.password_policy.dictionary_check	*<boolean>*	Disallow passwords based on common words	
account_policy.password_policy.difference	*<integer>*	Minimum number of character differences required between two passwords. 0 disables this check.	Minimum 0;

account_policy.password_policy.digits	*<integer>*	Minimum number of digits. 0 Disables this check.	Minimum 0;
account_policy.password_policy.expiration	*<object>*	Password expiration settings	Required properties: [time, inactive, warn];
account_policy.password_policy.expiration.inactive	*<object>*	Account inactivity settings	
account_policy.password_policy.expiration.inactive.enabled	*<boolean>*	Whether to mark accounts inactive if their password remains expired for a period of time	Optional;
account_policy.password_policy.expiration.inactive.value	*<integer>*	Number of days before an account with an expired password is marked inactive	Optional; Minimum 0;
account_policy.password_policy.expiration.time	*<object>*	Password expiration settings	
account_policy.password_policy.expiration.time.enabled	*<boolean>*	Whether to expire passwords after a period of time	Optional;
account_policy.password_policy.expiration.time.value	*<integer>*	Number of days before a password expires	Optional; Minimum 0;
account_policy.password_policy.expiration.warn	*<integer>*	Number of days before password expiration to start warning a user	Minimum 0;
account_policy.password_policy.lower_case	*<integer>*	Minimum number of lowercase characters. 0 disables this check.	Minimum 0;
account_policy.password_policy.minimum_length	*<integer>*	Minimum password length.	Range: 1 to 64;
account_policy.password_policy.permit_empty_passwords	*<boolean>*	Allow users to have empty passwords.	
account_policy.password_policy.repeat	*<integer>*	Maximum times the same character can repeat consecutively. 0 disables this check.	Minimum 0;
account_policy.password_policy.reuse_interval	*<integer>*	Number of previous passwords to save. When setting a new password, the user cannot use a password that exists in their password history. 0 disables this check.	Range: 0 to 10;
account_policy.password_policy.symbols	*<integer>*	Minimum number of symbols. 0 disables this check.	Minimum 0;
account_policy.password_policy.upper_case	*<integer>*	Minimum number of uppercase characters. 0 disables this check.	Minimum 0;

Links

account_policy: get

```
GET http://{device}/api/mgmt.aaa/2.2/account_policy
```

Response Body

Returns an account_policy data object.

account_policy: set

```
PUT http://{device}/api/mgmt.aaa/2.2/account_policy
```

Request Body

Provide an account_policy data object.

Response Body

Returns an account_policy data object.

Resource: known_user

A remotely authenticated user known to the system

```
http://{device}/api/mgmt.aaa/2.2/known_users/items/{name}
```

JSON

```
{
  "cached_roles": [
    integer
  ],
  "last_auth_method": string,
  "last_auth_time": integer,
  "name": string
}
```

Property Name	Type	Description	Notes
known_user	*<object>*	A remotely authenticated user known to the system	Required properties: [name, last_auth_time, last_auth_method, cached_roles];
*known_user.*cached_roles	*<array of <integer>>*	The roles last granted to this user	
*known_user.*cached_roles[items]	*<integer>*	The id of a cached role	
*known_user.*last_auth_method	*<string>*	Last authentication method used for user.	
*known_user.*last_auth_time	*<integer>*	Unix epoch time the user was last authenticated.	
*known_user.*name	*<string>*	Name of the user	

Links

known_user: delete

```
DELETE http://{device}/api/mgmt.aaa/2.2/known_users/items/{name}
```

Response Body

On success, the server does not provide any body in the responses.

known_user: get

```
GET http://{device}/api/mgmt.aaa/2.2/known_users/items/{name}
```

Response Body

Returns a known_user data object.

Resource: known_users

All remotely authenticated users known to the system

```
http://{device}/api/mgmt.aaa/2.2/known_users
```

JSON

```
{
  "enable": boolean,
  "items": [ known_user ]
}
```

Property Name	Type	Description	Notes
known_users	*<object>*	All remotely authenticated users known to the system	Required properties: [enable];
*known_users.*enable	*<boolean>*	Whether the known_user cache is enabled or not. When disabled, all users will be removed from the cache and no new users will be added.	
*known_users.*items	*<array of <known_user>>*	All known_user instances	Read-only; Optional;
*known_users.*items[items]	*<known_user>*	A remotely authenticated user known to the system	

Links

known_users: get

```
GET http://{device}/api/mgmt.aaa/2.2/known_users
```

Response Body

Returns a known_users data object.

known_users: set

PUT http://{device}/api/mgmt.aaa/2.2/known_users

Request Body

Provide a known_users data object.

Response Body

Returns a known_users data object.

Resource: passwords

Local user password management

http://{device}/api/mgmt.aaa/2.2/passwords

JSON

```
{
}
```

Property Name	Type	Description	Notes
passwords	*<object>*	Local user password management	

Links

passwords: change_password

Change a local user's password. Old password is required when changing your own password.

POST http://{device}/api/mgmt.aaa/2.2/users/change_password

Request Body

Provide a request body with the following structure:

JSON

```
{
  "new_password": string,
  "old_password": string,
  "user": string
}
```

Property Name	Type	Description	Notes
*passwords.*links.change_password.request	*<object>*		Required properties: [user, new_password];
*passwords.*links.change_password.request.new_password	*<string>*	New password, in plaintext	
*passwords.*links.change_password.request.old_password	*<string>*	Old password, in plaintext	Optional;
*passwords.*links.change_password.request.user	*<string>*	User account to change password	

Response Body

On success, the server returns a response body with the following structure:

JSON

```
{
  "changed": boolean,
  "user": string
}
```

Property Name	Type	Description	Notes
passwords.links.change_password.response	*<object>*		Required properties: [user, changed];
passwords.links.change_password.response.changed	*<boolean>*	Whether the password was successfully changed	
passwords.links.change_password.response.user	*<string>*	User account	

Resource: permission_group

Service resource group used to assign permissions

```
http://{device}/api/mgmt.aaa/2.2/permission_groups/{name}
```

JSON

```
{
  "description": string,
  "name": string,
  "pretty_name": string,
  "resources": [ service_resource ]
}
```

Property Name	Type	Description	Notes
permission_group	*<object>*	Service resource group used to assign permissions	Required properties: [name, pretty_name, description, resources];
permission_group.description	*<string>*	Brief description of group	
permission_group.name	*<string>*	Unique ID for group	Read-only; Pattern: '[a-zA-Z0-9_]+$';
permission_group.pretty_name	*<string>*	Display name for group	
permission_group.resources	*<array of <service_resource>>*	List of resources that exist in this group	
permission_group.resources[items]	*<service_resource>*	Resources available from a service. If only the service_name property is present, all resources are included.	

Links

permission_group: get

```
GET http://{device}/api/mgmt.aaa/2.2/permission_groups/{name}
```

Response Body

Returns a permission_group data object.

Relations

permission_group: instances

Related resource

permission_groups

Resource: permission_groups

Collection of service resource groups

```
http://{device}/api/mgmt.aaa/2.2/permission_groups
```

JSON

```
{
  "items": [ permission_group ]
}
```

Property Name	Type	Description	Notes
permission_groups	*<object>*	Collection of service resource groups	Required properties: [items];
permission_groups.items	*<array of <permission_group>>*	List of service resource groups	
permission_groups.items[items]	*<permission_group>*	Service resource group used to assign permissions	

Links

permission_groups: get

```
GET http://{device}/api/mgmt.aaa/2.2/permission_groups
```

Response Body

Returns a permission_groups data object.

Resource: radius_server

A RADIUS authentication server

```
http://{device}/api/mgmt.aaa/2.2/radius_servers/items/{id}
```

JSON

```
{
  "enabled": boolean,
  "host": string,
  "id": integer,
  "new_key": string,
  "port": integer,
  "timeout": integer
}
```

Property Name	Type	Description	Notes
radius_server	*<object>*	A RADIUS authentication server	Required properties: [host, port, timeout];
radius_server.enabled	*<boolean>*	Whether this RADIUS server is enabled or not. A server is enabled when it is in the server_order list in the radius_servers resource.	Read-only; Optional;
radius_server.host	*<string>*	The hostname or IP address of the RADIUS server	
radius_server.id	*<integer>*	Server ID	Read-only; Optional;
radius_server.new_key	*<string>*	The secret key used to encrypt communications. An empty string indicates no encryption is used.	Optional;
radius_server.port	*<integer>*	The port of the RADIUS server	Range: 1 to 65535; Default is 1812;
radius_server.timeout	*<integer>*	Max time, in seconds, to wait for the server to respond to an auth request.	Range: 1 to 30;

Links

radius_server: delete

```
DELETE http://{device}/api/mgmt.aaa/2.2/radius_servers/items/{id}
```

Response Body

On success, the server does not provide any body in the responses.

radius_server: get

```
GET http://{device}/api/mgmt.aaa/2.2/radius_servers/items/{id}
```

Response Body
Returns a radius_server data object.

radius_server: set

PUT http://{device}/api/mgmt.aaa/2.2/radius_servers/items/{id}

Request Body
Provide a radius_server data object.

Response Body
Returns a radius_server data object.

Resource: radius_servers

The configured RADIUS servers

http://{device}/api/mgmt.aaa/2.2/radius_servers

JSON

```
{
  "available_encryption": [
    string
  ],
  "encryption_protocol": string,
  "server_priority": [
    integer
  ],
  "servers": [ radius_server ]
}
```

Property Name	Type	Description	Notes
radius_servers	*<object>*	The configured RADIUS servers	Required properties: [server_priority, encryption_protocol];
radius_servers.available_encryption	*<array of <string>>*	Available encryption protocols	Read-only; Optional;
radius_servers.available_encryption [items]	*<string>*		Read-only;
radius_servers.encryption_protocol	*<string>*	The encryption protocol to use. Available protocols are listed under available_encryption.	
radius_servers.server_priority	*<array of <integer>>*	The order in which authentication requests are made to the configured servers. Servers not in this list will be disabled.	
radius_servers.server_priority[items]	*<integer>*		
radius_servers.servers	*<array of <radius_server>>*	The configured RADIUS servers	Read-only; Optional;
radius_servers.servers[items]	*<radius_server>*	A RADIUS authentication server	

Links

radius_servers: create

POST http://{device}/api/mgmt.aaa/2.2/radius_servers

Request Body
Provide a radius_server data object.

Response Body
Returns a radius_server data object.

radius_servers: get

GET http://{device}/api/mgmt.aaa/2.2/radius_servers

Response Body

Returns a radius_servers data object.

radius_servers: set

```
PUT http://{device}/api/mgmt.aaa/2.2/radius_servers
```

Request Body

Provide a radius_servers data object.

Response Body

Returns a radius_servers data object.

Resource: refresh_tokens

Active refresh tokens. Only the first few characters of the token are revealed, enough for the caller to differentiate the tokens they own.

```
http://{device}/api/mgmt.aaa/2.2/refresh_tokens
```

JSON

```
{
  "items": [
    {
      "issued_at": any,
      "last_redeemed": integer,
      "partial_token": string,
      "times_redeemed": integer,
      "user": string
    }
  ]
}
```

Property Name	Type	Description	Notes
refresh_tokens	*<object>*	Active refresh tokens. Only the first few characters of the token are revealed, enough for the caller to differentiate the tokens they own.	Required properties: [items];
refresh_tokens.items	*<array of <object>>*		
refresh_tokens.items[items]	*<object>*	A single refresh token	Required properties: [user, partial_token, issued_at, last_redeemed, times_redeemed];
refresh_tokens.items[items].issued_at	*<any>*	The Unix epoch time that the refresh token was issued	
refresh_tokens.items[items].last_redeemed	*<integer>*	The Unix epoch time that the token was last redeemed. 0 if it has never been used.	Minimum 0;
refresh_tokens.items[items].partial_token	*<string>*	The first few characters of the token	
refresh_tokens.items[items].times_redeemed	*<integer>*	The number of times the token has been redeemed	Minimum 0;
refresh_tokens.items[items].user	*<string>*	The user name which owns this token	

Links

refresh_tokens: get

```
GET http://{device}/api/mgmt.aaa/2.2/refresh_tokens
```

Response Body

Returns a refresh_tokens data object.

refresh_tokens: revoke

Revoke a refresh token

POST http://{device}/api/mgmt.aaa/2.2/refresh_tokens/revoke

Request Body

Provide a request body with the following structure:

JSON

```
{
  "refresh_token": string
}
```

Property Name	Type	Description	Notes
*refresh_tokens.*links.revoke.request	*<object>*		Required properties: [refresh_token];
*refresh_tokens.*links.revoke.request.refresh_token	*<string>*	The refresh token to revoke	

Response Body

On success, the server does not provide any body in the responses.

Resource: remote_authentication

Remote authentication settings

http://{device}/api/mgmt.aaa/2.2/remote_authentication

JSON

```
{
  "auth_methods_available": [
    string
  ],
  "auth_sequence": [
    string
  ],
  "default_roles": [
    integer
  ],
  "next_method_on_reject": boolean
}
```

Property Name	Type	Description	Notes
remote_authentication	*<object>*	Remote authentication settings	Required properties: [auth_sequence, next_method_on_reject, default_roles];
*remote_authentication.*auth_methods_available	*<array of <string>>*	Available authentication methods	Read-only; Optional;
*remote_authentication.*auth_methods_available[items]	*<string>*		Read-only;
*remote_authentication.*auth_sequence	*<array of <string>>*	Authentication methods to use, in priority order of first to last. Possible values are listed in auth_methods_available.	
*remote_authentication.*auth_sequence[items]	*<string>*		
*remote_authentication.*default_roles	*<array of <integer>>*	The roles to assign to a remotely-authenticated user when the authentication server does not specify any.	
*remote_authentication.*default_roles[items]	*<integer>*		
*remote_authentication.*next_method_on_reject	*<boolean>*	If True, when a login is rejected, the system will still attempt to authenticate via the next method in auth_sequence. If False, the login attempt is denied immediately when any auth method rejects the user credentials.	

Links

remote_authentication: get

GET http://{device}/api/mgmt.aaa/2.2/remote_authentication

Response Body
Returns a remote_authentication data object.

remote_authentication: set

PUT http://{device}/api/mgmt.aaa/2.2/remote_authentication

Request Body
Provide a remote_authentication data object.

Response Body
Returns a remote_authentication data object.

Resource: role

A set of permissions that may be assigned to a user

http://{device}/api/mgmt.aaa/2.2/roles/{id}

JSON

```
{
  "description": string,
  "id": integer,
  "member_of": [
    integer
  ],
  "permissions": [
    {
      "operation": string,
      "permission_group": string
    }
  ],
  "pretty_name": string,
  "system_default": boolean
}
```

Property Name	Type	Description	Notes
role	*<object>*	A set of permissions that may be assigned to a user	Required properties: [pretty_name];
*role.*description	*<string>*	Role description	Optional;
*role.*id	*<integer>*	Unique role identifier	Read-only; Optional;
*role.*member_of	*<array of <integer>>*	Roles that this role is a member of	Optional;
*role.*member_of[items]	*<integer>*	A role identifier	
*role.*permissions	*<array of <object>>*	A set of permissions granted to this role	Optional;
*role.*permissions[items]	*<object>*	One permission group and the access rights granted to it	
*role.*permissions[items].operation	*<string>*	The access rights granted to the permission group	Optional; Values: read_only, read_write;
*role.*permissions[items].permission_group	*<string>*	The permission group	Optional;
*role.*pretty_name	*<string>*	Unique role name	
*role.*system_default	*<boolean>*	If true, role is a system default entry that cannot be modified	Read-only; Optional;

Links

role: delete

DELETE http://{device}/api/mgmt.aaa/2.2/roles/{id}

Response Body
On success, the server does not provide any body in the responses.

role: get

GET http://{device}/api/mgmt.aaa/2.2/roles/{id}

Response Body

Returns a role data object.

role: set

PUT http://{device}/api/mgmt.aaa/2.2/roles/{id}

Request Body

Provide a role data object.

Response Body

Returns a role data object.

Resource: role_names

The list of roles and their names

http://{device}/api/mgmt.aaa/2.2/role_names

JSON


```
{
  "items": [
    {
      "description": string,
      "id": integer,
      "pretty_name": string
    }
  ]
}
```


Property Name	Type	Description	Notes
role_names	*<object>*	The list of roles and their names	Required properties: [items];
role_names.items	*<array of <object>>*		
role_names.items[items]	*<object>*	Name and description for a single role	Required properties: [id, pretty_name, description];
role_names.items[items].description	*<string>*	Role description	
role_names.items[items].id	*<integer>*	Unique role identifier	
role_names.items[items].pretty_name	*<string>*	Unique role name	

Links

role_names: get

GET http://{device}/api/mgmt.aaa/2.2/role_names

Response Body

Returns a role_names data object.

Resource: roles

All configured roles

http://{device}/api/mgmt.aaa/2.2/roles

JSON


```
{
  "items": [ role ]
}
```

Property Name	Type	Description	Notes
roles	*<object>*	All configured roles	
roles.items	*<array of <role>>*	A role identifier	Optional;
roles.items[items]	*<role>*	A set of permissions that may be assigned to a user	

Links

roles: create

POST http://{device}/api/mgmt.aaa/2.2/roles

Request Body

Provide a role data object.

Response Body

Returns a role data object.

roles: get

GET http://{device}/api/mgmt.aaa/2.2/roles

Response Body

Returns a roles data object.

Resource: tacacs_server

A TACACS+ authentication server

http://{device}/api/mgmt.aaa/2.2/tacacs_servers/items/{id}

JSON

```
{
  "enabled": boolean,
  "host": string,
  "id": integer,
  "new_key": string,
  "port": integer
}
```

Property Name	Type	Description	Notes
tacacs_server	*<object>*	A TACACS+ authentication server	Required properties: [host, port];
tacacs_server.enabled	*<boolean>*	Whether this TACACS+ server is enabled or not. A server is enabled when it is in the server_order list in the tacacs_servers resource.	Read-only; Optional;
tacacs_server.host	*<string>*	The hostname or IP address of the TACACS+ server	
tacacs_server.id	*<integer>*	Server ID	Read-only; Optional;
tacacs_server.new_key	*<string>*	The secret key used to encrypt communications. An empty string indicates no encryption is used.	Optional;
tacacs_server.port	*<integer>*	The post of the TACACS+ server	Range: 1 to 65535; Default is 49;

Links

tacacs_server: delete

DELETE http://{device}/api/mgmt.aaa/2.2/tacacs_servers/items/{id}

Response Body

On success, the server does not provide any body in the responses.

tacacs_server: get

GET http://{device}/api/mgmt.aaa/2.2/tacacs_servers/items/{id}

Response Body

Returns a tacacs_server data object.

tacacs_server: set

PUT http://{device}/api/mgmt.aaa/2.2/tacacs_servers/items/{id}

Request Body

Provide a tacacs_server data object.

Response Body

Returns a tacacs_server data object.

Resource: tacacs_servers

The configured TACACS+ servers

http://{device}/api/mgmt.aaa/2.2/tacacs_servers

JSON

```
{
  "server_priority": [
    integer
  ],
  "servers": [ tacacs_server ],
  "timeout": integer
}
```

Property Name	Type	Description	Notes
tacacs_servers	*<object>*	The configured TACACS+ servers	Required properties: [server_priority, timeout];
*tacacs_servers.*server_priority	*<array of <integer>>*	The order in which authentication requests are made to the configured servers. Servers not in this list will be disabled.	
*tacacs_servers.*server_priority[items]	*<integer>*		
*tacacs_servers.*servers	*<array of <tacacs_server>>*	The configured TACACS+ servers	Read-only; Optional;
*tacacs_servers.*servers[items]	*<tacacs_server>*	A TACACS+ authentication server	
*tacacs_servers.*timeout	*<integer>*	Max time, in seconds, to wait for a server to respond to an auth request.	Range: 1 to 30;

Links

tacacs_servers: create

POST http://{device}/api/mgmt.aaa/2.2/tacacs_servers

Request Body

Provide a tacacs_server data object.

Response Body

Returns a tacacs_server data object.

tacacs_servers: get

GET http://{device}/api/mgmt.aaa/2.2/tacacs_servers

Response Body

Returns a tacacs_servers data object.

tacacs_servers: set

PUT http://{device}/api/mgmt.aaa/2.2/tacacs_servers

Request Body

Provide a tacacs_servers data object.

Response Body

Returns a tacacs_servers data object.

Resource: user

A user configured for local authentication

http://{device}/api/mgmt.aaa/2.2/users/{name}

JSON

```
{
  "account_never_inactive": boolean,
  "description": string,
  "enable": boolean,
  "logged_in": boolean,
  "login_failure": {
    "count": integer,
    "date": timestamp,
    "source": string
  },
  "name": string,
  "new_password": {
    "cleartext": string,
    "hashed": string
  },
  "password": {
    "change_allowed_in": integer,
    "expires_on": timestamp,
    "locks_on": timestamp
  },
  "password_never_expires": boolean,
  "roles": [
    integer
  ],
  "status": string
}
```

Property Name	Type	Description	Notes
user	*<object>*	A user configured for local authentication	Required properties: [name];
user.account_never_inactive	*<boolean>*	User account will never become inactive, preventing login, due to an expired password	Optional; Default is False;
user.description	*<string>*	Description for the user account	Optional; Default is ;
user.enable	*<boolean>*	Whether the user is allowed to log in	Optional; Default is False;
user.logged_in	*<boolean>*	User is currently logged in	Read-only; Optional;
user.login_failure	*<object>*	Login failure information	Read-only; Optional;
user.login_failure.count	*<integer>*	Number of failed login attempts	Read-only; Optional;
user.login_failure.date	*<timestamp>*	Date, in Unix epoch time, of the most recent login failure	Read-only; Optional; Seconds since January 1, 1970;
user.login_failure.source	*<string>*	Address of the most recent login failure	Read-only; Optional;
user.name	*<string>*	Account name	
user.new_password	*<object>*	Set this user's password to a new value. Used for creation and bulk importing of users. Normal password changes should go through the password resource. Changing passwords using this API may result in passwords which violate the password policy.	Optional;
user.new_password.cleartext	*<string>*	Set the user's password in plain text	Optional;
user.new_password.hashed	*<string>*	Set the user's password as a hash	Optional;
user.new_password.oneOf[0]	*<object>*		Required properties: [cleartext];

user.new_password.oneOf[0].<prop>	*<any>*		Optional;
user.new_password.oneOf[1]	*<object>*		Required properties: [hashed];
user.new_password.oneOf[1].<prop>	*<any>*		Optional;
user.password	*<object>*	Password settings	Required properties: [expires_on, locks_on, change_allowed_in]; Optional;
user.password.change_allowed_in	*<integer>*	Days remaining until the user can change their password. A value of 0 indicates the password may be changed immediately.	Read-only;
user.password.expires_on	*<timestamp>*	Date, in Unix epoch time, after which the user's password will expire. If 0, the password will never expire.	Read-only; Seconds since January 1, 1970;
user.password.locks_on	*<timestamp>*	Date, in Unix epoch time, after which the user account will be locked due to an expired password. If 0, the account will never be locked.	Read-only; Seconds since January 1, 1970;
user.password_never_expires	*<boolean>*	User account password will never expire	Optional; Default is False;
user.roles	*<array of <integer>>*	List of roles granted to this user	Optional;
user.roles[items]	*<integer>*	The role identifier	
user.status	*<string>*	Status of the account	Read-only; Optional; Values: active, inactive, disabled, login_failure_lockout;

Links

user: delete

```
DELETE http://{device}/api/mgmt.aaa/2.2/users/{name}
```

Response Body

On success, the server does not provide any body in the responses.

user: get

```
GET http://{device}/api/mgmt.aaa/2.2/users/{name}
```

Response Body

Returns an user data object.

user: set

```
PUT http://{device}/api/mgmt.aaa/2.2/users/{name}
```

Request Body

Provide an user data object.

Response Body

Returns an user data object.

Resource: users

The users configured for local authentication

```
http://{device}/api/mgmt.aaa/2.2/users
```

JSON

```
{
  "items": [ user ]
}
```

Property Name	Type	Description	Notes
users	*<object>*	The users configured for local authentication	
users.items	*<array of <user>>*		Optional;

users.items[items]	*<user>*	A user configured for local authentication	

Links

users: create

POST http://{device}/api/mgmt.aaa/2.2/users

Request Body
Provide an user data object.

Response Body
Returns an user data object.

users: get

GET http://{device}/api/mgmt.aaa/2.2/users

Response Body
Returns an users data object.

Type: refresh_token_assertion

A refresh token assertion

JSON

string

Property Name	Type	Description	Notes
refresh_token_assertion	*<string>*	A refresh token assertion	

Type: service_resource

Resources available from a service. If only the service_name property is present, all resources are included.

JSON

```
{
  "all_except": [
    string
  ],
  "only_include": [
    string
  ],
  "service_name": string
}
```

Property Name	Type	Description	Notes
service_resource	*<object>*	Resources available from a service. If only the service_name property is present, all resources are included.	Required properties: [service_name];
service_resource.all_except	*<array of <string>>*	List of resources excluded from this group. All other resources from this service are included.	Optional;
service_resource.all_except[items]	*<string>*		
service_resource.only_include	*<array of <string>>*	List of resources included in this group. All other resources from this service are excluded.	Optional;
service_resource.only_include[items]	*<string>*		
service_resource.service_name	*<string>*	Name of the service	Read-only;
service_resource.not	*<object>*		Required properties: [all_except, only_include];

service_resource.not.<prop>	*<any>*		Optional;

Type: user_credentials_assertion

A username/password assertion

JSON

```
{
  "password": string,
  "username": string
}
```

Property Name	Type	Description	Notes
user_credentials_assertion	*<object>*	A username/password assertion	Required properties: [username, password];
user_credentials_assertion.password	*<string>*	Password	
user_credentials_assertion.username	*<string>*	Username	