

# Aaa Profile

## Endpoints Summary

Method	Path	Swagger
GET	<a href="#">/aaa_profile/</a>	<a href="#">Swagger ↗</a>
POST	<a href="#">/aaa_profile/</a>	<a href="#">Swagger ↗</a>
GET	<a href="#">/aaa_profile/{id}/</a>	<a href="#">Swagger ↗</a>
PUT	<a href="#">/aaa_profile/{id}/</a>	<a href="#">Swagger ↗</a>
PATCH	<a href="#">/aaa_profile/{id}/</a>	<a href="#">Swagger ↗</a>
DELETE	<a href="#">/aaa_profile/{id}/</a>	<a href="#">Swagger ↗</a>

“ The AAA Profile API enables management of Authentication, Authorization, and Accounting profiles used for network access control. These endpoints allow you to create, configure, and manage RADIUS attribute profiles that define user authentication parameters and access policies. Common use cases include setting up user access levels, configuring network device authentication, and managing RADIUS reply and check attributes for network security.

**Base URL:** <https://gate.zequenze.com/api/v1>

**Authentication:** All endpoints require a Bearer token:

```
Authorization: Bearer <your-api-token>
```

## Overview

The AAA Profile API provides comprehensive management of Authentication, Authorization, and Accounting profiles within the GATE platform. AAA profiles define sets of RADIUS attributes that control network access authentication and authorization policies.

## Key Concepts:

- **AAA Profiles:** Named collections of RADIUS attributes that define authentication and authorization rules
- **Reply Attributes:** RADIUS attributes sent back to the authenticating device after successful authentication
- **Check Attributes:** RADIUS attributes used to validate authentication requests before granting access
- **Attribute Operators:** Define how attributes are processed (assignment, comparison, addition, etc.)

## Common Scenarios:

- Setting up different access levels for various user groups (admin, user, guest)
- Configuring VLAN assignments based on user authentication
- Managing bandwidth limitations and session timeouts
- Implementing role-based access control for network resources
- Creating standardized authentication profiles for network devices

The API follows REST principles with full CRUD operations, supporting both complete updates (PUT) and partial modifications (PATCH) for flexible profile management.

---

# Endpoints

## GET /aaa\_profile/

**Description:** Retrieves a paginated list of all AAA profiles in your organization. This endpoint is essential for viewing existing authentication profiles, discovering available configurations, and implementing profile selection interfaces.

### Use Cases:

- Displaying available authentication profiles in management dashboards
- Implementing profile selection dropdowns in user interfaces
- Auditing existing authentication configurations
- Synchronizing profiles with external systems

### Full URL Example:

```
https://gate.zequenze.com/api/v1/aaa_profile/?limit=25&offset=0
```

### Parameters:

Parameter	Type	In	Required	Description
limit	integer	query	No	Number of results to return per page (default: 20, max: 100)
offset	integer	query	No	The initial index from which to return results for pagination

### cURL Example:

```
curl -X GET "https://gate.zequenze.com/api/v1/aaa_profile/?limit=10&offset=0" \
-H "Authorization: Bearer YOUR_API_TOKEN" \
-H "Content-Type: application/json"
```

### Example Response:

```
{
  "count": 15,
  "next": "https://gate.zequenze.com/api/v1/aaa_profile/?limit=10&offset=10",
  "previous": null,
  "results": [
    {
      "id": 1,
      "name": "Admin Access Profile",
      "short_name": "admin-access",
      "description": "Full administrative access with elevated privileges",
      "organization_id": "org_12345",
      "reply_attribute": [
        {
          "attribute": "Framed-IP-Address",
          "op": "=",
          "value": "192.168.1.100"
        }
      ],
      "check_attribute": [
        {
          "attribute": "User-Name",
          "op": "!=",
          "value": "guest"
        }
      ]
    }
  ]
}
```

```
    ]
  },
  {
    "id": 2,
    "name": "Guest Network Profile",
    "short_name": "guest-network",
    "description": "Limited access profile for guest users",
    "organization_id": "org_12345",
    "reply_attribute": [
      {
        "attribute": "Tunnel-Type",
        "op": ":",
        "value": "VLAN"
      }
    ],
    "check_attribute": []
  }
]
```

### Response Codes:

Status	Description
200	Success - Returns paginated list of AAA profiles
401	Unauthorized - Invalid or missing API token
403	Forbidden - Insufficient permissions
500	Internal Server Error - Server processing error

## POST /aaa\_profile/

**Description:** Creates a new AAA profile with specified RADIUS attributes and configuration settings. This endpoint enables you to programmatically define new authentication and authorization policies for your network infrastructure.

### Use Cases:

- Automating AAA profile creation during network onboarding
- Creating standardized profiles for different user roles
- Implementing dynamic profile generation based on organizational requirements

- Bulk creation of profiles for multi-tenant environments

### Full URL Example:

```
https://gate.zequenze.com/api/v1/aaa_profile/
```

### cURL Example:

```
curl -X POST "https://gate.zequenze.com/api/v1/aaa_profile/" \  
-H "Authorization: Bearer YOUR_API_TOKEN" \  
-H "Content-Type: application/json" \  
-d '{  
  "name": "Developer Access Profile",  
  "short_name": "dev-access",  
  "description": "Development team access with limited administrative rights",  
  "reply_attribute": [  
    {  
      "attribute": "Tunnel-Type",  
      "op": ":",  
      "value": "VLAN"  
    },  
    {  
      "attribute": "Tunnel-Medium-Type",  
      "op": ":",  
      "value": "IEEE-802"  
    }  
  ],  
  "check_attribute": [  
    {  
      "attribute": "NAS-Port-Type",  
      "op": "=",  
      "value": "Ethernet"  
    }  
  ]  
}'
```

### Request Body Example:

```
{  
  "name": "Developer Access Profile",  
  "short_name": "dev-access",
```

```

"description": "Development team access with limited administrative rights",
"reply_attribute": [
  {
    "attribute": "Tunnel-Type",
    "op": ":",
    "value": "VLAN"
  },
  {
    "attribute": "Tunnel-Medium-Type",
    "op": ":",
    "value": "IEEE-802"
  },
  {
    "attribute": "Session-Timeout",
    "op": "=",
    "value": "3600"
  }
],
"check_attribute": [
  {
    "attribute": "NAS-Port-Type",
    "op": "==",
    "value": "Ethernet"
  },
  {
    "attribute": "Calling-Station-Id",
    "op": "=*",
    "value": "^[0-9A-Fa-f]{2}[:-]){5}([0-9A-Fa-f]{2})$"
  }
]
}

```

### Example Response:

```

{
  "id": 25,
  "name": "Developer Access Profile",
  "short_name": "dev-access",
  "description": "Development team access with limited administrative rights",
  "organization_id": "org_12345",

```

```

"reply_attribute": [
  {
    "attribute": "Tunnel-Type",
    "op": ":",
    "value": "VLAN"
  },
  {
    "attribute": "Tunnel-Medium-Type",
    "op": ":",
    "value": "IEEE-802"
  },
  {
    "attribute": "Session-Timeout",
    "op": "=",
    "value": "3600"
  }
],
"check_attribute": [
  {
    "attribute": "NAS-Port-Type",
    "op": "==",
    "value": "Ethernet"
  },
  {
    "attribute": "Calling-Station-Id",
    "op": "=*",
    "value": "^[0-9A-Fa-f]{2}[:-]){5}([0-9A-Fa-f]{2})$"
  }
]
}

```

## Response Codes:

Status	Description
201	Created - AAA profile successfully created
400	Bad Request - Invalid data format or missing required fields
401	Unauthorized - Invalid or missing API token
403	Forbidden - Insufficient permissions

Status	Description
409	Conflict - Profile with same short_name already exists

## GET /aaa\_profile/{id}/

**Description:** Retrieves detailed information about a specific AAA profile by its unique identifier. This endpoint provides complete profile configuration including all RADIUS attributes, operators, and values.

### Use Cases:

- Viewing complete profile configuration for auditing purposes
- Retrieving profile details for editing or cloning operations
- Validating profile settings before applying to network devices
- Debugging authentication issues by examining profile attributes

### Full URL Example:

```
https://gate.zequenze.com/api/v1/aaa_profile/15/
```

### cURL Example:

```
curl -X GET "https://gate.zequenze.com/api/v1/aaa_profile/15/" \  
-H "Authorization: Bearer YOUR_API_TOKEN" \  
-H "Content-Type: application/json"
```

### Example Response:

```
{  
  "id": 15,  
  "name": "Network Administrator Profile",  
  "short_name": "network-admin",  
  "description": "Full network administrative access with monitoring capabilities",  
  "organization_id": "org_12345",  
  "reply_attribute": [  
    {  
      "attribute": "Service-Type",  
      "op": "=",  
      "value": "Administrative-User"  
    },  
  ],  
}
```

```

{
  "attribute": "Framed-Protocol",
  "op": ":",
  "value": "PPP"
},
{
  "attribute": "Idle-Timeout",
  "op": "=",
  "value": "1800"
}
],
"check_attribute": [
  {
    "attribute": "User-Password",
    "op": "!=",
    "value": ""
  },
  {
    "attribute": "NAS-IP-Address",
    "op": "==",
    "value": "192.168.100.1"
  }
]
}

```

### Response Codes:

Status	Description
200	Success - Returns the requested AAA profile
401	Unauthorized - Invalid or missing API token
403	Forbidden - Insufficient permissions to view this profile
404	Not Found - AAA profile with specified ID does not exist

## PUT /aaa\_profile/{id}/

**Description:** Completely updates an existing AAA profile, replacing all current configuration with the provided data. This operation requires all required fields and overwrites the entire profile configuration.

## Use Cases:

- Implementing major profile reconfiguration
- Standardizing profiles across multiple environments
- Applying template-based profile updates
- Migrating profile configurations between systems

## Full URL Example:

```
https://gate.zequenze.com/api/v1/aaa_profile/15/
```

## cURL Example:

```
curl -X PUT "https://gate.zequenze.com/api/v1/aaa_profile/15/" \  
-H "Authorization: Bearer YOUR_API_TOKEN" \  
-H "Content-Type: application/json" \  
-d '{  
  "name": "Updated Network Admin Profile",  
  "short_name": "network-admin",  
  "description": "Enhanced network administrative access with additional security",  
  "reply_attribute": [  
    {  
      "attribute": "Service-Type",  
      "op": "=",  
      "value": "Administrative-User"  
    },  
    {  
      "attribute": "Session-Timeout",  
      "op": "=",  
      "value": "7200"  
    }  
  ],  
  "check_attribute": [  
    {  
      "attribute": "User-Password",  
      "op": "!=",  
      "value": ""  
    },  
    {  
      "attribute": "Calling-Station-Id",  
      "op": "=*",
```

```
        "value": "^00:11:22"
      }
    ]
  }'
```

### Request Body Example:

```
{
  "name": "Updated Network Admin Profile",
  "short_name": "network-admin",
  "description": "Enhanced network administrative access with additional security",
  "reply_attribute": [
    {
      "attribute": "Service-Type",
      "op": "=",
      "value": "Administrative-User"
    },
    {
      "attribute": "Session-Timeout",
      "op": "=",
      "value": "7200"
    },
    {
      "attribute": "Framed-MTU",
      "op": ":=",
      "value": "1500"
    }
  ],
  "check_attribute": [
    {
      "attribute": "User-Password",
      "op": "!=",
      "value": ""
    },
    {
      "attribute": "Calling-Station-Id",
      "op": "=*",
      "value": "^00:11:22"
    },
    {

```

```
    "attribute": "NAS-Port-Type",
    "op": "==",
    "value": "Ethernet"
  }
]
```

### Response Codes:

Status	Description
200	Success - Profile successfully updated
400	Bad Request - Invalid data format or missing required fields
401	Unauthorized - Invalid or missing API token
403	Forbidden - Insufficient permissions to modify this profile
404	Not Found - AAA profile with specified ID does not exist

## PATCH /aaa\_profile/{id}/

**Description:** Partially updates an existing AAA profile, modifying only the specified fields while preserving other configuration elements. This is ideal for making targeted changes without affecting the entire profile.

### Use Cases:

- Adding or removing specific RADIUS attributes
- Updating profile descriptions or names
- Modifying individual attribute values or operators
- Making incremental configuration changes

### Full URL Example:

```
https://gate.zequenze.com/api/v1/aaa_profile/15/
```

### cURL Example:

```
curl -X PATCH "https://gate.zequenze.com/api/v1/aaa_profile/15/" \  
-H "Authorization: Bearer YOUR_API_TOKEN" \  
-H "Content-Type: application/json" \  
-d '{
```

```
"description": "Network administrator profile with enhanced security features",
"reply_attribute": [
  {
    "attribute": "Service-Type",
    "op": "=",
    "value": "Administrative-User"
  },
  {
    "attribute": "Session-Timeout",
    "op": "=",
    "value": "14400"
  }
]
}'
```

### Request Body Example:

```
{
  "description": "Network administrator profile with enhanced security features",
  "reply_attribute": [
    {
      "attribute": "Service-Type",
      "op": "=",
      "value": "Administrative-User"
    },
    {
      "attribute": "Session-Timeout",
      "op": "=",
      "value": "14400"
    },
    {
      "attribute": "Idle-Timeout",
      "op": "=",
      "value": "3600"
    }
  ]
}
```

### Response Codes:

Status	Description
200	Success - Profile successfully updated
400	Bad Request - Invalid data format
401	Unauthorized - Invalid or missing API token
403	Forbidden - Insufficient permissions to modify this profile
404	Not Found - AAA profile with specified ID does not exist

## DELETE /aaa\_profile/{id}/

**Description:** Permanently removes an AAA profile from the system. This operation cannot be undone and will affect any network devices or users currently assigned to this profile.

### Use Cases:

- Cleaning up obsolete or unused authentication profiles
- Removing test profiles after development completion
- Implementing profile lifecycle management
- Decommissioning deprecated authentication methods

### Full URL Example:

```
https://gate.zequenze.com/api/v1/aaa_profile/15/
```

### cURL Example:

```
curl -X DELETE "https://gate.zequenze.com/api/v1/aaa_profile/15/" \  
-H "Authorization: Bearer YOUR_API_TOKEN"
```

### Response Codes:

Status	Description
204	No Content - Profile successfully deleted
401	Unauthorized - Invalid or missing API token
403	Forbidden - Insufficient permissions to delete this profile
404	Not Found - AAA profile with specified ID does not exist
409	Conflict - Profile is in use and cannot be deleted

# Common Use Cases

## Use Case 1: Setting Up Role-Based Network Access

Create different AAA profiles for various organizational roles (admin, employee, guest) with appropriate VLAN assignments and access restrictions. Use GET to list existing profiles, POST to create new role-specific profiles, and PATCH to adjust permissions as roles evolve.

## Use Case 2: Implementing Guest Network Authentication

Configure a guest access profile with time-limited sessions and restricted network access. Create a profile with Session-Timeout and Idle-Timeout reply attributes, then use Tunnel-Type attributes to direct guests to an isolated VLAN.

## Use Case 3: Managing Device-Specific Authentication

Set up profiles that validate specific device characteristics using check attributes like Calling-Station-Id (MAC address) and NAS-Port-Type to ensure only authorized devices can access network resources.

## Use Case 4: Bulk Profile Management for Multi-Site Networks

Use the list endpoint with pagination to audit existing profiles across multiple sites, then implement standardization by creating template profiles and updating existing ones using PUT operations.

## Use Case 5: Dynamic Profile Updates for Security Compliance

Monitor and update AAA profiles to maintain security compliance by modifying session timeouts, adding new check attributes for enhanced validation, and removing deprecated authentication methods using PATCH operations.

---

# Best Practices

- **Attribute Operators:** Understand the difference between reply attribute operators (=, +=, :=) and check attribute operators. Use := for assignment, == for exact comparison, and \*= for regex pattern matching.
- **Profile Naming:** Use descriptive names and consistent short\_name formats (slug format with hyphens) to ensure profiles are easily identifiable and manageable at scale.
- **Error Handling:** Always check response codes and implement proper error handling, especially for 409 conflicts when profile names already exist or when profiles are in use during deletion attempts.
- **Pagination Strategy:** When listing profiles, use appropriate limit values (recommended: 25-50 per page) and implement proper pagination handling for large profile sets.
- **Security Considerations:** Regularly audit check attributes to ensure authentication requirements remain secure, and avoid storing sensitive information in profile descriptions.
- **Profile Dependencies:** Before deleting profiles, ensure they're not actively assigned to users or network devices, as this could disrupt network access.
- **Testing Changes:** Use PATCH for incremental updates during testing, then apply complete configurations with PUT once changes are validated.
- **Version Control:** Maintain external documentation of profile configurations for rollback scenarios, as the API doesn't provide built-in versioning.

---

Revision #1

Created 2026-02-11 03:11:47 UTC by ipena@zequenze.com

Updated 2026-02-11 03:11:47 UTC by ipena@zequenze.com