Configuration guide - v2.4 - SecureAuth IdP RADIUS server

Introduction

After installing the RADIUS Windows service, use the RADIUS Server admin console to configure the server and client, and optionally configure any SecureAuth IdP realm to be used with RADIUS.

NOTES:

- These instructions pertain to SecureAuth IdP RADIUS server v2.4. For the prior version, see SecureAuth IdP RADIUS Server v2.3.9+ Integration Guide.
- If using NetMotion VPN, then before configuring PEAP Settings under Step A: Settings configuration, be sure Microsoft Visual C++ runtime (Redistributable for Visual Studio 2012 Update 4) is installed on the Windows Server where SecureAuth IdP RADIUS server is deployed.

CONTENTS OF THIS DOCUMENT:

SecureAuth IdP RADIUS Server admin console

Access the RADIUS Server admin console at http://localhost:8088/configuration – the user interface is restricted to local machine access by default:

- Step A: Configure the Settings tab.
- Step B: Click the IdP Realms tab to add / edit Authentication API realms to be used with the RADIUS server.
- Step C: Click the RADIUS Clients tab to add and configure settings for the RADIUS client(s).

Create additional SecureAuth IdP RADIUS servers, back up the configuration

To simplify the task of creating additional SecureAuth IdP RADIUS servers, the configuration can be exported to a .cfg file and imported on the target SecureAuth IdP RADIUS server. The .cfg file can also be used to back up the configuration. See Export / Import RADIUS configuration.

WARNING: If the .cfg file is imported via the RADIUS admin console server, the configuration made on the Settings tab, IdP Realms tab, and RADIUS Clients tab will be overwritten by the configuration in this file.

Step A: Settings configuration

RADIUS Server Settings

1. Input the **Shared Secret** that was entered on the management console of the RADIUS client.

   The Authentication Port number **1812** appears by default.

Syslog Settings

2. OPTIONAL: Specify whether to **Enable Syslog Logging**.

    NOTE: The standard Syslog Protocol RFC5424 is supported.

3. If the Syslog Logging option is enabled, enter the **Syslog Server** IP address.

    The Syslog Port number **514** appears by default.

4. OPTIONAL: Enter the **Private Enterprise Number** (PEN).

PEAP Settings

5. If using NetMotion VPN:

    5a. Click **Choose File** to browse and select the Private Key PFX File.

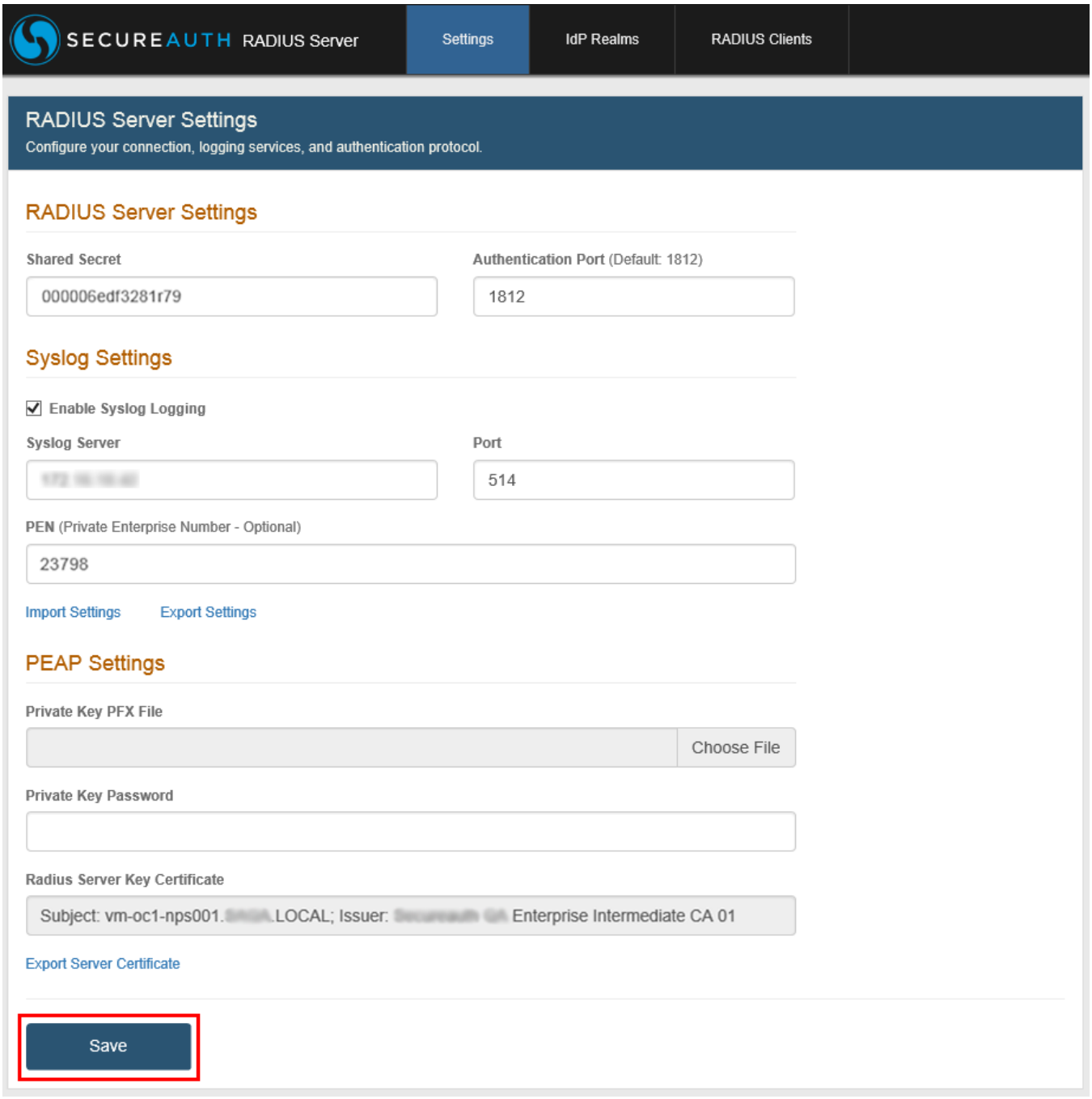
    5b. Enter the **Private Key Password** configured for the .PFX file.

    Radius Server Key Certificate information appears and identifies the SecureAuth IdP RADIUS server .PEM certificate.

    See Export SecureAuth IdP RADIUS server certificate for information about using the **Export Server Certificate** link.

6. Click **Save** after all server entries are made.

NOTE: The Shared Secret field displays **[Encrypted Value]** once the input values are saved.



Export SecureAuth IdP RADIUS server certificate

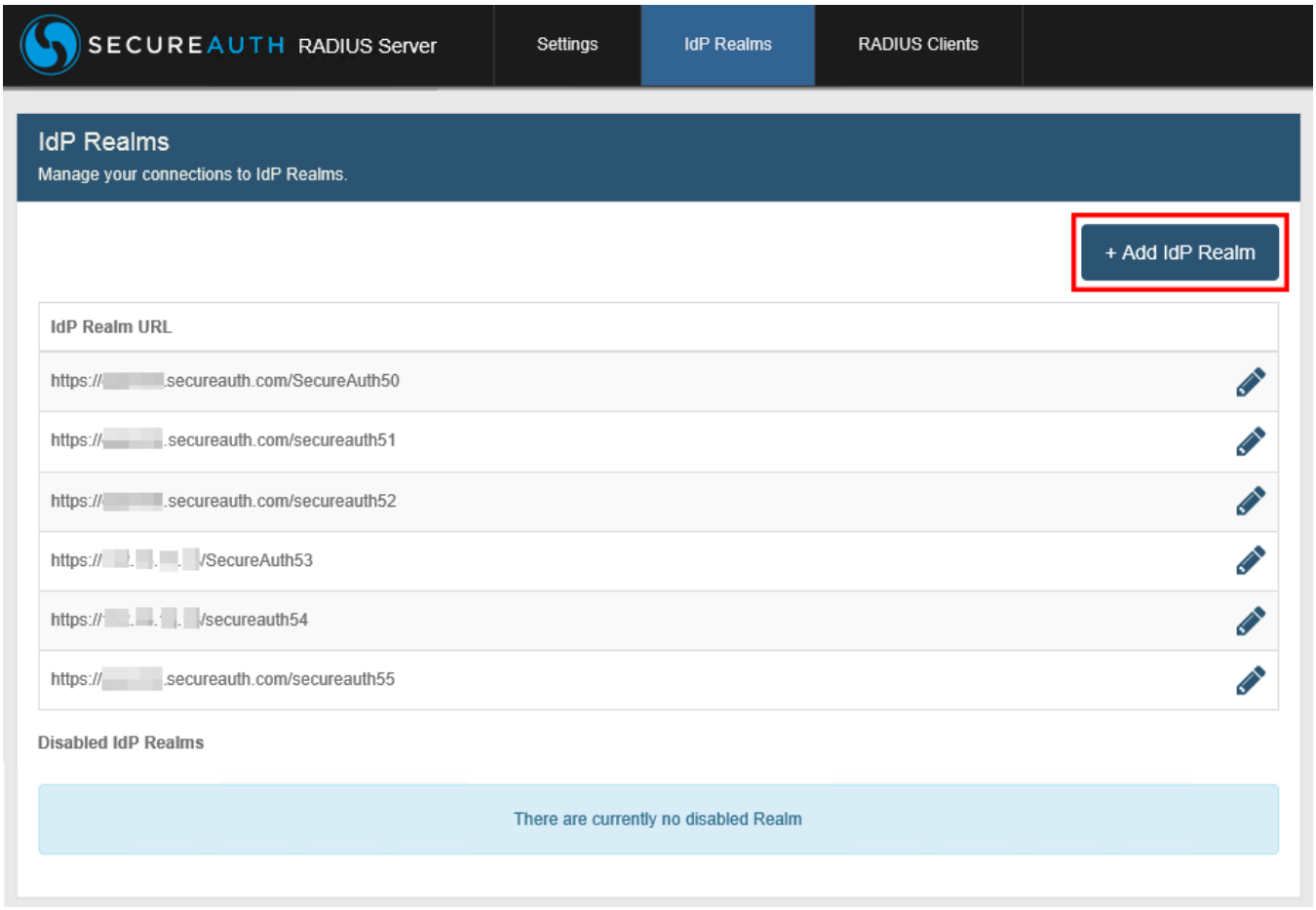
If the SecureAuth IdP RADIUS server certificate has been uploaded to this server, the Export Server Certificate link is active.

1. Click **Export Server Certificate** to download the .PEM certificate. This self-signed certificate must be imported to the Trust Store on the NetMotion client installed on the end-user mobile device.

    NOTE: SecureAuth IdP server certificates are *not* exported via this utility.

Step B: IdP Realms configuration

1. On the IdP Realms page, click **Add IdP Realm**.



Add IdP Realm

Ensure that the SecureAuth IdP API can connect to User properties. In the API realm in "API Permissions," check that "User Management" is enabled. If disabled, check the box.

2. In the Primary IdP Host field, **localhost** appears by default.

    If the realm is hosted on a different SecureAuth IdP than the one hosting this RADIUS server, enter the IdP host name or the IP address of the SecureAuth IdP realm to be used with this RADIUS server. Examples: hostname.secureauth.com or XXX.XXX.XXX.XXX (in which "X" represents a number in the IP address).

3. OPTIONAL: In the **Backup IdP Host** field, enter the host name or IP address of each SecureAuth IdP appliance to use for failover functionality, with each entry separated by a comma (,).

    Failover to a backup server can occur in these scenarios:

    - Communications are faulty with the target SecureAuth IdP.
    - RADIUS server receives no response.
    - RADIUS server receives errors from SecureAuth IdP.

    During failover, end-users can log on the VPN without disruption.

    NOTE: Refer to the Sample logs for different RADIUS failover scenarios in the SecureAuth IdP RADIUS server v2.4 integration guide for more information.

4. Enter the **IdP Realm** name and number. Examples: secureauth53 or SecureAuth84

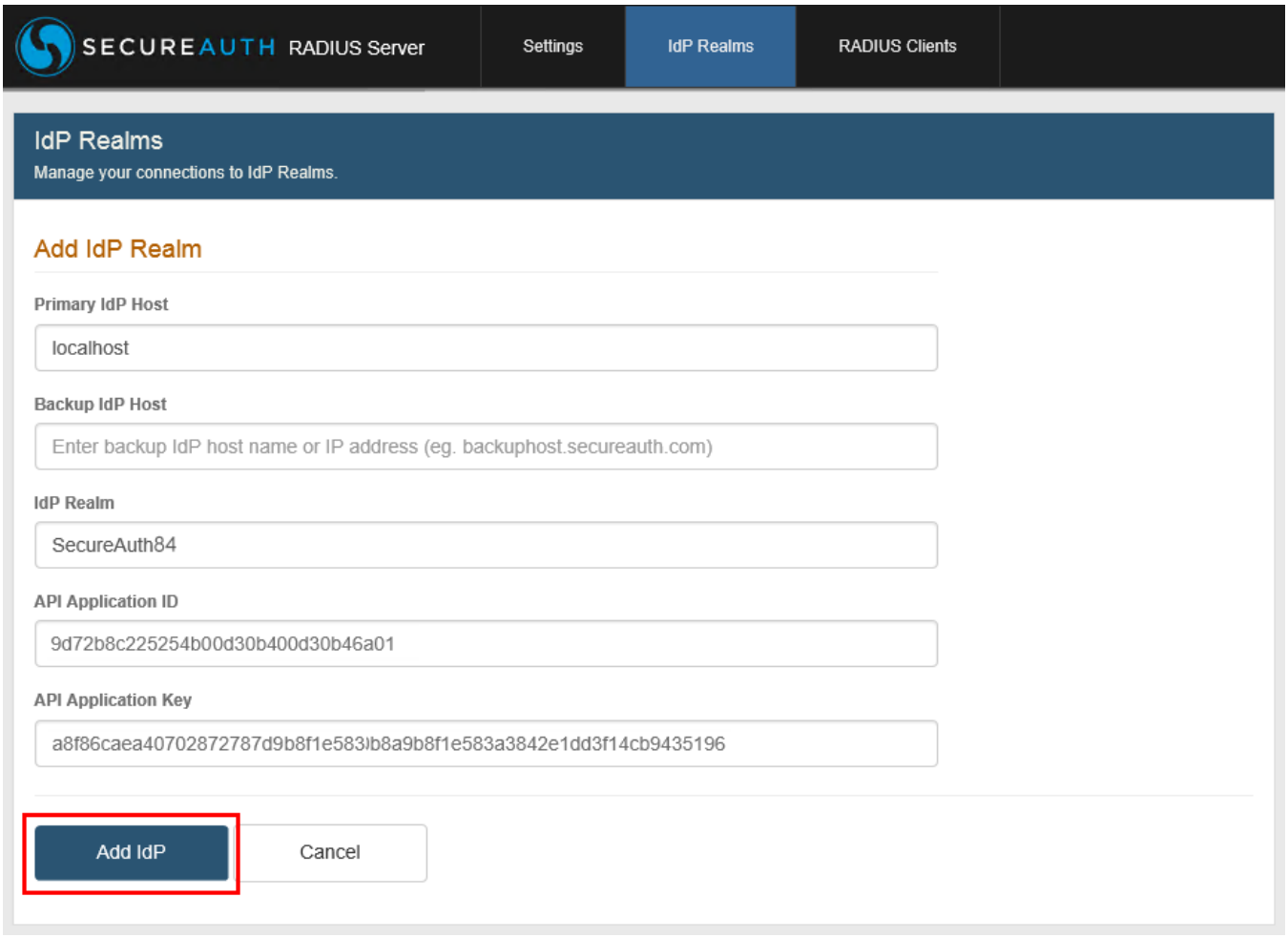
5. From the SecureAuth IdP server, copy the Application ID generated for the realm and paste that content in the **API Application ID** field.

    NOTE: Refer to Authentication API Guide (v9.1+) for steps on generating the Application ID in the API Key section of the API tab.

6. From the SecureAuth IdP server, copy the Application Key generated for the realm and paste that content in the **API Application Key** field.

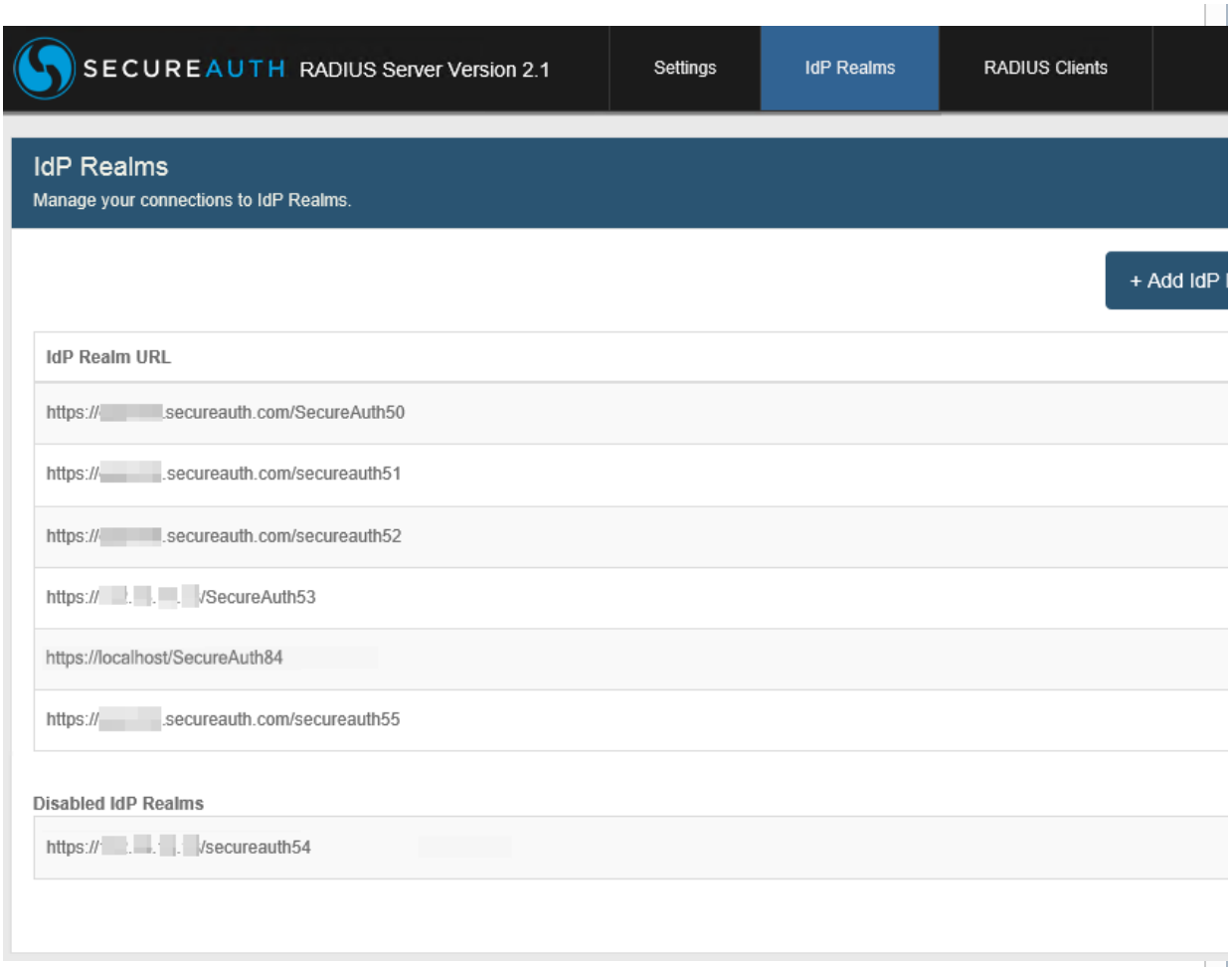
    NOTE: Refer to Authentication API Guide (v9.1+) for steps on generating the Application Key in the API Key section of the API tab.

7. Click **Add IdP** to enable the realm for use with the RADIUS server, or click **Cancel** to return to the IdP Realms page without adding the realm.



To edit a realm's information or remove a realm from the list...

1. Find the IdP Realm to be edited and click its "edit" icon at the far right.



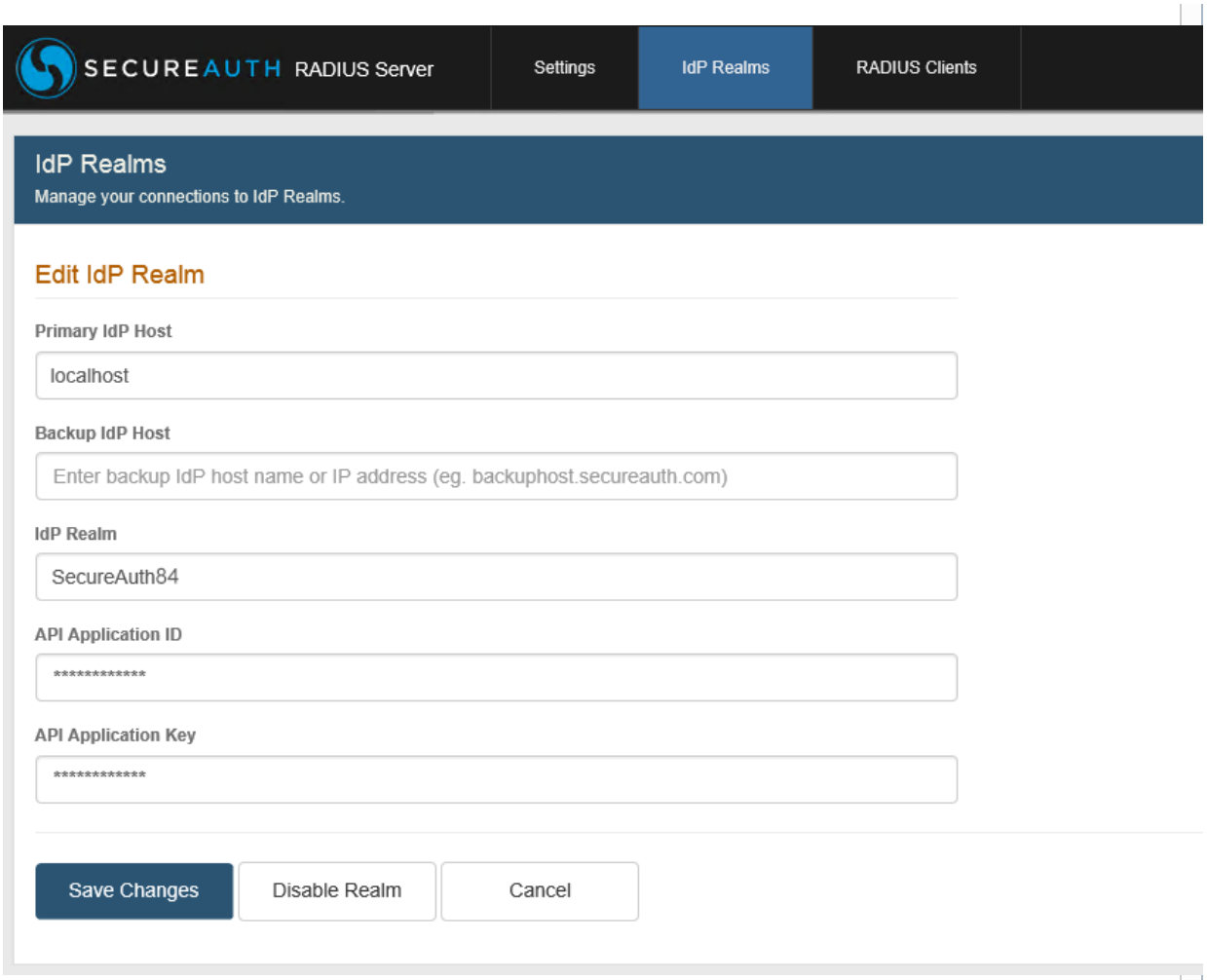
Edit IdP Realm

2. Do one of the following:

a. Click **Cancel** if no changes will be made – the IdP Realm URL list appears;

b. Update any information that has changed on the realm and click **Save Changes** – note encrypted values appear for the saved **API Application ID** and **API Application Key**; or

c. Click **Disable Realm** if the realm will no longer be used with the RADIUS server. This action moves the realm to the Disabled IdP Realms list – an example of a disabled IdP realm appears in the sample screen above.

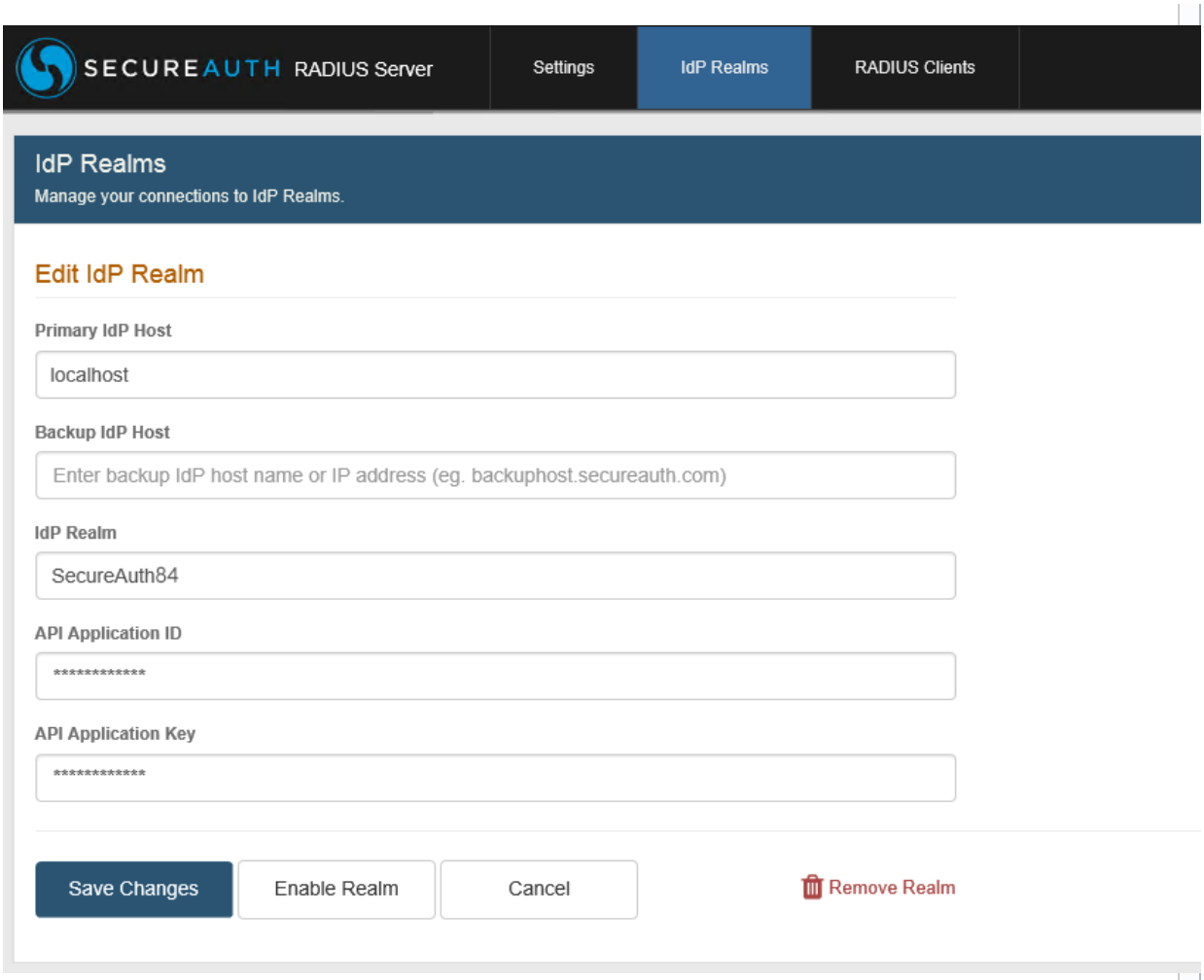


3. If **Disable Realm** was clicked, the Remove Realm option becomes available. Do one of the following:

    a. Click **Cancel** if no changes will be made – the IdP Realm URL list appears;

    b. Click **Remove Realm** to remove the realm from the Disabled IdP Realms list and from the RADIUS server; or

    c. Click **Enable Realm** to enable the realm for use with the RADIUS server. This action removes the realm from the Disabled IdP Realms list and includes it in the IdP Realm URL list.



Step C: RADIUS Clients configuration

By default a single row appears populated with client information that can be modified on the Edit RADIUS Client page:

- **Client Name** – a friendly name for the client can be manually entered.
- **Client IP Address** – asterisk (*) indicates the client IP will be mapped to all RADIUS client IPs configured.
- **Authentication Workflow** – default workflow selection is Password | Timed Passcode or Second Factor.

To view details about a client...

1. Click the "i" at the start of the row – a window appears showing details about the RADIUS client.

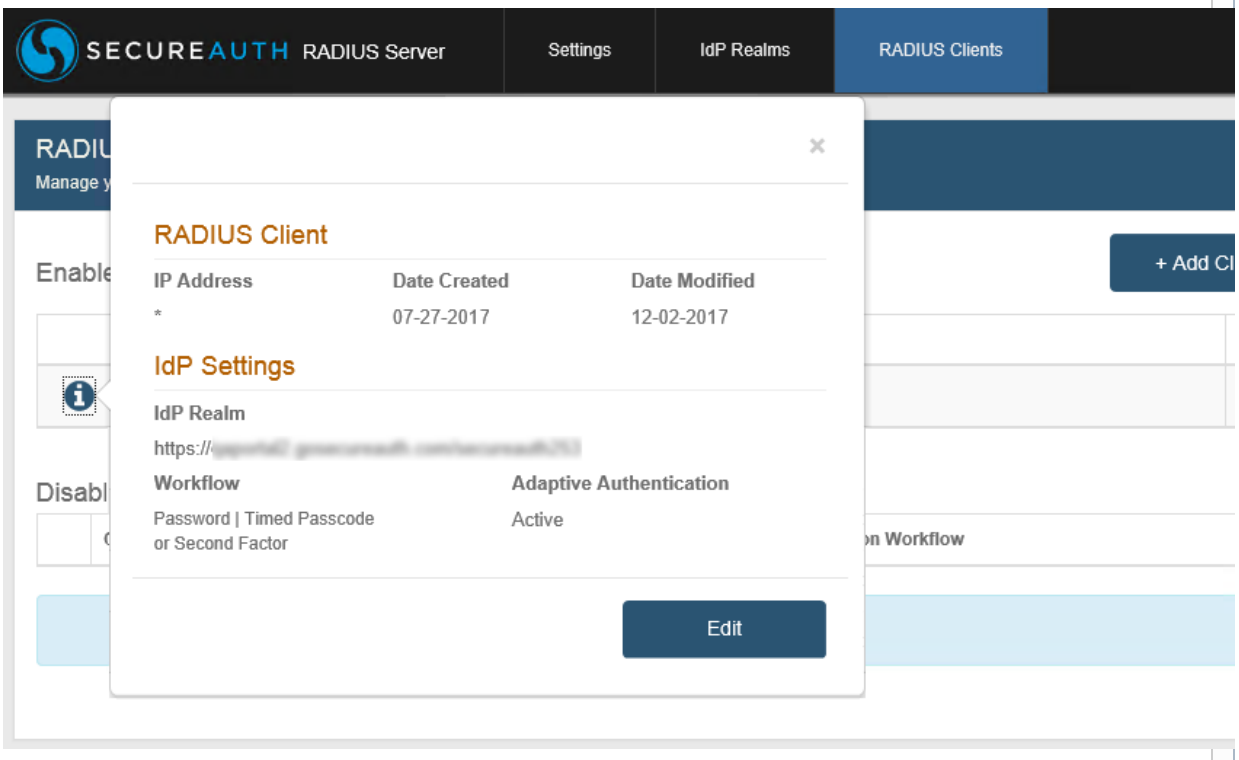
RADIUS Client section shows:

- **IP Address** – the client's IP address, or an asterisk (*) which indicates the client IP will be mapped to all RADIUS client IPs configured.
- **Date Created** – client creation date using the MM-DD-YYYY format.
- **Date Modified** – most recent client modification date using the MM-DD-YYYY format.

IdP Settings section shows:

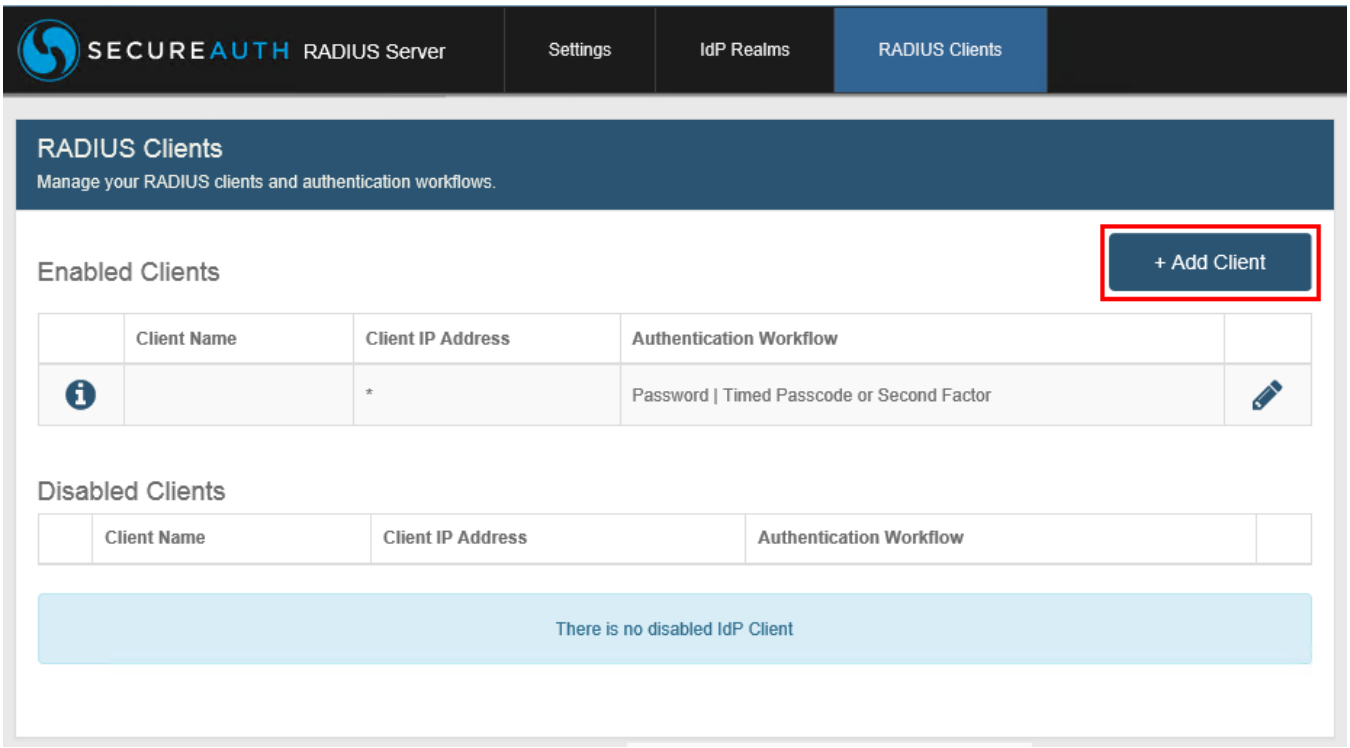
- **IdP Realm** – URL / realm number selected.
- **Workflow** – one of eight selections made for this client (the default is Password | Timed Passcode or Second Factor).
- **Adaptive Authentication** – "Active" or "Inactive" status depending on whether or not this feature is enabled.

2. Click **Edit** to go to the Edit RADIUS Client page, or click the "X" in the upper right corner to exit the window.



Add RADIUS Client

1. Click **Add Client**.



2. Enter a friendly **Client Name**. For example: "Cisco".

3. Enter the **IP Address** to filter the RADIUS client. In general, the NAS-IP address should be entered.

    However, to filter the RADIUS client by the client IP address, and not NAS-IP address, then additionally enable **Use Client Source IP Address**.

    TIP: You can use a wild card to only allow machines from a specified subnet to connect, as in this example: 10.1.2.*

SecureAuth IdP Settings

4. Select the SecureAuth **IdP Realm** from the dropdown.

    Selections only include Authentication API realms added on the IdP Realms page.

5. Select the **Authentication Workflow** from the dropdown – this must match a workflow configured and enabled on the realm selected in step 4:

- **Password | Timed Passcode or Second Factor**
- **Password & Mobile Login Request** (Approve / Deny)
- **Password Only**
- **Timed Passcode Only**
- **Timed Passcode / Password**
- **Password | Timed Passcode**
- **Timed Passcode | Password**
- **Username | Second Factor**
- **Username | Second Factor | Password**
- **PIN + TOTP**
- **Password & Timed Passcode**

    NOTE: Not all authentication workflows are supported by all RADIUS clients due to RADIUS client configuration limitations. See Multi-Factor Methods configuration for links to versions of documents that explain how to configure realms for the supported authentication workflows.

6. OPTIONAL: If using Adaptive Authentication, check **Enable Adaptive Authentication**.

    6a. Note that **Calling-Station-Id** appears by default in the **RADIUS End User IP** field – this attribute is used to verify the end-user's IP address.

    6b. Edit the value in this field if using Palo Alto Networks or Juniper Networks platforms:

    - For Palo Alto Networks, enter **PaloAlto-Client-Source-IP**
    - For Juniper Networks, enter **Tunnel-Client-Endpoint**

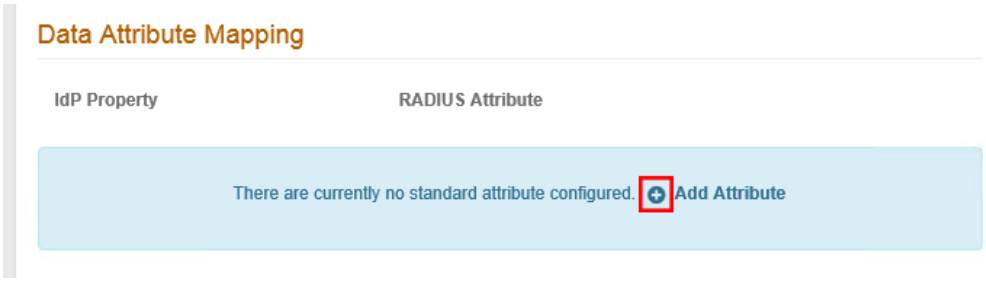
    NOTE: IP verification is only supported on Cisco, NetScaler, and Palo Alto Networks platforms.

7. **Data Attribute Mapping** is used to map an attribute from the configured SecureAuth IdP Data Store to the RADIUS client – this feature is often used with a VPN for making policy decisions.

NOTE: Only string values are supported for data attribute mapping.

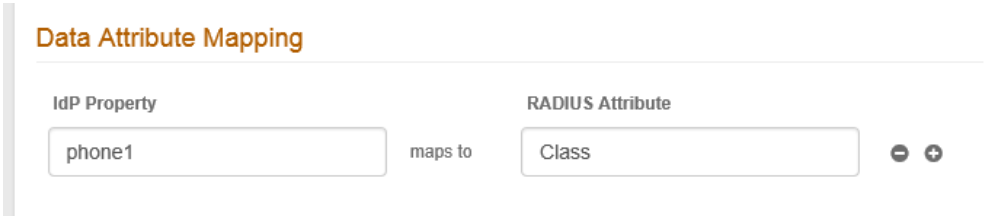
To add a row and map a data attribute...

7a. Click the "**+**" button preceding **Add Attribute**.

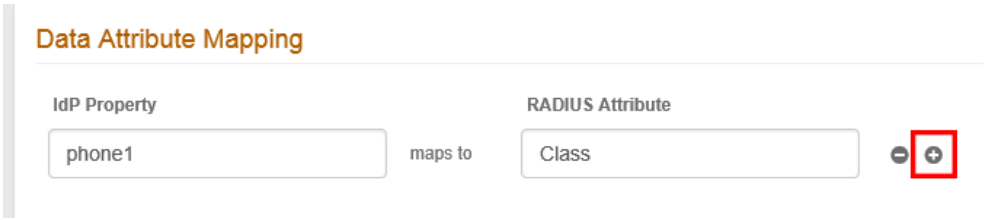


7b. By default **auxId1** appears under **IdP Property**. Modify this entry to map a field or a User Group to a supported SecureAuth IdP Property; this entry is case-sensitive.

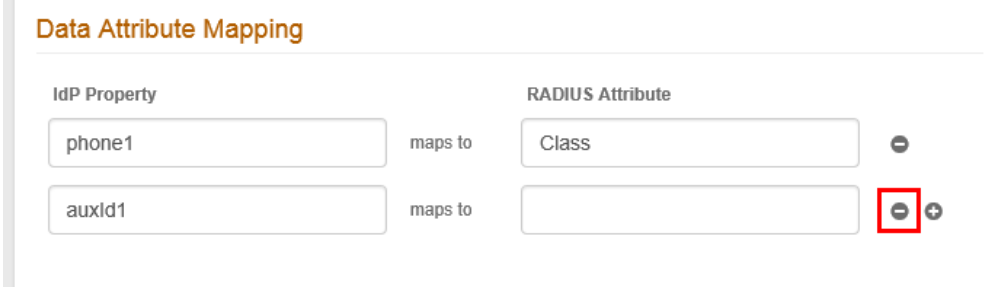
7c. For **RADIUS Attribute**, enter the name of the RADIUS client attribute (for example, Class) that is mapped to the SecureAuth IdP Property specified in step 7b; this entry is case-sensitive.



7d. To map another attribute, click the "**+**" button at the end of the last row; this action adds a new row below.



NOTE: To remove a row from the Data Attribute Mapping table, click the "**-**" button at the end of the row to be removed.



8. **Custom Attribute Mapping** is used to map an attribute from the configured SecureAuth IdP Data Store to a vendor specific attribute – this usually occurs in a scenario in which the VPN appliance is unable to perform an LDAP lookup.

To add a row and map a custom attribute...

8a. Click the "**+**" button preceding **Add Attribute**.

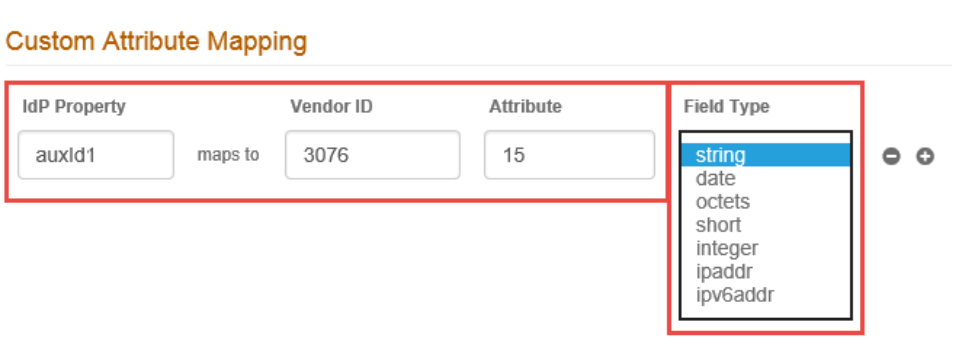
8b. By default **auxId1** appears under **IdP Property**. Modify this entry to map a field or a User Group to a supported SecureAuth IdP Property; this entry is case-sensitive.

8c. Enter the numeric **Vendor ID**.

8d. Enter the numeric Vendor-Specific **Attribute** that is mapped to the SecureAuth IdP Property specified in step 8b.

8e. Select the RADIUS attribute type from the **Field Type** dropdown:

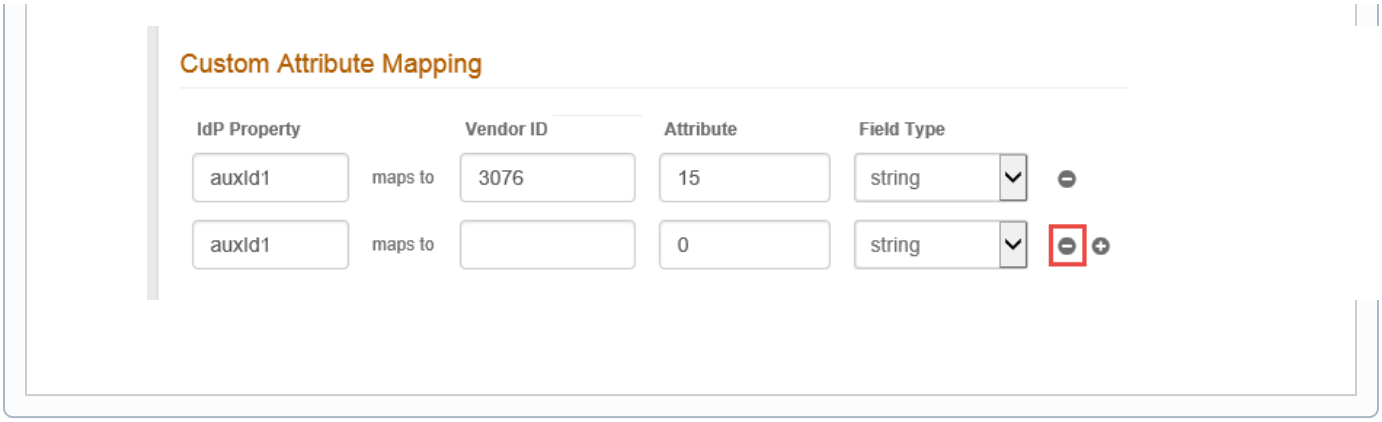
- **string** – variable-length string field used for printable text strings.
- **date** – UNIX timestamp in seconds, as of January 1, 1970 GMT.
- **octets** – variable-length string field used for binary data.
- **short** – two-byte integer.
- **integer** – unsigned 32-bit integer.
- **ipaddr** – IPv4 address.
- **ipv6addr** – IPv6 address.



NOTE: The Field Type selection must be accurately defined in order to be accepted by the client.

8f. To map another attribute, click the "**+**" button at the end of the last row; this action adds a new row below.

NOTE: To remove a row from the Custom Attribute Mapping table, click the "**-**" button at the end of the row to be removed.



9. **Static Value Mapping** is used to map data to the RADIUS Vendor-Specific Attribute (VSA) configuration.

To add a row and map a static value attribute...

9a. Click the "**+**" button preceding **Add Attribute**.

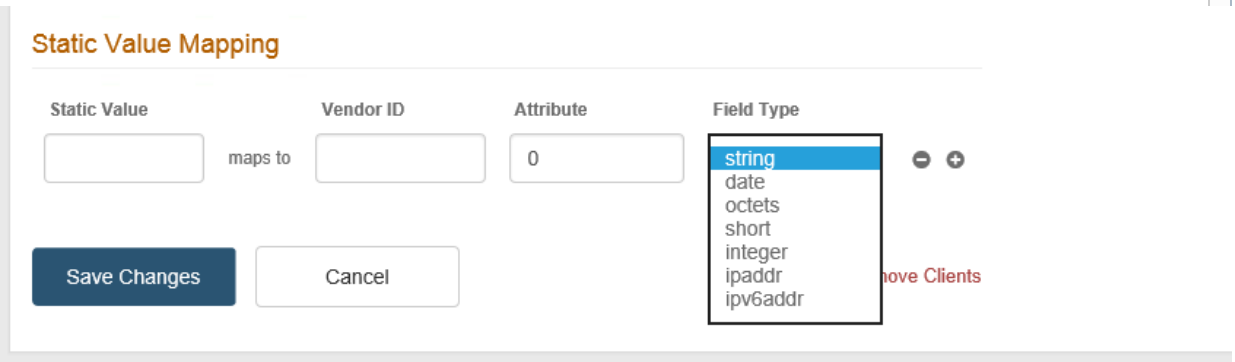
9b. Enter a **Static Value** to be mapped to the RADIUS Attribute.

9c. Enter the numeric **Vendor ID**.

9d. Enter the numeric Vendor-Specific **Attribute** that is mapped to the Static Value specified in step 9b.

9e. Select the RADIUS attribute type from the **Field Type** dropdown:

- **string** – variable-length string field used for printable text strings.
- **date** – UNIX timestamp in seconds, as of January 1, 1970 GMT.
- **octets** – variable-length string field used for binary data.
- **short** – two-byte integer.
- **integer** – unsigned 32-bit integer.
- **ipaddr** – IPv4 address.
- **ipv6addr** – IPv6 address.

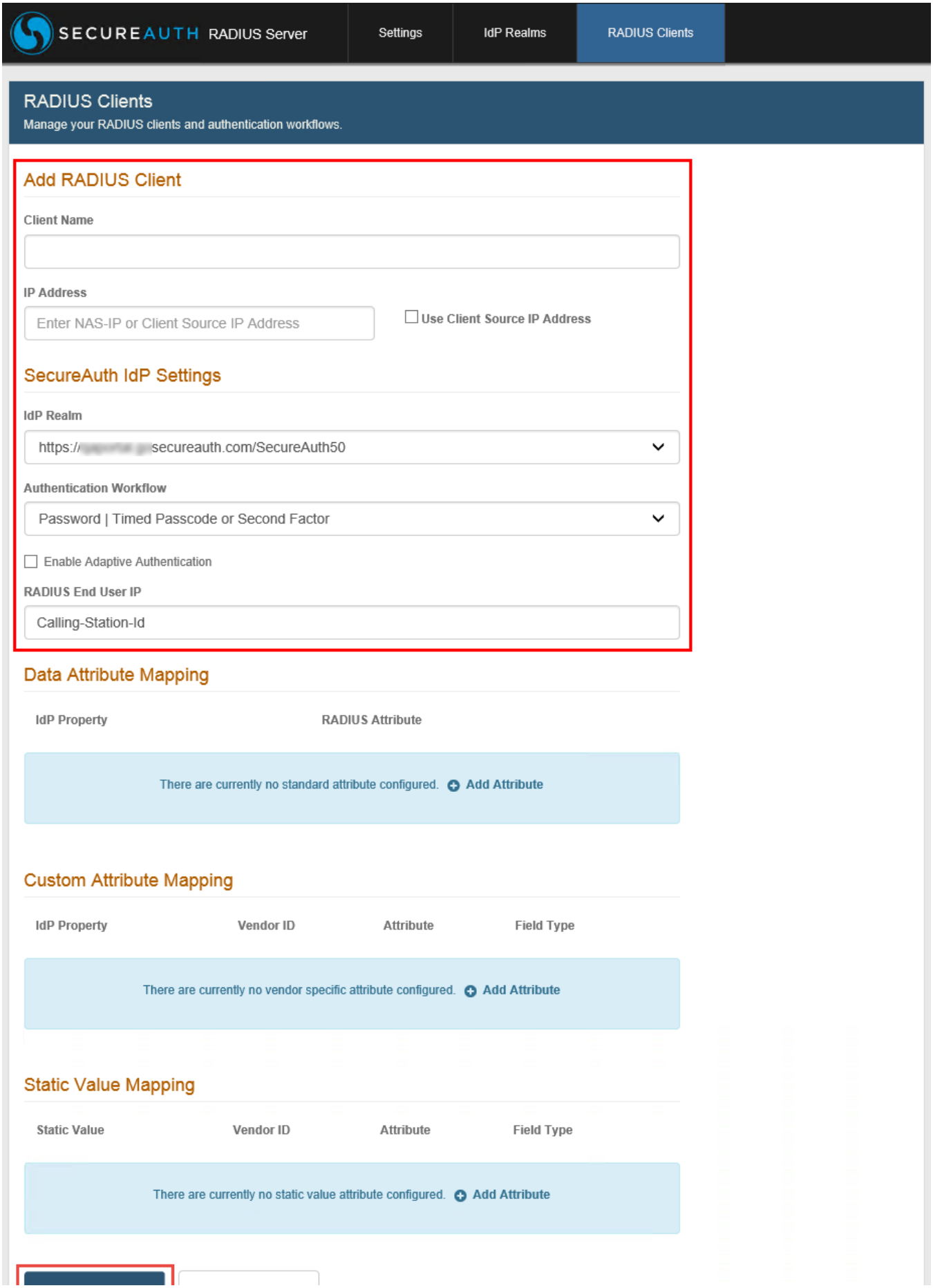


NOTE: The Field Type selection must be accurately defined in order to be accepted by the client.

9f. To map another attribute, click the "**+**" button at the end of the last row; this action adds a new row below.

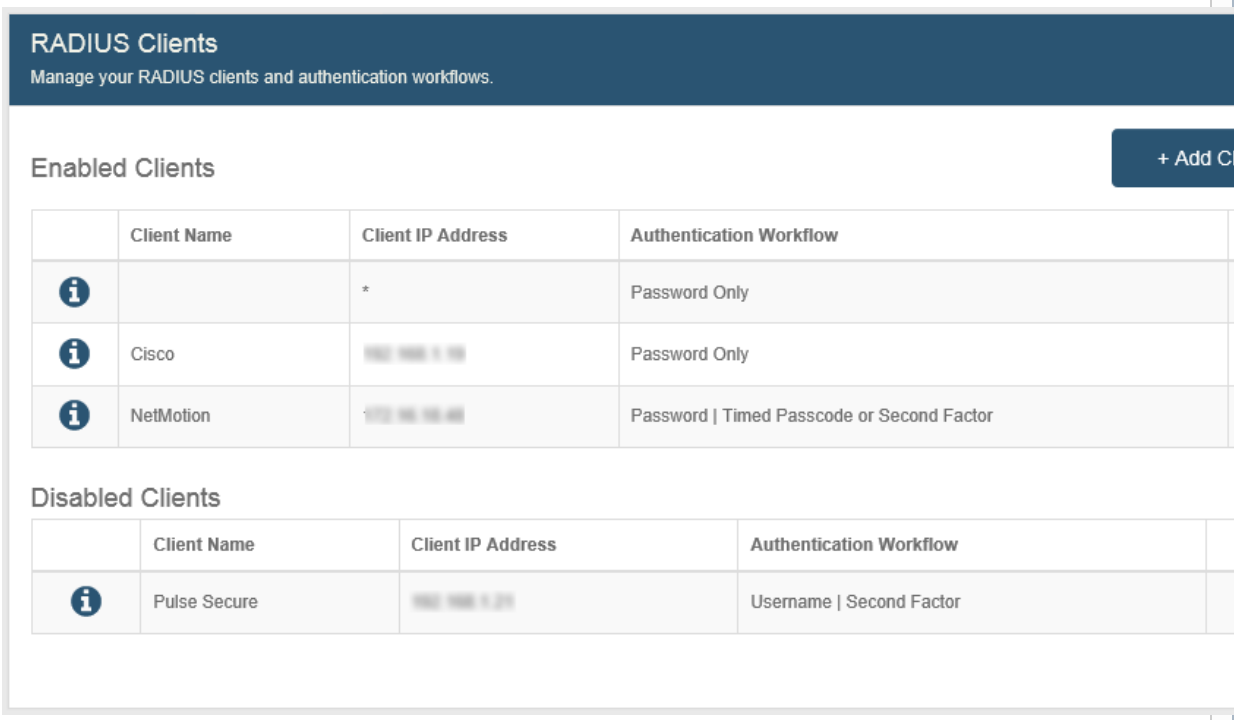
NOTE: To remove a row from the Static Value Mapping table, click the "**-**" button at the end of the row to be removed.

10. Click **Add Client** after all client entries are made, or click **Cancel** to return to the **RADIUS Clients** page without adding a client.


SECUREAUTH RADIUS Server
Settings
IdP Realms
RADIUS Clients
RADIUS Clients
Manage your RADIUS clients and authentication workflows.
Add RADIUS Client
Client Name
IP Address
Enter NAS-IP or Client Source IP Address
Use Client Source IP Address
SecureAuth IdP Settings
IdP Realm
https://[redacted]secureauth.com/SecureAuth50
Authentication Workflow
Password | Timed Passcode or Second Factor
Enable Adaptive Authentication
RADIUS End User IP
Calling-Station-Id
Data Attribute Mapping
IdP Property
RADIUS Attribute
There are currently no standard attribute configured. Add Attribute
Custom Attribute Mapping
IdP Property
Vendor ID
Attribute
Field Type
There are currently no vendor specific attribute configured. Add Attribute
Static Value Mapping
Static Value
Vendor ID
Attribute
Field Type
There are currently no static value attribute configured. Add Attribute

To edit a client's information or remove a client from the list...

1. Find the RADIUS client to be edited and click its "edit" icon at the far right.



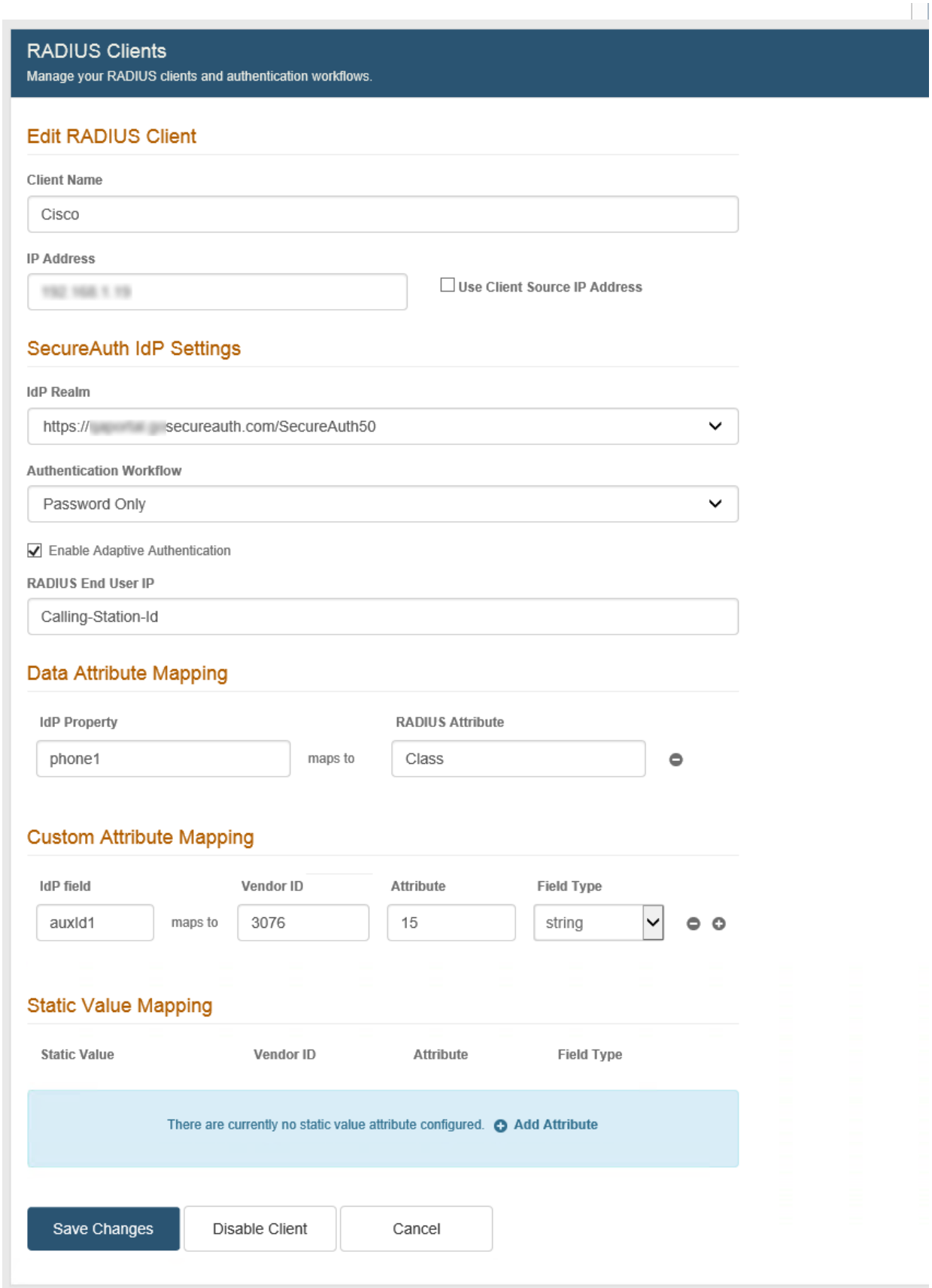
Edit RADIUS Client

2. Do one of the following:

a. Click **Cancel** if no changes will be made – the **RADIUS Clients** page appears;

b. Update any information that has changed for the client and click **Save Changes**; or

c. Click **Disable Client** if the client will no longer be used with the realm or RADIUS server. This action moves the client to the Disabled Clients list – an example of a disabled client appears in the sample screen above.

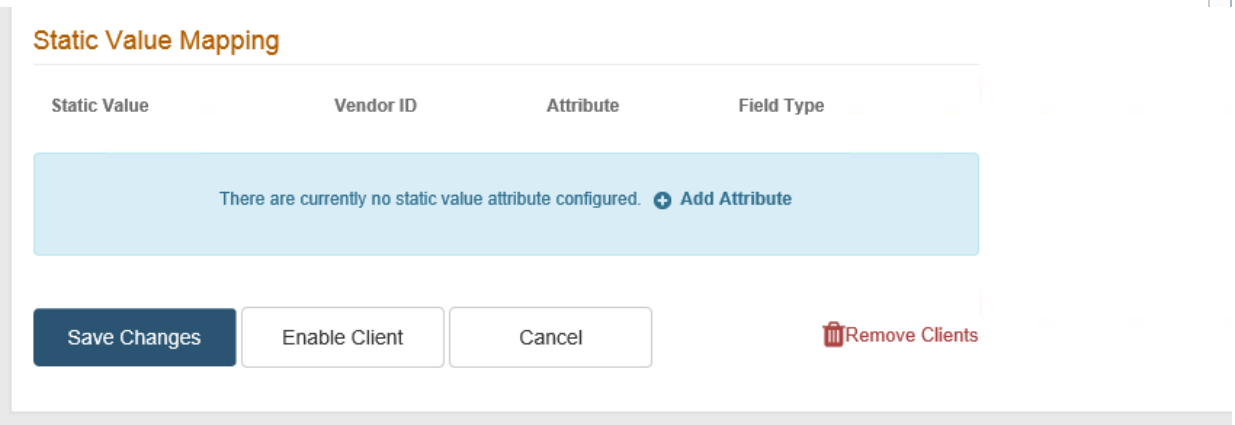


3. If **Disable Client** was clicked, the Remove Clients option becomes available. Do one of the following:

a. Click **Cancel** if no changes will be made – the RADIUS clients list appears;

b. Click **Remove Clients** to remove the client from the Disabled Clients list and from the RADIUS server; or

c. Click **Enable Client** to enable the client for use with the realm and RADIUS server. This action removes the client from the Disabled Clients list and includes it in the Enabled Clients list.



Export / Import RADIUS configuration

The saved RADIUS Admin Console configuration can be downloaded as a .cfg file via the **Export Settings** function.

Use the **Import Settings** function of the RADIUS Admin Console:

- To restore the RADIUS backup configuration to the same SecureAuth IdP.
- To expedite configuring RADIUS server on another SecureAuth IdP.

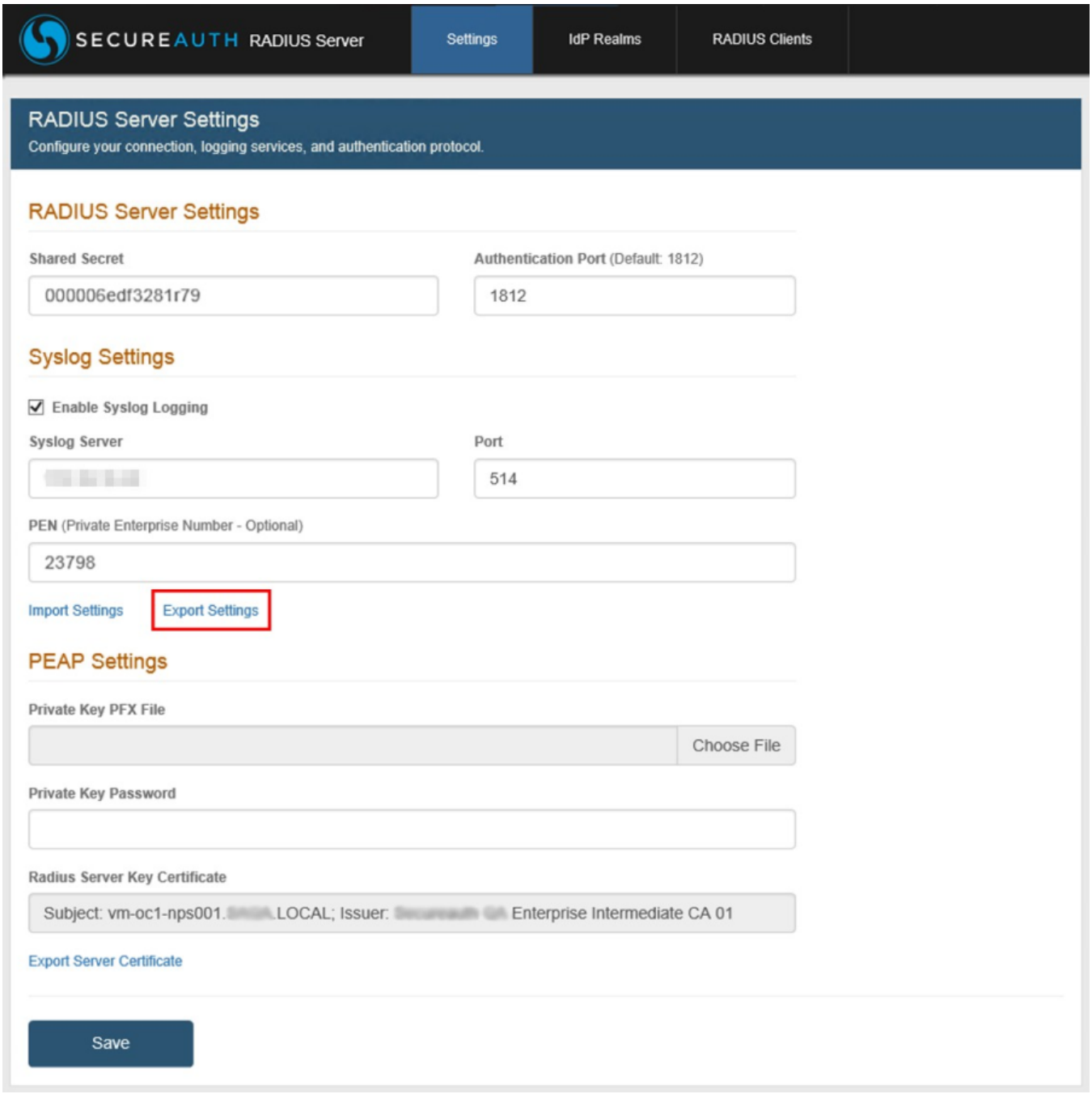
Export RADIUS configuration

1. In the Syslog Settings section, click **Export Settings**.

    NOTE: If there is no configuration to download, this button is enabled but will return an error if clicked.

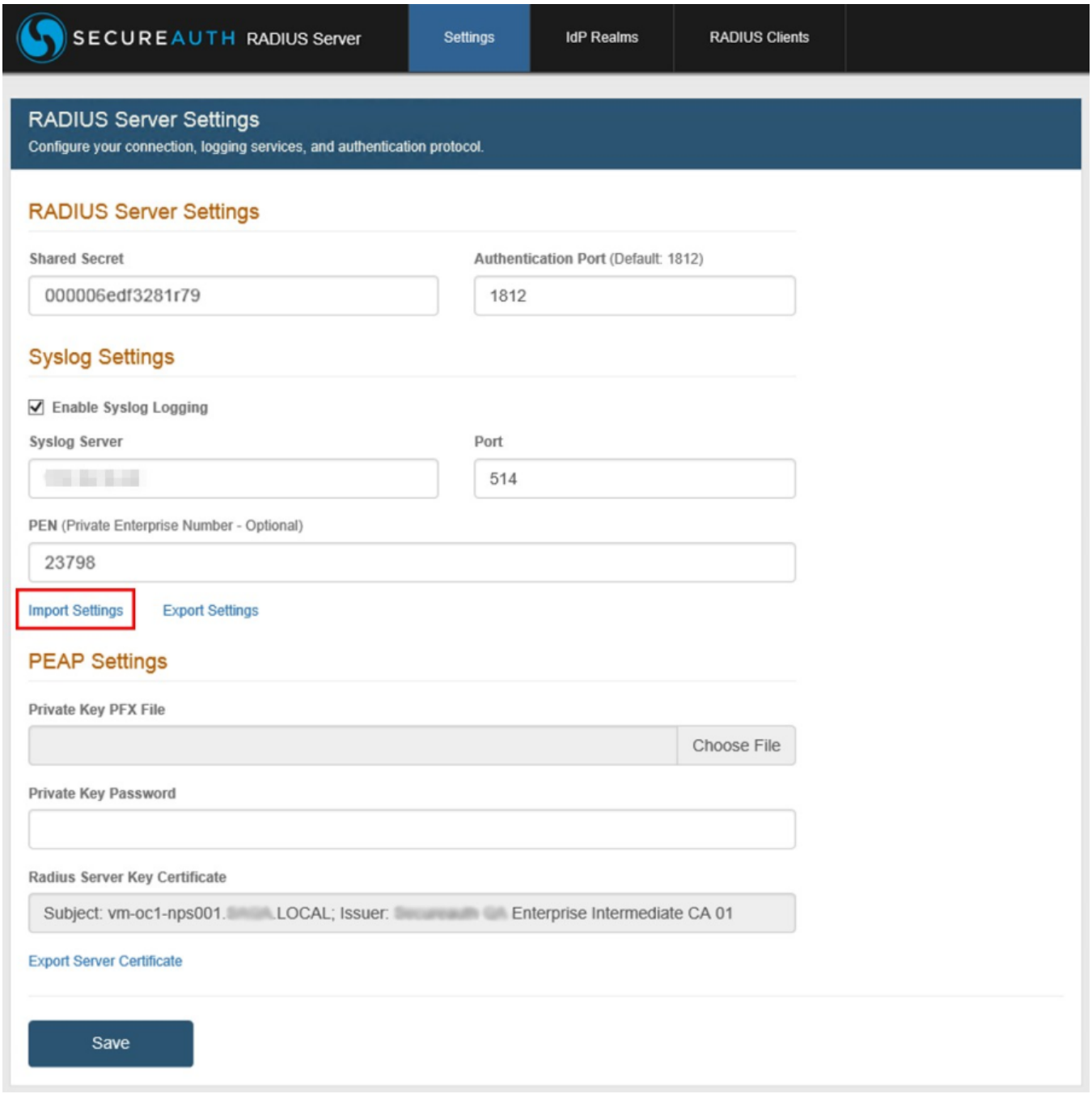
2. Download the .cfg file that contains settings configured on the RADIUS Admin Console.

    NOTE: The .cfg file can be imported into a new or existing RADIUS Admin Console to overwrite the current configuration**.**



Import RADIUS configuration

1. In the Syslog Settings section, click **Import Settings**.

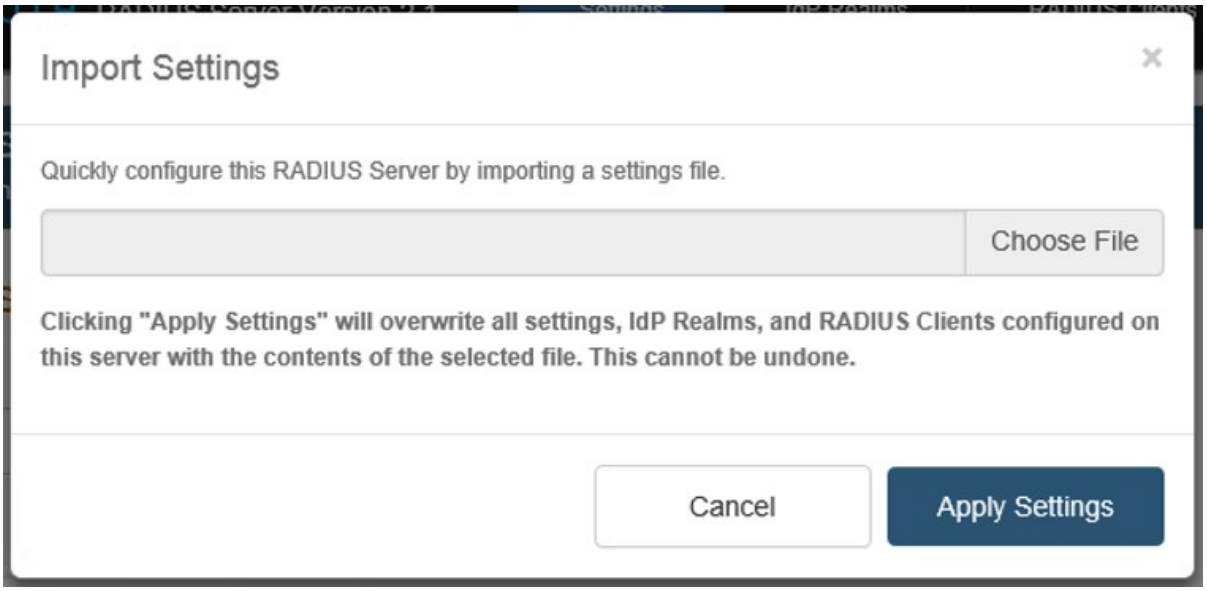


2. In the Import Settings window, click **Choose File**.

3. Browse to find and select the .cfg file configured on the RADIUS Admin Console containing settings to be uploaded to this RADIUS server.

    NOTE: Clicking Apply Settings immediately overwrites the configuration on server Settings, IdP Realms, and RADIUS Clients tabs of the RADIUS Admin Console.

4. Click **Apply Settings** to import the configuration from the .cfg file, or click **Cancel** to close the window.



Client user interface configuration options

Configure conversion of Domain\SAM-account-name logon format to UPN

If using the Domain\SAM-account-name logon format in the environment, the Security Account Manager (SAM) format must be converted to the User Principal Name (UPN) format in order for the RADIUS server to accept end-user logins. For example: Convert acme\jsmith to jsmith@acme.com

To convert the login format from SAM to UPN:

1. Go to C:\idpRADIUS\bin\conf\domainUPNSuffixes.properties

    NOTE: If domainUPNSuffixes.properties does not exist, then the file must be created and placed in this path.

2. Add an entry to convert the domain. For example:

```
acme=acme.local
```

    or

```
Acme1=acme1.com
```

3. Save the entry.

When the end-user makes a Domain name\username entry in the user ID field, the RADIUS server will automatically convert the entry to the UPN format.

Modify text showing on client user interface during login

Text that shows on the client user interface during the login process. For example: "Enter a time-based passcode", "SEND LOGIN REQUEST TO PHONE", etc. can be modified in the uiTextsBundle properties file.

To edit the properties file:

1. Go to C:\idpRADIUS\bin\conf\uiTextsBundle.properties.

2. Edit only the text that follows the "=" sign.

3. Save edits.

Final step...

See the end-user experience