Introduction

Use this guide to enable end-user desktop, web, and mobile 2-Factor Authentication login access to a VPN and remote resources via RADIUS. Certificates generated on the RADIUS server are used in authentication requests.

**NOTE**: Click [here](#) for the latest version of the SecureAuth IdP RADIUS Server Integration Guide

Prerequisites

1. Have SecureAuth IdP version 8.1+  
2. Have a RADIUS server installed on a SecureAuth IdP appliance or another server running Windows Server 2008 R2, 2012, or 2012 R2  
3. Ensure TCP port 8088 is blocked on the RADIUS server – this is the default setting on a SecureAuth appliance  
4. Have a supported platform / RADIUS client
   - Cisco ASA with AnyConnect and Web Client
   - Cisco IPSec
   - Citrix NetScaler with Web Client
   - Juniper VPN (IVE, MAG) Pulse Secure thick client
   - VMware Horizon HTML Access
   - VMware Horizon View
5. On the RADIUS client’s management console
   - Configure the RADIUS server IP address
   - Create a shared secret to use between the RADIUS server and RADIUS client(s)
   - Enter each RADIUS client IP address to be used
   - Specify Port 1812 to use for RADIUS authentication requests
   - Configure the group policy to identify resources that end-users can access once logged on the network
   - Create a connection profile to identify the DNS server that end-users will use to access the VPN
6. Have a SecureAuth IdP realm configured for Authentication API

   RADIUS 2.0.1 supports the following registration methods for 2-Factor Authentication workflows
   - Time-based One-Time Passcode (TOTP) (legacy from RADIUS v1.0.x)
   - SMS
   - Phone
   - Email
   - Passcode OTP (Push Notification)
   - Mobile Login Request (Push-to-Accept Notification – requires SecureAuth IdP version 8.2 and above)
7. (OPTIONAL) Have Adaptive Authentication configured on the Authentication API realm

NOTE: Adaptive Authentication in SecureAuth IdP version 8.2 supports user group checking. See Optional Feature: Adaptive Authentication for RADIUS responses with user group checking enabled

8. Download RADIUS
NOTE: The latest version of SecureAuth IdP RADIUS Server is available from the SecureAuth downloads page by clicking here.

Click here for the latest version of the SecureAuth IdP RADIUS Server Integration Guide.

See Third Party Software License Notices for information about the use of Java with this software.

9. If SecureAuth RADIUS v1.0.x is currently installed, review the upgrade instructions in the SecureAuth IdP RADIUS Server v2.0.1 Installation Guide before installing the newer version of RADIUS.

   If installing RADIUS v2.0.1 for the first time on the designated appliance, follow the installation instructions in the SecureAuth IdP RADIUS Server v2.0.1 Installation Guide.

10. Install the SecureAuth approved version of Java service in the Windows Services console on the SecureAuth IdP appliance or on the designated Windows appliance on your network.

SecureAuth RADIUS Admin Console Configuration Steps

After the RADIUS Windows service is installed and configured, use the RADIUS Admin Console to configure the server and client.

1. Access the RADIUS Admin Console at http://localhost:8088/configuration – the user interface is restricted to local machine access by default.

2. Configure server settings on the RADIUS Server tab.

3. Click the RADIUS Client tab to add and configure settings for the RADIUS client(s).

RADIUS Server Configuration
RADIUS Server Settings

Shared Secret
000006edf3281r79

Authentication Port
1812  Default: 1812

SecureAuth IdP Settings

IDP Server  API Realm
localhost  SecureAuth

API Application ID
5e0f655a77484a0ea799bafdf0f04c28c

API Application Key
5a264feaa95a348d8fa64bf38d8ad50638bd807f0940e817e1045c518d57d

☑ Check Group Restrictions in Adaptive Authentication

Syslog Settings

☑ Enable Syslog Logging

Syslog Server  Port
1514

Private Enterprise Number (Optional)
23798

Save
1. In the **RADIUS Server Settings** section, enter the **Shared Secret** that was entered in the management console of the RADIUS client.

2. The **Authentication Port** field is pre-populated with the default port number **1812**.

3. In the **SecureAuth IdP Settings** section, the **IdP Server** field is pre-populated with **localhost**.
   - If using a server other than the local host server, enter the host name (e.g., hostname.secureauth.com).

4. Enter the **API Realm** name and number.
   - e.g., SecureAuth23

5. Copy and paste the **API Application ID** which comes from the **Authentication API** section of the Registration Methods tab.

6. Copy and paste the **Application Key**.

7. (OPTIONAL) If using Adaptive Authentication and its User / Group Restriction option, enable the **Check Group Restricts in Adaptive Authentication** option.

8. (OPTIONAL) In the **Syslog Settings** section, specify whether to **Enable Syslog Logging**.

   - The standard Syslog Protocol RFC5424 is supported.

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

10. Enter the Syslog **Port** number.

11. (OPTIONAL) Enter the **Private Enterprise Number (PEN)**.

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

   - The Shared Secret, API Application ID, and Application Key fields each display **[Encrypted Value]** once the input values are saved.
1. In the **RADIUS Clients** section, by default an asterisk ( * ) appears in the IP field; this indicates the client IP will be mapped to all RADIUS client IPs configured. Modify this entry by inputting a specific RADIUS client IP address.

2. Select the **Authentication Workflow Type** (one of six authentication workflows) from the dropdown:
   - Password + Time-based Passcode or 2-Factor Challenge Options
   - Password & Mobile Login Request (Accept / Deny)
   - Password
   - Time-based Passcode
   - Time-based Passcode / Password
   - Password + Time-based Passcode

   - **This selection must match one of the authentication workflows configured on the Authentication API realm.**

3. Click **Add new client**

4. A row is added in the table.

5. Repeat steps 1 to 4 to add and configure another client.

   - **Click Remove row at the end of the row to remove a client from the table.**

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

---

**End-user Experience**

The authentication workflow requires the entry of the username followed by at least one other code entry, such as a password or passcode, before the login button is enabled for VPN access.
### Single screen login workflows

![VPN Login](image)

**Password**

1. Enter the username
2. Enter the password

**Time-based Passcode**

1. Enter the username
2. In the password field, enter the TOTP

**Time-based Passcode / Password**

1. Enter the username
2. In the password field, enter the TOTP, then a "/" (forward slash), followed by the password

   e.g. 563719/Password!

### Multi-screen login workflows

The images in this section provide examples of some user interfaces from the end-user login experience; the appearances of user interfaces will differ depending on the type of VPN client and mobile device used.
Password + Time-based Passcode

1. On the VPN login screen, enter the username

2. Enter the password
   
   A time-based passcode is sent

3. Enter the TOTP – a response entry field is not presented
Mobile VPN Login

Please enter your username and password.

Admin55

Password

Login

Done

1234567890

- / : ; ( ) $ & @ "
Login Request

SecureAuth Corporation
Google Apps

Admin55

14:27:07 at 02/16/2016
Los Angeles, US
Password & Mobile Login Request (Accept / Deny)

1. On the VPN login screen, enter the username
2. Enter the password
   - The VPN waits for RADIUS to respond
3. In the Login Request screen on the mobile app, tap Accept or Deny
   - a response entry field is not presented
Password + Time-based Passcode or 2-Factor Challenge Options

1. On the VPN login screen, enter the username

2. Enter the password

3. The response screen prompts for one of two options
   a. Entry of a time-based passcode (TOTP)
   b. Entry of a number corresponding to an available 2-Factor Authentication method
      
      1 = SMS / Text Message
      2 = Phone
      3 = Email
      4 = Send Passcode to Phone (Push Notification)
      5 = Send Login Request to Phone (Push-to-Accept)

4. Make the appropriate entry
   
   For option ‘a’ above, enter the time-based passcode in the response screen
   
   For option ‘b’ above, enter number in the response screen, and then proceed with the 2nd Authentication Factor workflow
   
   if option 5 is entered, the VPN waits for RADIUS to respond
   
   When the Login Request screen appears on the mobile app, tap Accept or Deny on the screen – a response entry field is not presented
Optional Feature: Adaptive Authentication

If Adaptive Authentication is used with the user group check feature enabled, RADIUS responds accordingly in these login failure scenarios:

<table>
<thead>
<tr>
<th>Login failure scenario</th>
<th>End-user experience from RADIUS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hard stop</td>
<td>Login Failed message delivered</td>
</tr>
<tr>
<td>Step up authentication</td>
<td>Prompt received for 2nd Authentication Factor</td>
</tr>
<tr>
<td>Step down authentication</td>
<td>2nd Authentication Factor skipped; login request fulfilled</td>
</tr>
<tr>
<td>Resume authentication</td>
<td>Prompt received for 2nd Authentication Factor</td>
</tr>
<tr>
<td>Post authentication</td>
<td>2nd Authentication Factor skipped; login request fulfilled</td>
</tr>
<tr>
<td>Redirection</td>
<td>Login Failed message delivered</td>
</tr>
<tr>
<td>No failure</td>
<td>Prompt received for 2nd Authentication Factor</td>
</tr>
</tbody>
</table>