

SecureAuth IdP RADIUS server v2.5 integration guide

Introduction

SecureAuth IdP RADIUS server lets you configure two-factor authentication login access to a VPN and remote resources via RADIUS. This optional component of the SecureAuth IdP product is typically installed on a stand-alone server or on a SecureAuth IdP appliance.

Using the RADIUS feature, enterprises can provide strong adaptive authentication for RADIUS clients, such as VPNs and other applications, that leverage RADIUS for two-factor authentication used with SecureAuth IdP.

See the [Release notes](#) to learn about new features, enhancements, [Resolved issues](#), and known issues.

See [SecureAuth IdP RADIUS server v2.4 integration guide](#) for information about the previous product release.

This document is organized into four parts:

1. Topics in this guide include:
 - [Prerequisites](#)
 - [Adaptive Authentication](#)
 - [SecureAuth IdP RADIUS server logs](#)
 - [Release notes](#)
 - [Related documentation](#)
2. Installation – see [Installation guide - v2.5 - SecureAuth IdP RADIUS server](#)
3. Configuration – see [Configuration guide - v2.5 - SecureAuth IdP RADIUS server](#)
4. End-user experience – see [End-user experience - v2.5 - SecureAuth IdP RADIUS server](#)

Prerequisites

- SecureAuth IdP version 9.1 or later
- [Authentication API \(v9.1+\)](#) configured and enabled on the realm

Supported SecureAuth IdP components and integrated components

SecureAuth IdP features	SecureAuth IdP version	Configuration notes
Adaptive Authentication	v9.1+	Configure threat checking for: <ul style="list-style-type: none">• User Groups – See Adaptive Authentication for RADIUS responses with user group checking enabled.• End-user Client IPs – Cisco, NetScaler, and Palo Alto Networks platforms only.
Push-to-Accept	v9.1+	
Attribute Mapping	v9.1+	Configure and enable Identity Management API (v9.1+) on the realm to grant / deny end-user logon access. Group based authentication – Optionally configure Membership Connection Settings to grant / deny logon access: <ul style="list-style-type: none">• Specify the name of the user group to be granted / denied access, or• Designate a Property from Profile Fields to identify the user group to be granted / denied access.
UPN Logon	v9.1+	
Multi-Factor Authentication methods	SecureAuth IdP version	SecureAuth IdP v9.x supported server and required components
Time-based One-Time Passcode (TOTP)	v9.1+	NetMotion Wireless VPN: <ul style="list-style-type: none">• PEAP protocol support requirements:<ul style="list-style-type: none">• Public or private certificate• .PFX file• Private Key and Private Key Password• Microsoft Visual C++ requirements:<ul style="list-style-type: none">• Redistributable for Visual Studio 2012 Update 4 installed on the Windows server on which SecureAuth IdP RADIUS server is deployed
HMAC-based One-Time Passcode (HOTP)	v9.1+	
SMS (OTP only)	v9.1+	
Phone	v9.1+	
Email (OTP only)	v9.1+	NOTE: Refer to the NetMotion Mobility RADIUS configuration guide .

Passcode OTP (Push Notification)	v9.1+
Mobile Login Request	v9.1+
PIN	v9.1+

Supported platforms

Server:

- Windows Server 2008 R2
- Windows Server 2012 R2
- Windows Server 2016

Protocols:

- PAP
- PEAP (NetMotion only)
- MS-CHAPv2

SecureAuth IdP Adaptive Authentication IP Checking feature:

Platform	RADIUS end user IP
Cisco Systems	Calling-Station-Id
Citrix NetScaler	Calling-Station-Id
Juniper Networks	Tunnel-Client-Endpoint
Palo Alto Networks	PaloAlto-Client-Source-IP

Port settings

Inbound:

- Allow RADIUS Listener – Default is UDP port 1812.
- Block TCP port 8088 – This port is used for the administrative web interface and should be blocked for security reasons.

RADIUS VPN and product support

Supported RADIUS clients:

- Checkpoint
- Cisco ASA with AnyConnect and Web Client
- Cisco IPSec
- Citrix NetScaler with Web Client
- F5
- Fortigate
- Juniper VPN (IVE, MAG)
- Pulse Secure thick client
- NetMotion Wireless VPN
- Palo Alto Networks
- SonicWall
- VMware Horizon HTML Access
- VMware Horizon View
- WatchGuard

Other compatible RADIUS clients include:

- Avocent
- Barracuda
- Microsoft Forefront

Contact SecureAuth Professional Services with inquiries.

To configure a Palo Alto Networks GlobalProtect VPN to send the client IP to SecureAuth IdP RADIUS server:

- See Palo Alto Networks GlobalProtect VPN Configuration Guide (RADIUS) (v9.1+).

RADIUS client configuration

Though not all RADIUS clients are configured in the same manner, the following basic connectivity parameters must be configured on RADIUS clients to be used with SecureAuth IdP:

- RADIUS server IP address.
- Shared secret to use between the RADIUS server and RADIUS client(s).
- Port 1812 to use for RADIUS authentication requests, and Port "0" for accounting when applicable or if used as the default port.
- Timeout value Retries value.
- Connection profile that will use the SecureAuth RADIUS authentication serverGroup policy of the connection profile to identify resources end-users can access once logged on the network.

NOTE: A valid certificate must be installed if using NetMotion Wireless VPN.

Sample RADIUS authentication server configuration:

Add Server dialog	SecureAuth IdP RADIUS Server information	Configuration notes
Name	RADIUS Server description name (friendly name)	This configuration enables the administrator to control static IP assignment of the VPN client via SecureAuth IdP and the RADIUS server.
RADIUS Server	IP Address or Name of the RADIUS Server	NOTE: SecureAuth IdP RADIUS server v2.5 can be configured to pass an IP address to the VPN for static IP assignment to the VPN client (for example: PC or Mac).
Authentication Port	1812	See SecureAuth IdP RADIUS Server Static IP Address Configuration Guide for step-by-step instructions.
Shared Secret	SecureAuth RADIUS Shared Secret	
Timeout	60 Seconds (recommended)	
Retries	3 (recommended)	

SecureAuth IdP RADIUS server v2.5 installation

Upgrade

If SecureAuth RADIUS v1.0.x is currently installed, review the **upgrade** instructions in the [Installation guide](#) *before* installing the newer version of RADIUS.

If SecureAuth IdP RADIUS server v2.0.x - v2.2.x is currently installed, use the **install** instructions in [Install SecureAuth IdP RADIUS server v2.5](#) to upgrade while retaining the current configuration settings.

If SecureAuth IdP RADIUS server v2.3.9 / v2.3.12 is currently installed, use the **install** instructions in [Install SecureAuth IdP RADIUS server v2.5](#) to upgrade while retaining the current configuration settings .

If SecureAuth IdP RADIUS server v2.4.x is currently installed, use the **install** instructions in [Install SecureAuth IdP RADIUS server v2.5](#) to upgrade while retaining the current configuration settings.

New installation

If installing SecureAuth IdP RADIUS server v2.5.x for the first time on the designated appliance, follow the **install** instructions in the installation guide.

SecureAuth IdP RADIUS logs for troubleshooting

See [SecureAuth IdP RADIUS server logs](#) for information about using the RADIUS logs for troubleshooting.

Adaptive Authentication

If Adaptive Authentication is used with the user group check feature enabled, RADIUS responds accordingly in these login failure scenarios based on the authentication workflow.

Note that the following workflows do not correlate exactly to the workflows in SecureAuth IdP. Some of the following workflows are not included in SecureAuth IdP "Login Screen Options" and vice versa. For example, RADIUS does not have an option for "Username only" (while SecureAuth IdP does) and SecureAuth IdP does not have an option for "PIN + OTP" (while RADIUS does).

- Workflow 1 = **Password | One-Time Passcode (TOTP/HOTP) or Second Factor**
- Workflow 2 = **Password & Mobile Login Request** (Approve / Deny)
- Workflow 3 = **Password Only**
- Workflow 4 = **One-Time Passcode (TOTP/HOTP) Only**

- Workflow 5 = **One-Time Passcode (TOTP/HOTP) / Password**
- Workflow 6 = **Password | One-Time Passcode (TOTP/HOTP)**
- Workflow 7 = **One-Time Passcode (TOTP/HOTP) | Password**
- Workflow 8 = **Username | Second Factor**
- Workflow 9 = **Username | Second Factor | Password**
- Workflow 10 = **PIN + TOTP**
- Workflow 11 = **Password & One-Time Passcode (TOTP/HOTP)**

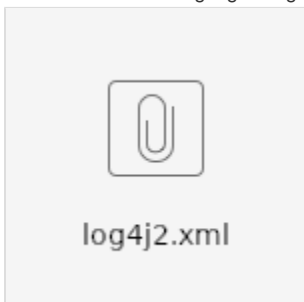
Login failure scenario	End-user experience from RADIUS -- Workflows 1, 2, 6, 7, 8, 9, 11	End-user experience from RADIUS -- Workflows 3, 4, 5, 10
Hard stop; refuse authentication request	Login failed message received	Login failed message received
Step up, require two-factor authentication	Prompt received for second authentication factor	Login request fulfilled
Step down, skip two-factor authentication	Second authentication factor skipped; login request fulfilled	Login request fulfilled
Resume authentication workflow	Prompt received for second authentication factor	Login request fulfilled
Skip to post-authentication	Second authentication factor skipped; login request fulfilled	Login request fulfilled
Redirect to realm or URL	Login failed message delivered	Login failed message received
No failure	Prompt received for second authentication factor	Login request fulfilled

SecureAuth IdP RADIUS server logs

Enable logs

Set up logs for the SecureAuth IdP RADIUS server by completing the following:

1. Download the following log configuration file, and place it in a temporary folder on the SecureAuth RADIUS server.



2. Rename **C:\idpRADIUS\bin\conf\log4j2.xml** so you can use it to disable logging when you finish debugging.

The paths you use might be different, depending on your RADIUS server version or the destination folder selected when you installed the RADIUS server. The following are examples of default paths:

- C:\idpRADIUS\bin\conf\log4j2.xml
 - C:\Program Files (x86)\SecureAuth Corporation\SecureAuth IdP RADIUS Agent\bin\conf\log4j2.xml
 - C:\Program Files\SecureAuth Corporation\SecureAuth IdP RADIUS Agent\bin\conf\log4j2.xml
3. Place the downloaded **log4j2.xml** file in the ***bin\conf** folder, which is the same folder used in step 2.
 4. Run the **services.msc** application, then restart the **SecureAuth RADIUS** service.
 5. Replicate the issue you have encountered.
 6. Find log files stored in ***bin\Logs\saRadiusServer.log**.
 7. Receive assistance with resolving the issue by forwarding log files to the SecureAuth Support team when you [create a support ticket](#).
 8. Restore the original **log4j2.xml** after debugging is completed.

Trace level logging uses a substantial amount of disk space and can create disk space issues over time.

Sample logs for different RADIUS failover scenarios

Failover to a SecureAuth IdP RADIUS backup server is configured under Step B: IdP Realms configuration, Add IdP Realm in the [Configuration guide - v2. 5 - SecureAuth IdP RADIUS server](#).

Failover scenario: Primary RADIUS server fails over to secondary RADIUS server which functions

```
[25/Oct/2018:13:18:16 -0700] ERROR    IdPAPIAccess: Primary IdP server failed:
https://secureauth.company.com/SecureAuth3. Checking failover servers.
[25/Oct/2018:13:18:16 -0700] INFO     IdPAPIAccess: Falling back to server: sa01.company.com
[25/Oct/2018:13:18:17 -0700] INFO     AuditLog: Start authentication session for user: user-
adm; NAS-IP: 123.45.67.89
[25/Oct/2018:13:18:17 -0700] DEBUG    RadiusLibFacade: sending response: id=230 type=Access-
Challenge
[25/Oct/2018:13:18:17 -0700] DEBUG    RadiusLibFacade: sending response: id=231 type=Access-
Challenge
[25/Oct/2018:13:18:17 -0700] DEBUG    RadiusLibFacade: sending response: id=232 type=Access-
Challenge
[25/Oct/2018:13:18:17 -0700] DEBUG    RadiusLibFacade: sending response: id=233 type=Access-
Challenge
[25/Oct/2018:13:18:18 -0700] DEBUG    RadiusLibFacade: sending response: id=234 type=Access-
Challenge
[25/Oct/2018:13:18:18 -0700] DEBUG    RadiusLibFacade: sending response: id=235 type=Access-
Challenge
[25/Oct/2018:13:18:18 -0700] INFO     SARadiusServer: GTCHandler has been called.
[25/Oct/2018:13:18:19 -0700] DEBUG    RadiusLibFacade: sending response: id=236 type=Access-
Challenge
[25/Oct/2018:13:18:39 -0700] INFO     SARadiusServer: GTCHandler has been called.
[25/Oct/2018:13:18:39 -0700] DEBUG    RadiusLibFacade: sending response: id=237 type=Access-
Challenge
[25/Oct/2018:13:18:40 -0700] DEBUG    RadiusLibFacade: sending response: id=238 type=Access-
Accept
[25/Oct/2018:13:18:40 -0700] INFO     AuditLog: Granted access to user: user-adm; NAS-IP:
123.45.67.89
```

Failover scenario: Primary RADIUS server fails over to other RADIUS servers, none of which are functioning

```
[25/Oct/2018:14:22:27 -0700] INFO    AuditLog: Abandoned previous session for user: user-adm;
NAS-IP: 123.45.67.89
[25/Oct/2018:14:22:27 -0700] ERROR  IdPAPIAccess: Primary IdP server failed:
https://secureauth.company.com/SecureAuth3. Checking failover servers.
[25/Oct/2018:14:22:28 -0700] INFO    AuditLog: Start authentication session for user: user-
adm; NAS-IP: 123.45.67.89
[25/Oct/2018:14:22:28 -0700] DEBUG  RadiusLibFacade: sending response: id=6 type=Access-
Challenge
[25/Oct/2018:14:22:28 -0700] DEBUG  RadiusLibFacade: sending response: id=7 type=Access-
Challenge
[25/Oct/2018:14:22:28 -0700] DEBUG  RadiusLibFacade: sending response: id=8 type=Access-
Challenge
[25/Oct/2018:14:22:28 -0700] DEBUG  RadiusLibFacade: sending response: id=9 type=Access-
Challenge
[25/Oct/2018:14:22:28 -0700] DEBUG  RadiusLibFacade: sending response: id=10 type=Access-
Challenge
[25/Oct/2018:14:22:28 -0700] DEBUG  RadiusLibFacade: sending response: id=11 type=Access-
Challenge
[25/Oct/2018:14:22:29 -0700] INFO    SARadiusServer: GTCHandler has been called.
[25/Oct/2018:14:22:29 -0700] INFO    IdPAPIAccess: Password authentication failed: invalid;
message: AppId is unknown.
[25/Oct/2018:14:22:29 -0700] INFO    PasswordState: User/Password verification failed for
user: user-adm.
[25/Oct/2018:14:22:29 -0700] DEBUG  RadiusLibFacade: sending response: id=12 type=Access-
Reject
[25/Oct/2018:14:22:29 -0700] INFO    AuditLog: Denied access request by user: user-adm; NAS-
IP: 123.45.67.89
```

Failover scenario: Primary RADIUS server fails over to secondary server which fails, but failover attempt to third server is successful

```

[25/Oct/2018:14:30:55 -0700] ERROR IdPAPIAccess: Primary IdP server failed:
https://secureauth.company.com/SecureAuth3. Checking failover servers.
[25/Oct/2018:14:30:55 -0700] INFO IdPAPIAccess: Falling back to server: sa01.secureauth.com
[25/Oct/2018:14:30:56 -0700] INFO AuditLog: Start authentication session for user: user-
adm; NAS-IP: 123.45.67.89
[25/Oct/2018:14:30:56 -0700] DEBUG RadiusLibFacade: sending response: id=13 type=Access-
Challenge
[25/Oct/2018:14:30:56 -0700] DEBUG RadiusLibFacade: sending response: id=14 type=Access-
Challenge
[25/Oct/2018:14:30:56 -0700] DEBUG RadiusLibFacade: sending response: id=15 type=Access-
Challenge
[25/Oct/2018:14:30:56 -0700] DEBUG RadiusLibFacade: sending response: id=16 type=Access-
Challenge
[25/Oct/2018:14:30:57 -0700] DEBUG RadiusLibFacade: sending response: id=17 type=Access-
Challenge
[25/Oct/2018:14:30:57 -0700] DEBUG RadiusLibFacade: sending response: id=18 type=Access-
Challenge
[25/Oct/2018:14:30:57 -0700] INFO SARadiusServer: GTCHandler has been called.
[25/Oct/2018:14:30:57 -0700] DEBUG RadiusLibFacade: sending response: id=19 type=Access-
Challenge
[25/Oct/2018:14:31:18 -0700] INFO SARadiusServer: GTCHandler has been called.
[25/Oct/2018:14:31:18 -0700] DEBUG RadiusLibFacade: sending response: id=20 type=Access-
Challenge
[25/Oct/2018:14:31:18 -0700] DEBUG RadiusLibFacade: sending response: id=21 type=Access-
Accept
[25/Oct/2018:14:31:18 -0700] INFO AuditLog: Granted access to user: user-adm; NAS-IP:
123.45.67.89

=====
Primary IdP Host:
secureauth.company.com
Backup IdP Host:
secureauth2.company.com,sa01.secureauth.com

```

Release notes

New features and enhancements

Version: 2.5

Release Date: April 23, 2019

Compatibility: SecureAuth IdP versions 9.0 - 9.3

RAD-83	A warning is displayed when an installation of an older version of RADIUS is attempted while a newer version is installed.
RAD-150	End-users' phone numbers and email addresses displayed in authentication applications are hidden consistently with asterisks.
RAD-218	TOTP and HOTP with YubiKey as second factor is supported in RADIUS version 2.5.1.
RAD-237	RADIUS client user interface and documentation were refreshed with the latest brand logo and color.
RAD-238	SecureAuth RADIUS supports Windows Server 2016.

Resolved issues

RAD-179	SonicWall NetExtender created a hotfix to resolve a RADIUS client problem with 2FA methods. All 2FA methods are available.
RAD-202	Editing and saving a disabled realm no longer enables the realm.
RAD-204	The Static Value field is empty by default in the RADIUS Client tab, in the Static Value Mapping section.

RAD-206	The Static Value field allows up to 247 characters in the RADIUS Client tab, in the Static Value Mapping section.
RAD-208	Uppercase letters are allowed in the Static Value field, in the RADIUS Client tab, in the Static Value Mapping section.
RAD-212	Clicking the context-sensitive help (small i) over a disabled client setting shows information for disabled clients in the RADIUS Client tab.
RAD-249	Numerous minor bug fixes were completed.
RAD-252	When creating a RADIUS client and clicking the Add Attribute button, the client is no longer saved when the Add Client button is not selected.
RAD-253	RADIUS client attribute values are restricted to the supported RADIUS protocol length of 253 bytes.

Known issues

RA D- 210	<p>When running the RADIUS client with the Pulse Secure client and 2FA options, Pulse Secure limits the maximum number of characters to 210. End-users can see all options in the Pulse Secure web client when the number of characters is less than 210.</p> <p>A second Pulse Secure limitation causes options 5 - 8 to be cut off from end-users' view on the 2FA list. End-users can select options 5 - 8, even though they are off-screen and there is no scrollbar.</p> <p>Optionally, modify text in the RADIUS uiTextsBundle.properties configuration file to shorten messages from the multi-factors message. See "Modify text showing on client user interface during login" in Configuration guide - v2.5 - SecureAuth IdP RADIUS server.</p>
RA D- 485	<p>Invalid characters in user IDs sent to the RADIUS server cause a RADIUS server failure.</p> <p>Workaround: Ensure that user IDs contain the following valid characters only:</p> <ul style="list-style-type: none"> • A - z • 0 - 9 • . (dot), - (minus sign), @ (domain), and _ (underscore)

Version 2.4 - Release Date: October, 2018

New features and enhancements

Version: 2.4

Compatibility: SecureAuth IdP versions 8.2 - 9.2

---	IdP realms and RADIUS clients can be disabled and enabled.
RAD-13	Authentication workflow names are standardized for consistency with IdP naming conventions.
RAD-44	Additional logging is available for Adaptive Authentication steps.
RAD-58	Text hints appear on the IdP Realm page.
RAD-91	Toggling is available on RADIUS clients page to enter either a NAS-IP or client IP address.
RAD-107	Single page workflow was added for Username, Second Factor, and Password.
RAD-110	Wild cards are supported when defining RADIUS client IP values.
RAD-143	One or more backup IdP hosts can be specified for failover functionality.
RAD-147	PIN + TOTP end-user workflow was added.

Resolved issues

RAD-215	Custom API header with millisecond-precision dates now works with SecureAuth IdP version 9.2
---------	--

Next step...

[Install SecureAuth IdP RADIUS server v2.5](#)

Related documentation

[Installation guide - v2.5 - SecureAuth IdP RADIUS server](#)

[Configuration guide - v2.5 - SecureAuth IdP RADIUS server](#)

[End-user experience - v2.5 - SecureAuth IdP RADIUS server](#)

Prior version

[SecureAuth IdP RADIUS server v2.4 integration guide](#)

[Installation guide - v2.4 - SecureAuth IdP RADIUS server](#)

[Configuration guide - v2.4 - SecureAuth IdP RADIUS server](#)

[End-user experience - v2.4 - SecureAuth IdP RADIUS server](#)