

# Checkpoint Integration

## PINsafe to Checkpoint Gaia

### Integration Notes

## Contents

- 1 Overview
- 2 Baseline
- 3 Prerequisites
- 4 Gaia Configuration
  - ◆ 4.1 Enabling RADIUS Authentication in Gaia
- 5 Customising the Gaia Login Page
  - ◆ 5.1 Test the RADIUS authentication
- 6 Swivel Configuration
  - ◆ 6.1 Configuring the RADIUS server
  - ◆ 6.2 Enabling Session creation with username
  - ◆ 6.3 Setting up Swivel Dual Channel Transports
- 7 Testing
- 8 Troubleshooting
- 9 Additional Information

## Overview

Swivel can provide strong and two factor authentication to the Checkpoint Gaia. This document outlines the details required to carry this out.

## Baseline

Swivel 4.x

Checkpoint Gaia appliance version R77.30.

## Prerequisites

Working Checkpoint, smart console

Swivel 4.x

Note that modifications to the Connectra login page will affect ALL users (but not the administration page).

Use of the [TURing](#), Security String Index or [SMS](#) Confirmed message will require the use of a NAT.

When a Swivel appliance VIP is used, the real IP address should be used and not the VIP. For redundancy select Primary and Secondary RADIUS servers, see [VIP on PINsafe Appliances](#).

## Gaia Configuration

### Enabling RADIUS Authentication in Gaia

You need to configure Swivel as an authentication server on the Gaia appliance.

- Open Smart Dashboard and log in.
- Under Network and Resources -> Hosts, configure the Swivel server as a new host. You just need to give it a name and add the IP address.
- Under Users and Authentication -> Authentication -> RADIUS Servers, create a new RADIUS server. Select Swivel as the host, ?NEW-RADIUS? as the service, and enter the shared secret you previously set on the Swivel server. You can select RADIUS version 1 or 2, and PAP or MSChap as the protocol: Swivel will detect these protocols automatically. Note: When a Swivel appliance VIP is used, the real IP address should be used and not the VIP. For redundancy select Primary and Secondary RADIUS servers, see [VIP on PINsafe Appliances](#).

You will also need to configure authentication for the relevant users. The simplest way to handle this is to create a new user group containing all users that will be using Swivel (if you do not already have one):

- Go to Users and Authentication -> Internal Users -> User Groups.
- Then under User Templates, create a new template, or modify an existing one, containing the relevant group, and set the authentication to RADIUS, using the Swivel server.

Don't forget to save and install the policy once you have made all relevant changes.

## Customising the Gaia Login Page

**NOTE:** it is assumed here that you are familiar with Unix commands, in particular with the vi editor, as you will need to edit a file.

**NOTE:** There is an example [LoginPage.php](#) available which is the Login.php file with the modifications already included. This can be used for reference but may not be 100% suitable for specific installations and different Gaia versions.

## Test the RADIUS authentication

At this stage it should be possible to authenticate by SMS, hardware Token, Mobile Phone Client and Taskbar to verify that the RADIUS authentication is working for users. Browse to the SSL VPN login page, and enter Username and if being used, the password. From the Swivel Administration console select User Administration and the required user then View Strings, and select an appropriate authentication string or OTC for the user. At the SSL VPN login enter the required OTC. Check the Swivel logs for a RADIUS success or rejected message. If no RADIUS message is seen, check that the Swivel RADIUS server is started and that the correct ports are being used.

10.10.110.72 - Check Point SmartDashboard R77.30 - Mobile Access

Install Policy SmartConsole

Firewall Application & URL Filtering Data Loss Prevention IPS Threat Prevention Anti-Spam & Mail Mobile Access IPsec VPN

### Overview

Mobile Access allows your employees to securely read email and connect to intranet sites using a mobile device or web browser.

#### My Organization

1 Security Gateway is allowing Mobile Access [Add Gateway...](#)

	IP Address	Web	Mobile	Desktop	Compliance
VLABFWL002	10.10.110.72	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	N/A

#### Users and Policy

Active Sessions on Gateway/s:

Users

10  
9  
8  
7  
6  
5  
4  
3  
2  
1  
0

19:54:00 19:54:30 19:55:00 19:55:30 19:56:00 19:56:30 19:57:00 19:57:30

Network Objects

- Check Point
  - VLABFWL002
    - Nodes
    - Networks
      - CP\_default\_Office\_Mode\_addresses
    - Groups
    - Address Ranges
    - Dynamic Objects

- Overview
- Policy
- Gateways
- Applications
- Authentication
- Client Certificates
- Portal Settings
- IPS
- Endpoint Security On Demand
- Capsule Workspace Settings
- Additional Settings

## Overview

Mobile Access allows your employees to securely read email and connect to intranet sites using a mobile device or web browser.

### My Organization



1 Security Gateway is allowing

VLABFWL002

IP Address

10.10.110.72

### Users and Policy

Active Sessions on Gateway/s: All Gateways

10  
9  
8  
7  
6  
5  
4  
3  
2  
1  
0

Users

19:54:00 19:54:30 19:55:00 19:55:30 19:56:00 19:56:30 19:57:00 19:57:30



#### Network Objects

- Check Point
  - VLABFWL002
- Nodes
- Networks
  - CP\_default\_Office\_Mode\_addresses
- Groups
- Address Ranges
- Dynamic Objects

### Check Point Gateway - VLABFWL002

#### General Properties

- Topology
- NAT
- HTTPS Inspection
- HTTP/HTTPS Proxy
- Platform Portal
- VPN Clients
- Mobile Access
  - Authentication
  - Office Mode
  - Portal Customization
  - Portal Settings
  - SSL Clients
  - HTTP Proxy
  - Name Resolution
  - Link Translation
  - Endpoint Compliance
  - Check Point Security
- Logs
  - Optimizations
  - Hit Count
- Other

#### Check Point Gateway - General

##### Machine

Name: VLABFWL002  
IPv4 Address: 10.10.110.72  
IPv6 Address:  
Comment:

##### Secure Internal Communication

Communication... Certificate

##### Platform

Hardware: Open server

##### Software Blades

Network Security Blades: SG

Network Security (2) Manage

- ☒ Firewall
- ☐ IPsec VPN
  - ☐ Policy Server
- ☒ Mobile Access
- ☐ IPS
- ☐ Anti-Bot
- ☐ Anti-Virus
- ☐ Anti-Spam & Email Security
- ☐ Identity Awareness
- ☐ Monitoring

- Overview
- Policy
- Gateways
- Applications
- Authentication
- Client Certificates
- Portal Settings
- IPS
- Endpoint Security On Demand
- Capsule Workspace Settings
- Additional Settings

## Overview

Mobile Access allows your employees to securely read email and connect to intranet sites using a mobile device or web browser.

### My Organization



1 Security Gateway is allowing

VLABFWL002

IP Address

10.10.110.72

### Users and Policy

Active Sessions on Gateway/s: All Gateways

10  
9  
8  
7  
6  
5  
4  
3  
2  
1  
0

Users

19:54:30 19:55:00 19:55:30 19:56:00 19:56:30 19:57:00 19:57:30

Check Point Gateway - VLABFWL002

- General Properties
- Topology
- NAT
- HTTPS Inspection
- HTTP/HTTPS Proxy
- Platform Portal
- VPN Clients
- Mobile Access
  - Authentication
  - Office Mode
  - Portal Customization
  - Portal Settings
  - SSL Clients
  - HTTP Proxy
  - Name Resolution
  - Link Translation
  - Endpoint Compliance
  - Check Point Security
- Logs
  - Optimizations
  - Hit Count
  - Other

### Authentication for Mobile Access

Authentication Method

- ☐ Defined on user record (Legacy)
- ☐ Username and password
- ☒ RADIUS
- ☐ SecurID
- ☐ Personal certificate

Two-Factor Authentication: 0 object(s)

- ☒ Global setting
- ☐ Custom settings

☒ Allow DynamicID for mobile

Certificate Authentication for mobile

- ☐ Require client certificate when connecting to intranet
- ☐ Require client certificate when connecting to Internet



- Overview
- Policy
- Gateways
- Applications
- Authentication
- Client Certificates
- Portal Settings
- IPS
- Endpoint Security On Demand
- Capsule Workspace Settings
- Additional Settings

## Overview

Mobile Access allows your employees to securely read email and connect to intranet sites using a mobile device or web browser.

### My Organization



1 Security Gateway is allowing

IP Address

VLABFWL002

10.10.110.72

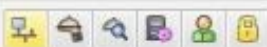
### Users and Policy

Active Sessions on Gateway/s: All Gateways

10  
9  
8  
7  
6  
5  
4  
3  
2  
1  
0

Users

19:54:30 19:55:00 19:55:30 19:56:00 19:56:30 19:57:00 19:57:30 19:58:00



#### Network Objects

- Check Point
  - VLABFWL002
- Nodes
- Networks
  - CP\_default\_Office\_Mode\_addresses
- Groups
- Address Ranges
- Dynamic Objects

Check Point Gateway - VLABFWL002

- General Properties
  - Topology
  - NAT
  - HTTPS Inspection
  - HTTP/HTTPS Proxy
  - Platform Portal
- VPN Clients
- Mobile Access
  - Authentication
  - Office Mode
  - Portal Customization
  - Portal Settings
  - SSL Clients
  - HTTP Proxy
  - Name Resolution
  - Link Translation
  - Endpoint Compliance
  - Check Point Security
- Logs
  - Optimizations
  - Hit Count
- Other

### Authentication for Mobile Access

Authentication Method

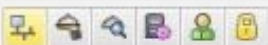
- ☐ Defined on user record (Legacy)
- ☐ Username and password

#### RADIUS Server Properties -

General Accounting

Name: SwivelCloud  
Comment:  
Color: Black  
Host:  
Service: UDP RADIUS  
Shared Secret:  
Version: RADIUS V  
Protocol: PAP  
Priority: 1

- Overview
- Policy
- Gateways
- Applications
- Authentication
- Client Certificates
- Portal Settings
- IPS
- Endpoint Security On Demand
- Capsule Workspace Settings
- Additional Settings



## Network Objects

- Check Point
  - VLABFWL002
- Nodes
- Networks
  - CP\_default\_Office\_Mode\_addresses
- Groups
- Address Ranges
- Dynamic Objects

## Overview

Mobile Access allows your employees to securely read email and connect to intranet sites using a mobile device or web browser.

## My Organization



1 Security Gateway is allowing

	IP Address
VLABFWL002	10.10.110.72

Host Node - demo.swivelcloud.com

- General Properties
- Topology
- NAT
- FireWall-1 GX
- Other

## Host Node - General Properties

## Machine

Name: demo.swivelcloud.com  
IPv4 Address: 52.18.78.73  
IPv6 Address:  
Comment:

## Products:

[Configure Servers...](#)

## Users and Policy

Active Sessions on Gateway/s: All Gateways

Users

19:54:30 19:55:00 19:55:30 19:56:00 19:56:30 19:57:00 19:57:30 19:58:00

- Overview
- Policy
- Gateways
- Applications
- Authentication
- Client Certificates
- Portal Settings
- IPS
- Endpoint Security On Demand
- Capsule Workspace Settings
- Additional Settings

## Overview

Mobile Access allows your employees to securely read email and connect to intranet sites using a mobile device or web browser.

### My Organization



1 Security Gateway is allowing

VLABFWL002

IP Address

10.10.110.72

### Users and Policy

Active Sessions on Gateway/s: All Gateways

10

9

8

7

6

5

4

3

2

1

0

Users

19:55:30

19:56:00

19:56:30

19:57:00

19:57:30

19:58:00

19:58:30

19:59:00



#### Network Objects

- Check Point
- VLABFWL002
- Nodes
- Networks
  - CP\_default\_Office\_Mode\_addresses
- Groups
- Address Ranges
- Dynamic Objects

Check Point Gateway - VLABFWL002

- General Properties
- Topology
- NAT
- HTTPS Inspection
- HTTP/HTTPS Proxy
- Platform Portal
- VPN Clients
- Mobile Access
  - Authentication
  - Office Mode
  - Portal Customization
  - Portal Settings
  - SSL Clients
  - HTTP Proxy
  - Name Resolution
  - Link Translation
  - Endpoint Compliance
  - Check Point Security
- Logs
  - Optimizations
  - Hit Count
- Other

### Authentication for Mobile Access

Authentication Method

- ☐ Defined on user record (Legacy)
- ☐ Username and password

#### RADIUS Server Properties -

General Accounting

Name: SwivelCloud

Comment:

Color: Black

Host: demo

Service: UDP NEW

Shared Secret: \*\*\*\*\*

Version: RADIUS V

Protocol: PAP

Priority: 1

- Overview
- Policy
- Gateways
- Applications
- Authentication
- Client Certificates
- Portal Settings
- IPS
- Endpoint Security On Demand
- Capsule Workspace Settings
- Additional Settings



## Network Objects

- Check Point
  - VLABFWL002
- Nodes
- Networks
  - CP\_default\_Office\_Mode\_addresses
- Groups
- Address Ranges
- Dynamic Objects

## Overview

Mobile Access allows your employees to securely read email and connect to intranet sites using a mobile device or web browser.

## My Organization



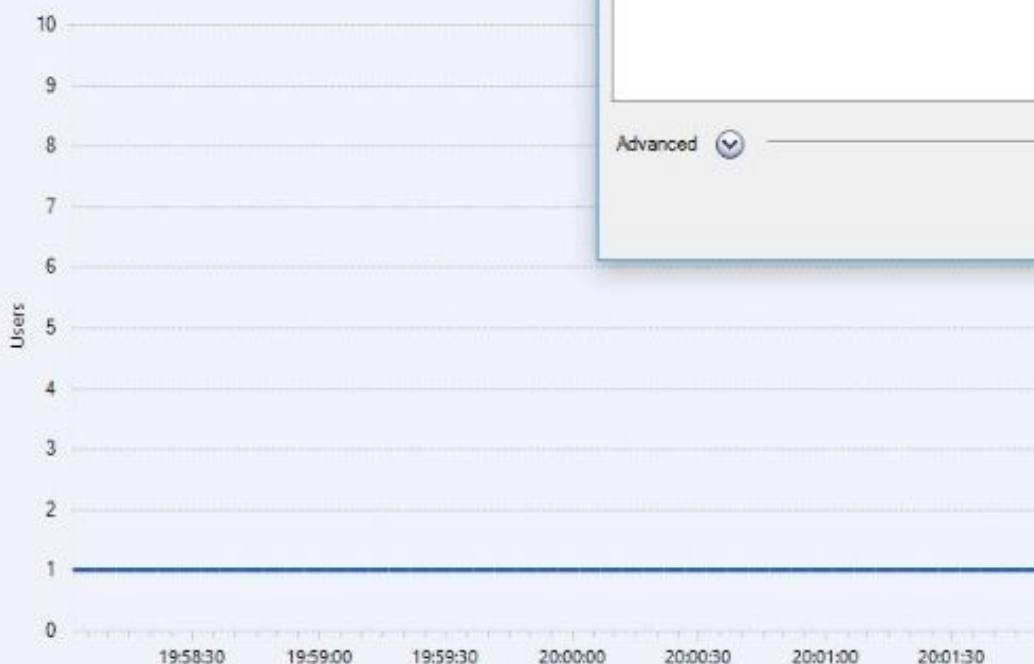
1 Security Gateway is allowing Mobile Access

Add Gateway...

	IP Address	Web	Mobile	Desktop	Compliance
VLABFWL002	10.10.110.72	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	N/A

## Users and Policy

Active Sessions on Gateway/s: All Gateways



## Install Policy



## Install Policy

1 gateway selected

Type to search



Select

Installation Targets

Network Security

VLABFWL002

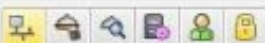


Advanced





- Overview
- Policy
- Gateways
- Applications
- Authentication
- Client Certificates
- Portal Settings
- IPS
- Endpoint Security On Demand
- Capsule Workspace Settings
- Additional Settings



## Network Objects

- Check Point
  - VLABFWL002
- Nodes
- Networks
  - CP\_default\_Office\_Mode\_addresses
- Groups
- Address Ranges
- Dynamic Objects

## Overview

Mobile Access allows your employees to securely read email and connect to intranet sites using a mobile device or web browser.

## My Organization



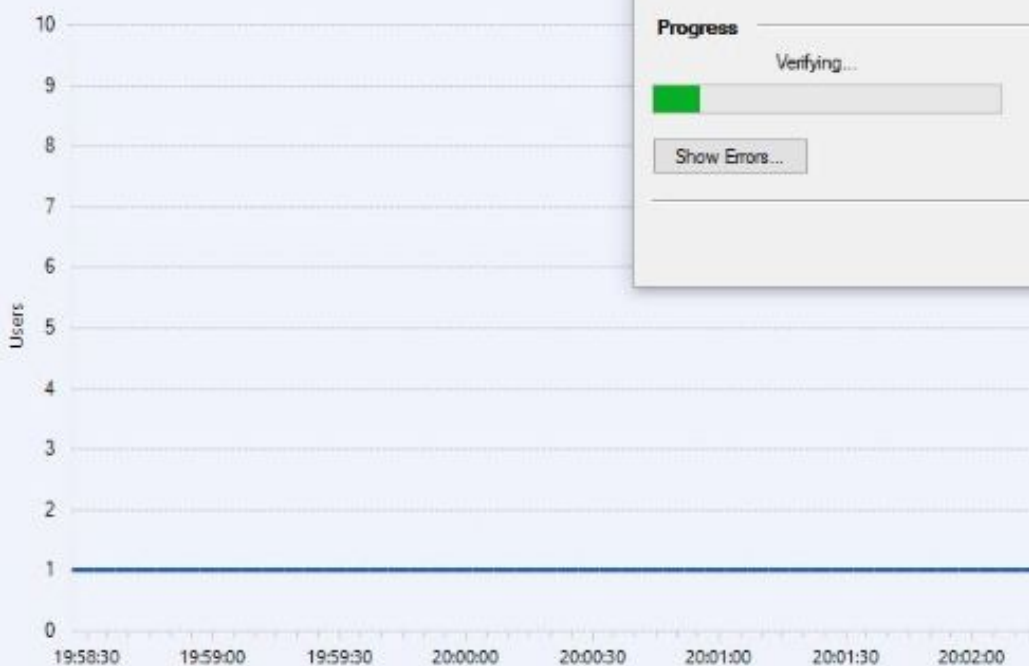
1 Security Gateway is allowing Mobile Access

Add Gateway...

	IP Address	Web	Mobile	Desktop	Compliance
VLABFWL002	10.10.110.72	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	N/A

## Users and Policy

Active Sessions on Gateway/s: All Gateways



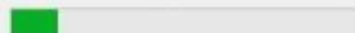
## Installation Process - Standard

## Installation

Installation Targets	Version	Network S
VLABFWL002	R77.30	Verify

## Progress

Verifying...



Show Errors...

10.10.110.72 - Check Point SmartDashboard R77.30 - Mobile Access

Install Policy SmartConsole

Firewall Application & URL Filtering Data Loss Prevention IPS Threat Prevention Anti-Spam & Mail Mobile Access IPSec VPN

Overview Policy Gateways Applications Authentication Client Certificates Portal Settings IPS Endpoint Security On Demand Capsule Workspace Settings Additional Settings

## Authentication

### Allowed Authentication Schemes on Gateways

Name	Check Point Password	SecurID
VLABFWL002	Allowed	Allowed

New... Edit... Delete

### Two-Factor Authentication with DynamicID

☐ Challenge users to provide the DynamicID one time password sent to their email account or mobile device via SMS.

SMS Provider and Email Settings

Specify the URL of your SMS provider, your email settings, or both. (See the online help for details and examples)

SMS provider and email settings:

SMS Provider Account Credentials (not necessary for email only):

Username:

Password:

Confirm password:

API ID:

Advanced...

RADIUS Server Properties - SwivelCloud

General Accounting

Name: SwivelCloud

Comment:

Color: Black

Host: demo.

Service: UDP NEW-I

Shared Secret:

Version: RADIUS V

Protocol: PAP

Priority: 1

Servers and OPSEC

- Servers
  - RADIUS
    - SwivelCloud
  - Trusted CAs
  - OPSEC Applications

Objects List Identity Awareness SmartWorkflow

## Swivel Configuration

### Configuring the RADIUS server

On the Swivel Administration console configure the RADIUS Server and NAS, see [RADIUS Configuration](#)

## Enabling Session creation with username


To allow the [TURING](#) image, [Pinpad](#) and other single channel images, under Server/Single Channel set [Allow session request by username](#) to Yes.

## Setting up Swivel Dual Channel Transports

See [Transport Configuration](#)

Swivel Administration Login

← → ↻ 🏠 Seguro | https://demo.swivelcloud.com:8080/sentry/



- [Login](#)

Swivel Administration Login

Username:

OTC:

Start Session

Login



- RADIUS>NAS
- 

NAS:

- Apply Reset



Swivel Configuration
What's My IP Address?

Seguro
https://demo.swivelcloud.com:8080/sentry/config/radius/nas

- Status
- Log Viewer
- Server
- Policy
- Logging
- Messaging
- Database
- Mode
- Repository
- RADIUS
  - Server
  - NAS
- Migration
- Windows GINA
- Appliance
- OATH
- Config Sync
- Reporting
- User Administration
- Save Configuration
- Upload Email Images
- Administration Guide
- Logout

## RADIUS>NAS

Please enter the details for any RADIUS network access servers. A NAS is

NAS:

- Juniper
- Netscaler
- CiscoASA
- Rob
- Watchguard
- Usbon\_Forti\_300C
- 


Identifier:	CheckPoint Dev
Hostname/IP:	89.114.238.196
Secret:	.....
Group:	---ANY---
EAP protocol:	
Authentication Mode:	
Vendor (Groups):	None
Change PIN warning:	No
Two Stage Auth:	No
Allow blank password at Stage One:	No
Send Security String after Stage One:	Yes
Even if User has Valid String:	Yes
Check password with repository:	No
Push Enabled:	No
Authenticate non-user with just password:	No
Username attribute for repository:	
Allow alternative usernames:	No
Alternative username attributes:	
OTC timeout (mins):	0
Internal IP ranges:	
Send username in challenge:	No

[New Entry](#)

Aguardar por demo.swivelcloud.com

## Testing

With the changes in place, when a user accesses the Gaia portal the will see the modified login page.

**Check Point™**  
SOFTWARE TECHNOLOGIES LTD.

Check Point Mob

Please enter your credentials

User name

OTC

TURing

1	2	3	4	5	6	7	8	9	0
5	4	6	7	8	1	3	0	2	9

Sign In

Language:

© Copyright 2004-2015 Check Point Software Technologies Ltd. All rights reserved.

After entering their username and either tabbing away from the username field or clicking the TURing button they will be presented with a TURing image. The PINsafe log should record a session start for that user.

The user can then use their PIN to extract their one-time code and enter this to authenticate. The PINsafe log show record the RADIUS dialogue associated with this authentication.

## Troubleshooting

Check the Swivel logs for Turing images and RADIUS requests.

- Swivel Log Viewer 10

Later

(sav

Filter: ALL 7

Search for:

Between

00:00:00

and

00:00:00

```
select date
```

```
select date
```

Events per page: 200

Apply

Reset

Timestamp	Level	
20:05:26 23/03/2017	INFO	RADIUS DEBUG: <191> Access-Reject(3) LEN=65 80
20:05:26 23/03/2017	INFO	RADIUS DEBUG: <191> ----- Pack Reject(3) 000: 03 BF 00 14 0D 08 61 B6 - 97 A0 0E 4 -----
20:05:26 23/03/2017	INFO	RADIUS DEBUG: <191> Access-Reject(3) LEN=65 80
20:05:26 23/03/2017	INFO	RADIUS: <191> Access-Request(1) LEN=65 89.114.2 AGENT_ERROR_USER_NOT_IN_GROUP
20:05:26 23/03/2017	INFO	RADIUS DEBUG: <191> Access-Request(1) LEN=65 8 AGENT_ERROR_USER_NOT_IN_GROUP
20:05:26 23/03/2017	INFO	From the IP Address 89.114.238.196 NAS ID Lisbon_1 repository to continue the authentication attempt.
20:05:26 23/03/2017	INFO	RADIUS: <191> Access-Request(1) LEN=65 89.114.3
20:05:26 23/03/2017	INFO	RADIUS DEBUG: <191> Access-Request(1) LEN=65 8
20:05:26 23/03/2017	INFO	RADIUS DEBUG: <191> ----- Pack Request(1) 000: 01 EF 00 41 0D 0F 90 B9 - 71 30 B1- 74 6F 72 02 12 3A 99 8D - 58 68 A8 AC 3F A1 23 57 Attributes: User-Name (1), Length: 15, Data: {admin 0x3A993D545B8BAC3FA1235716886E3581 Service-Ty 0x0A0A6E48 <191> -----
20:05:26 23/03/2017	INFO	RADIUS DEBUG: <191> Access-Request(1) LEN=65 8
20:05:21 23/03/2017	INFO	RADIUS DEBUG: <191> Access-Reject(3) LEN=65 80
20:05:21 23/03/2017	INFO	RADIUS DEBUG: <191> ----- Pack Reject(3) 000: 03 BF 00 14 0D 08 61 B6 - 97 A0 0E 4 -----
20:05:21 23/03/2017	INFO	RADIUS DEBUG: <191> Access-Reject(3) LEN=65 80

For assistance in the Swivel Secure installation and configuration please firstly contact your reseller and then email Swivel Secure support at [supportdesk@swivelsecure.com](mailto:supportdesk@swivelsecure.com)