

# 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.

The screenshot displays the Check Point SmartDashboard R77.30 interface for Mobile Access. The top navigation bar includes sections for Firewall, Application & URL Filtering, Data Loss Prevention, IPS, Threat Prevention, Anti-Spam & Mail, Mobile Access, and IPsec VPN. The left sidebar contains a navigation tree with categories like Overview, Policy, Gateways, Applications, Authentication, Client Certificates, Portal Settings, IPS, Endpoint Security On Demand, Capsule Workspace Settings, and Additional Settings. The main content area is titled "Overview" and includes a sub-section "My Organization" showing "1 Security Gateway is allowing Mobile Access" with an "Add Gateway..." button. Below this is a table of gateways:

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

The bottom section, "Users and Policy", features a dropdown menu for "Active Sessions on Gateway/s" set to "All Gateways". Below the dropdown is a line graph showing the number of active sessions over time. The y-axis is labeled "Users" and ranges from 0 to 10. The x-axis shows time from 19:54:00 to 19:57:00. A single horizontal line is plotted at the value of 1, indicating one active session throughout the period.

- 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.

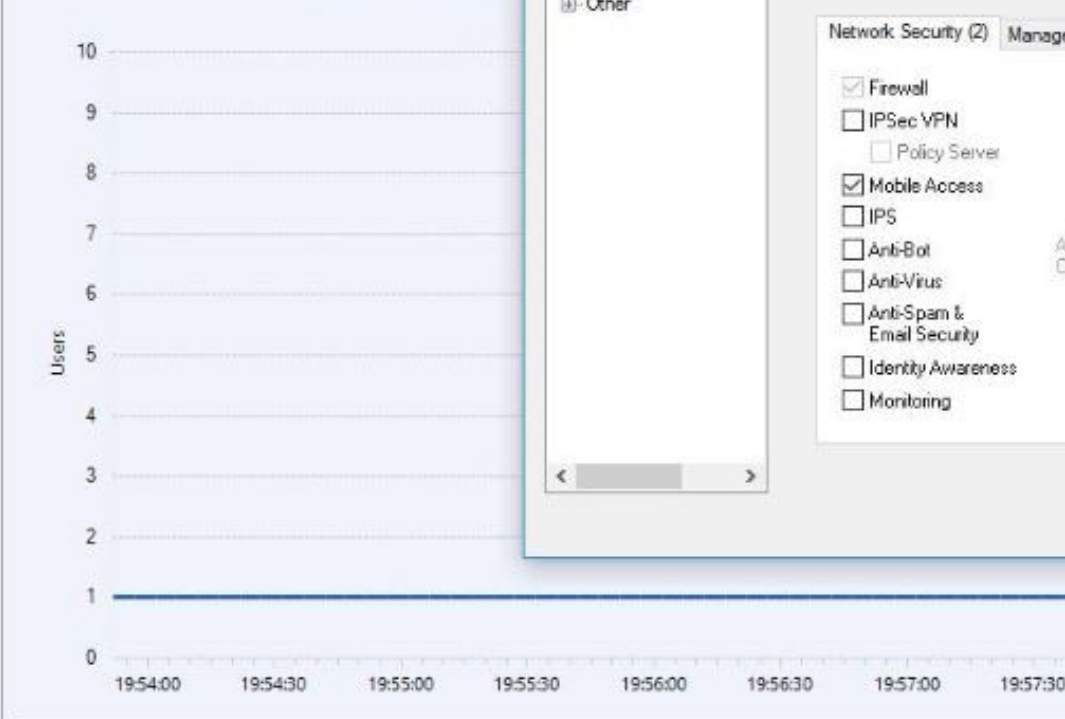
#### My Organization

1 Security Gateway is allowing

	IP Address
VLABFWL002	10.10.110.72

#### Users and Policy

Active Sessions on Gateway/s: All Gateways



#### 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

- 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.

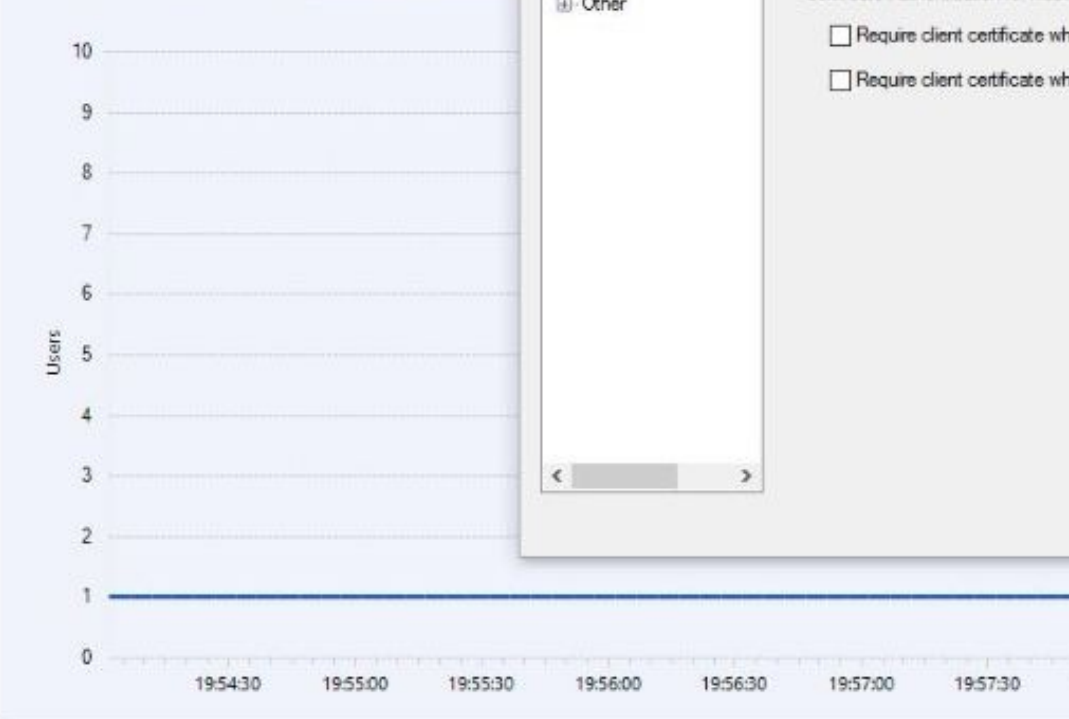
#### My Organization

1 Security Gateway is allowing

	IP Address
VLABFWL002	10.10.110.72

#### Users and Policy

Active Sessions on Gateway/s: All Gateways



#### 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 certificates

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

- #### 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

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



### 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 - SwivelCloud

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

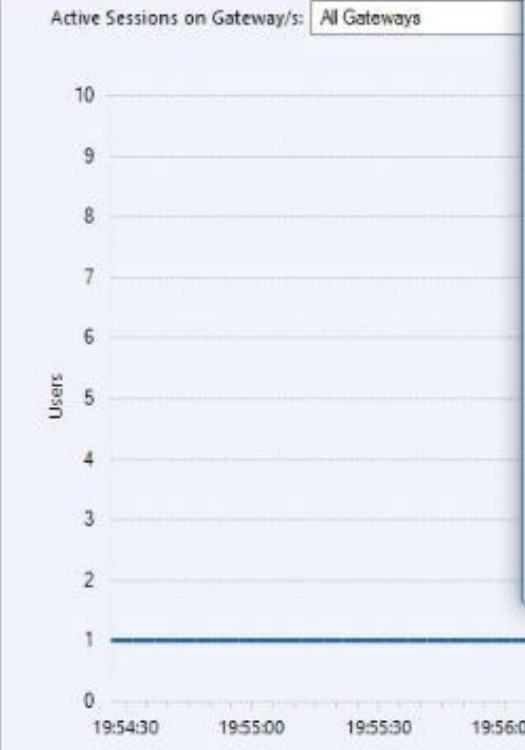
Mobile Access allows your employees to securely read email and connect to intranet sites using a mobile device or web browser.

### My Organization

1 Security Gateway is allowing

	IP Address
VLABFWL002	10.10.110.72

### Users and Policy



### Host Node - demo.swivelcloud.com

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

### Host Node - General Properties

Machine

Name:

IPv4 Address:

IPv6 Address:

Comment:

Products:

[Configure Servers...](#)

- 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.

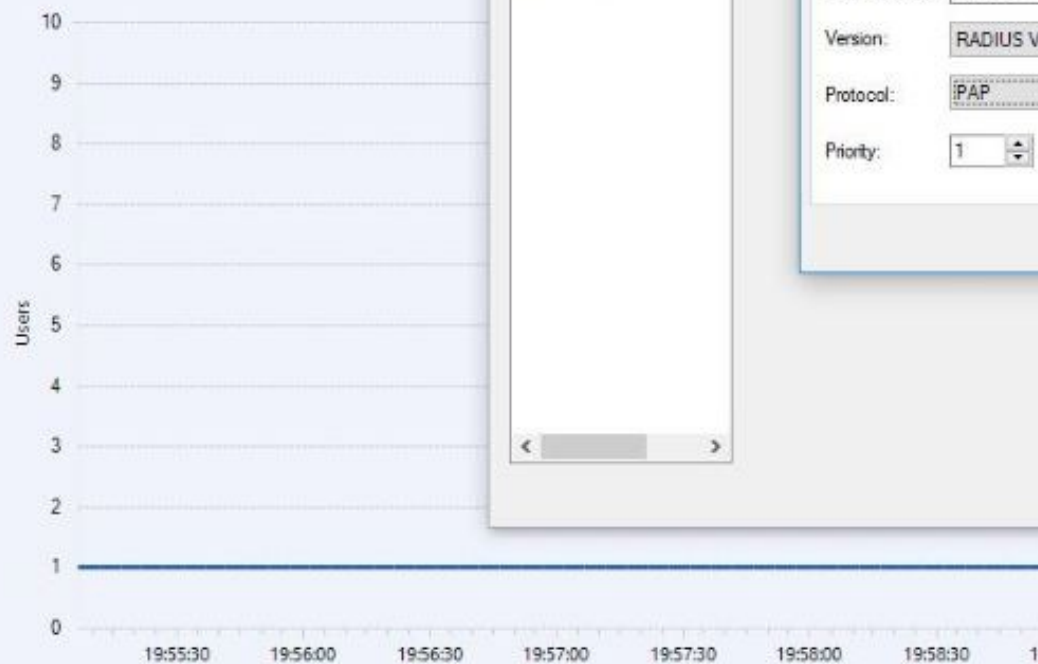
#### My Organization

1 Security Gateway is allowing

	IP Address
VLABFWL002	10.10.110.72

#### Users and Policy

Active Sessions on Gateway/s: All Gateways



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: IPAP

Priority: 1

- 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 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

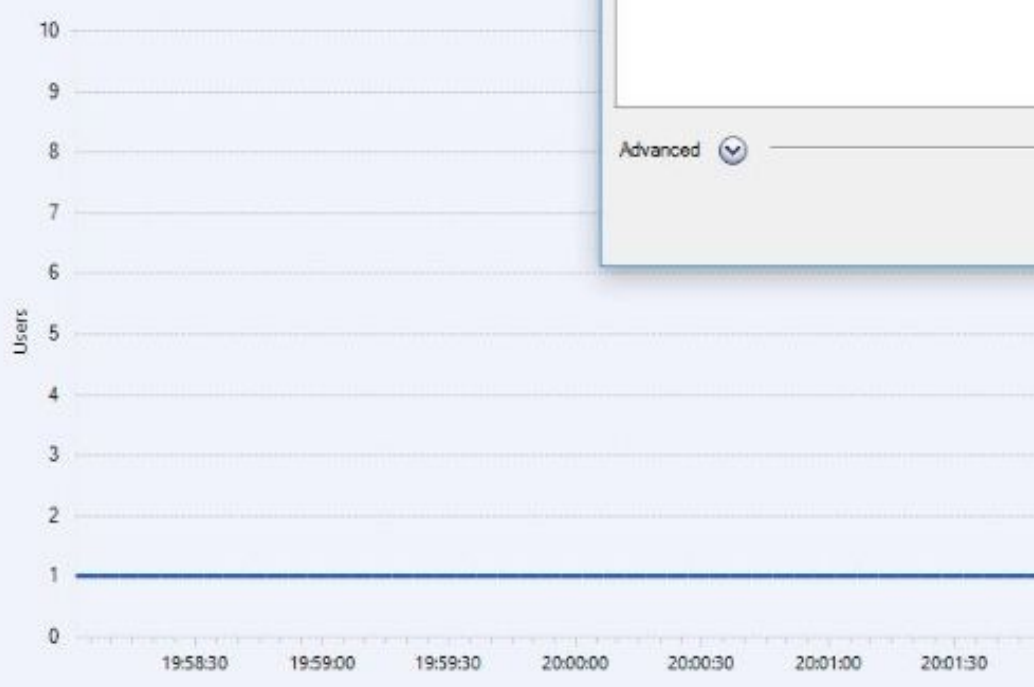
#### Install Policy

1 gateway selected

  
**Installation Targets**  
VLABFWL002   
**Network Security**

#### Users and Policy

Active Sessions on Gateway/s: All Gateways



- 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 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

Installation Process - Standard

#### Installation

Installation Targets	Version	Network S
VLABFWL002	R77.30	<a href="#">Verify</a>

<

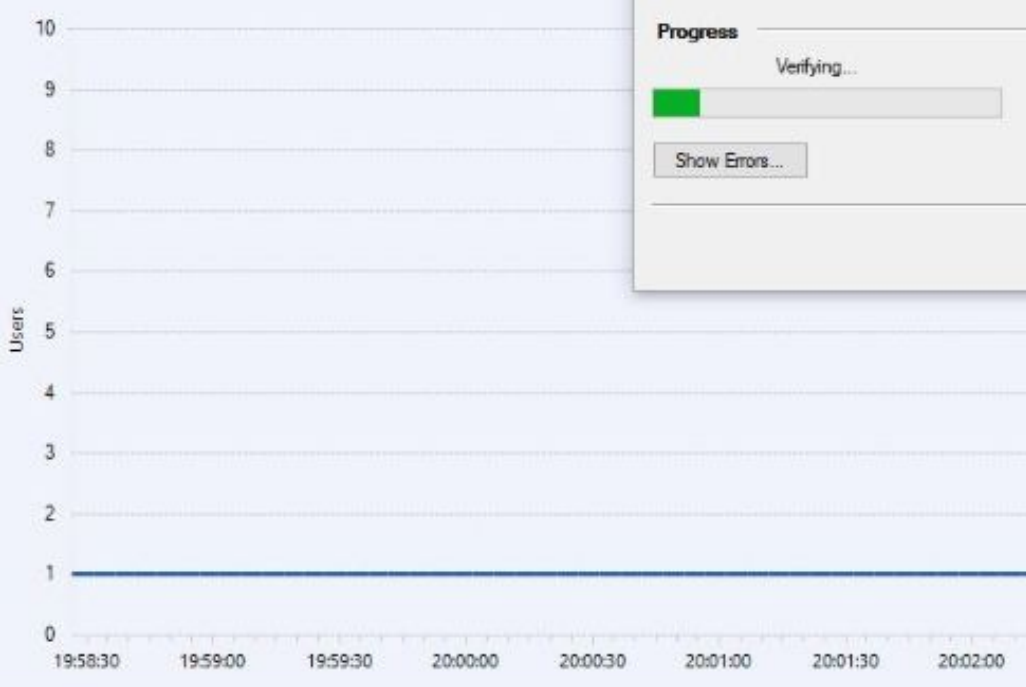
#### Progress

Verifying...

[Show Errors...](#)

#### Users and Policy

Active Sessions on Gateway/s:



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

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

General Accounting

Name: SwivelCloud

Comment:

Color: Black

Host: demo.

Service: UDP NEW-I

Shared Secret:

Version: RADIUS V

Protocol: PAP

Priority: 1

Objects List Identity Awareness SmartWorkflow

## Swivel Configuration

### Configuring the RADIUS server

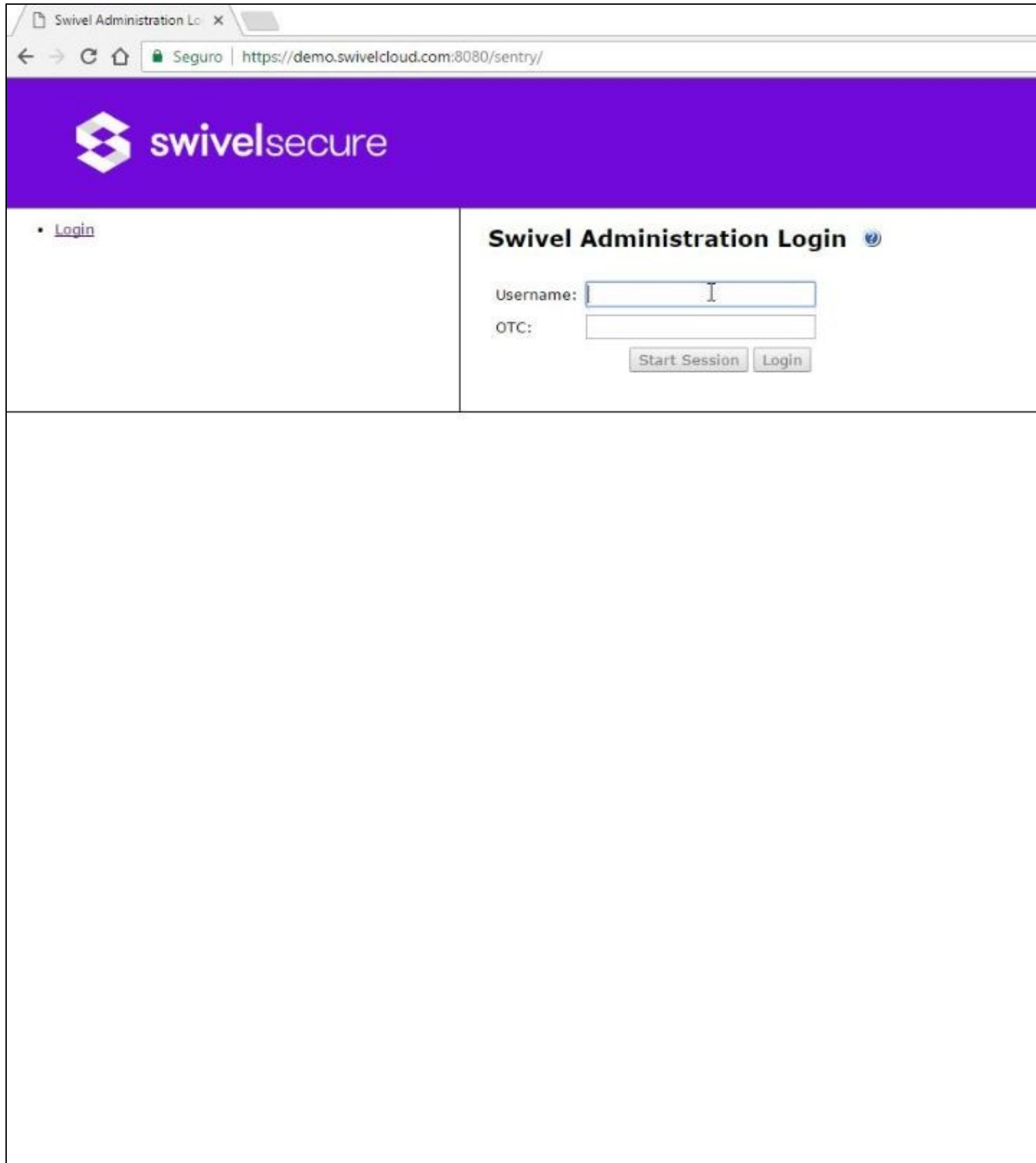
On the Swivel Administration console configure the RADIUS Server and NAS, see [RADIUS Configuration](#)

## 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/

 swivelsecure

- [Login](#)

### Swivel Administration Login

Username:

OTC:



- [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


NAS:

- ▣ [Juniper](#)
- ▣ [NetScaler](#)
- ▣ [CiscoASA](#)
- ▣ [Rob](#)
- ▣ [Watchguard](#)
- ▣ [Lisbon\\_Forti\\_300C](#)
- ▣ [New\\_Entry](#)



Swivel Configuration x What's My IP Address? | x

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](#)
- ▣ [Lisbon\\_Forti\\_300C](#)
- ▣

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

▣ [New Entry](#)

A aguardar por demo.swivelcloud.com

## Testing

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



Please enter your credentials

User name

user1

OTC

TURing



Sign In

Language: English

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 should record the RADIUS dialogue associated with this authentication.

## Troubleshooting

Check the Swivel logs for Turing images and RADIUS requests.

