Table of Contents

Table of Contents

1 Checkpoint Connectra Integration

PINsafe to Checkpoint Connectra

Integration Notes

2 Overview

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

3 Baseline

Swivel 3.x

Checkpoint Connectra appliance version NGX R66. Also tested with R70.

Checkpoint R75 Mobile Access login page

4 Prerequisites

Working Connectra VPN

Swivel 3.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.

5 Swivel Configuration

5.1 Configuring the RADIUS server

On the Swivel Administration console configure the RADIUS Server and NAS, see RADIUS Configuration

5.2 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.

5.3 Setting up Swivel Dual Channel Transports

See Transport Configuration

6 Connectra Configuration

6.1 Enabling RADIUS Authentication in Connectra

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

6.2 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.

7 Customising the Connectra 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 Connectra versions.

7.1 Login to the Connectra

To modify the Connectra login page, you need to log into the console, either physically on the appliance, or using a SSH terminal server such as Putty see PuTTY How To Guide. Switch into expert mode.

7.2 Locate the file LoginPage.php

Change directory to /opt/CPcvpn-R66/phpincs (note: the exact directory name CPcvpn-R** will vary depending on the Connectra revision number). Backup the file LoginPage.php by making a copy of it.

7.3 Edit the LoginPage.php

After making a backup copy, edit the file LoginPage.php.

First of all, search for the end of the page header, ?</HEAD>?. There should be a ?</script>? tag just before that. Insert the following just before the </script>:

```
function showTuring() {
turing = document.getElementById("imgTuring");
username = document.getElementById("userName").value;
turing.src = "https://pinsafe_server:8443/proxy/SCImage?username=" +username + "&random=" + Math.floor(Math.random()*100000);
turingRow = turing.parentNode.parentNode;
turingRow.style.display = "";
}
```

NOTE: you should replace "pinsafe_server" in the value of turing.src above with the actual internet-visible address of the Swivel instance.

For a Swivel virtual or hardware appliance: "https://pinsafe_server:8443/proxy/SCImage?username="

For a software only install see Software Only Installation

Now locate the input field with ID ?userName?.

Add the following attribute to the field: onblur="showTuring();". The complete line should appear as follows:

```
<input type="text" id="userName" name="userName" class="inputText" autocomplete="off" <?=$User_Read_Only?> style="<?=$User_Style_Var?>" value
```

Look for the second <tr> tag after this field. Insert the following before this tag:

```
<tr style="display:none"><td colspan="2" align="center">
<input type="button" value="<?= TURING ?>" onclick="showTuring();"><br>
<img src="" id="imgTuring" alt="<?= TURING ?>">
</td></tr>
```

You can now save the file.

7.4 Editing the password prompt

If you want to change the prompt for the password (e.g to prompt for One-Time Code), or to change the text displayed on the button that requests a new TURing image, you will need to edit the file Strings.en_US.php, or the appropriate Strings file for your local language (type ls Strings* to see what files are available). Locate the string ?PASSWORD?, and change the text within the quotes to the right of the => symbol to ?OTC?, or whatever you prefer.

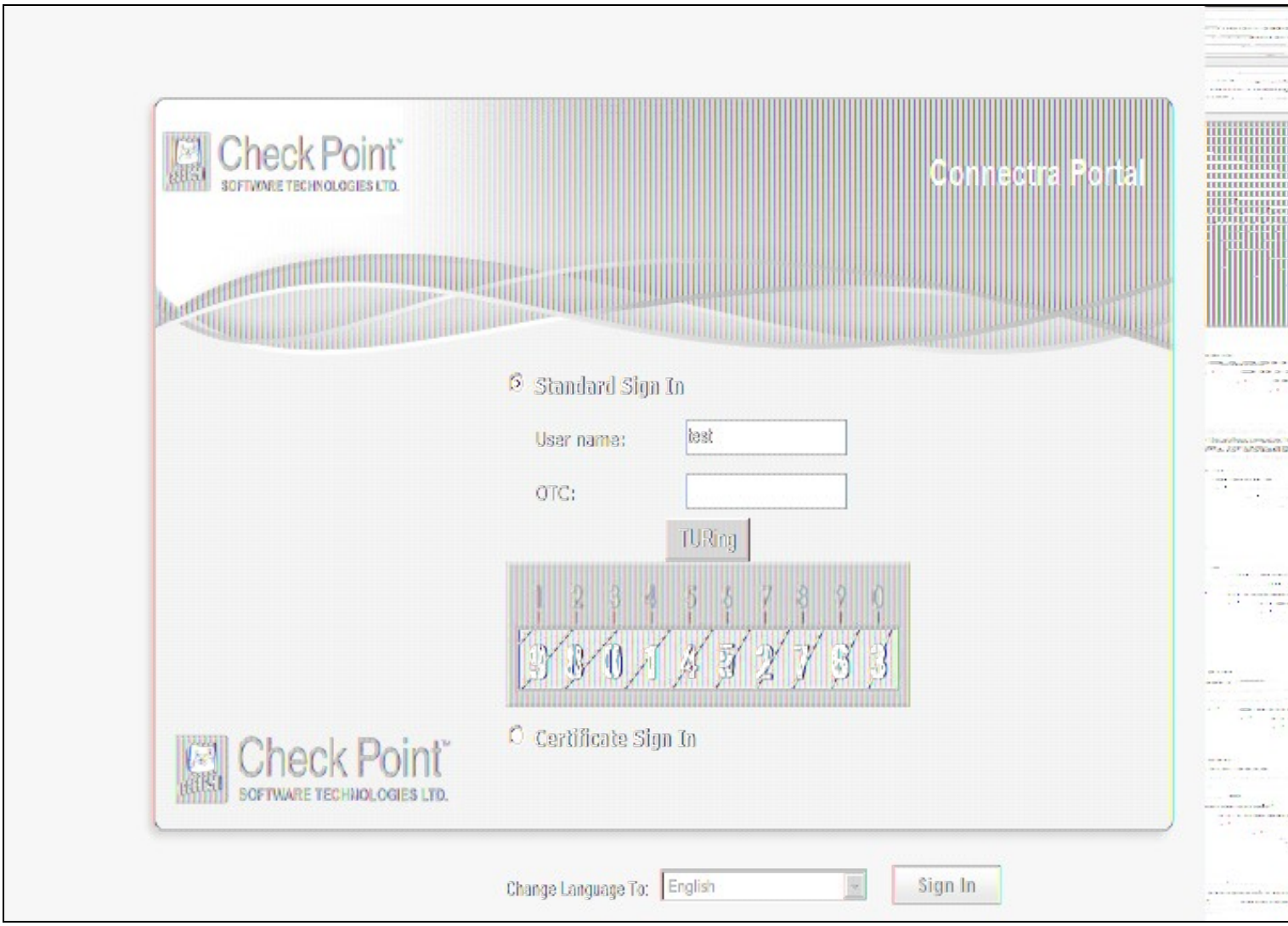
To set the text displayed on the TURing image button, insert a new line after this line, with the following content:

"TURING" => "TURing",

You can replace the right-hand text with anything you prefer. Don?t forget the comma at the end of the line.

8 Testing

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



After entering their username and either tabbing away from the username field of 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.

9 Troubleshooting

Check the Swivel logs for Turing images and RADIUS requests.

Image from PINsafe server absent

10 Known Issues and Limitations

11 Checkpoint Integration

PINsafe to Checkpoint Gaia

Integration Notes

12 Overview

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

13 Baseline

Swivel 4.x

Checkpoint Gaia appliance version R77.30.

14 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.

15 Gaia Configuration

15.1 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.

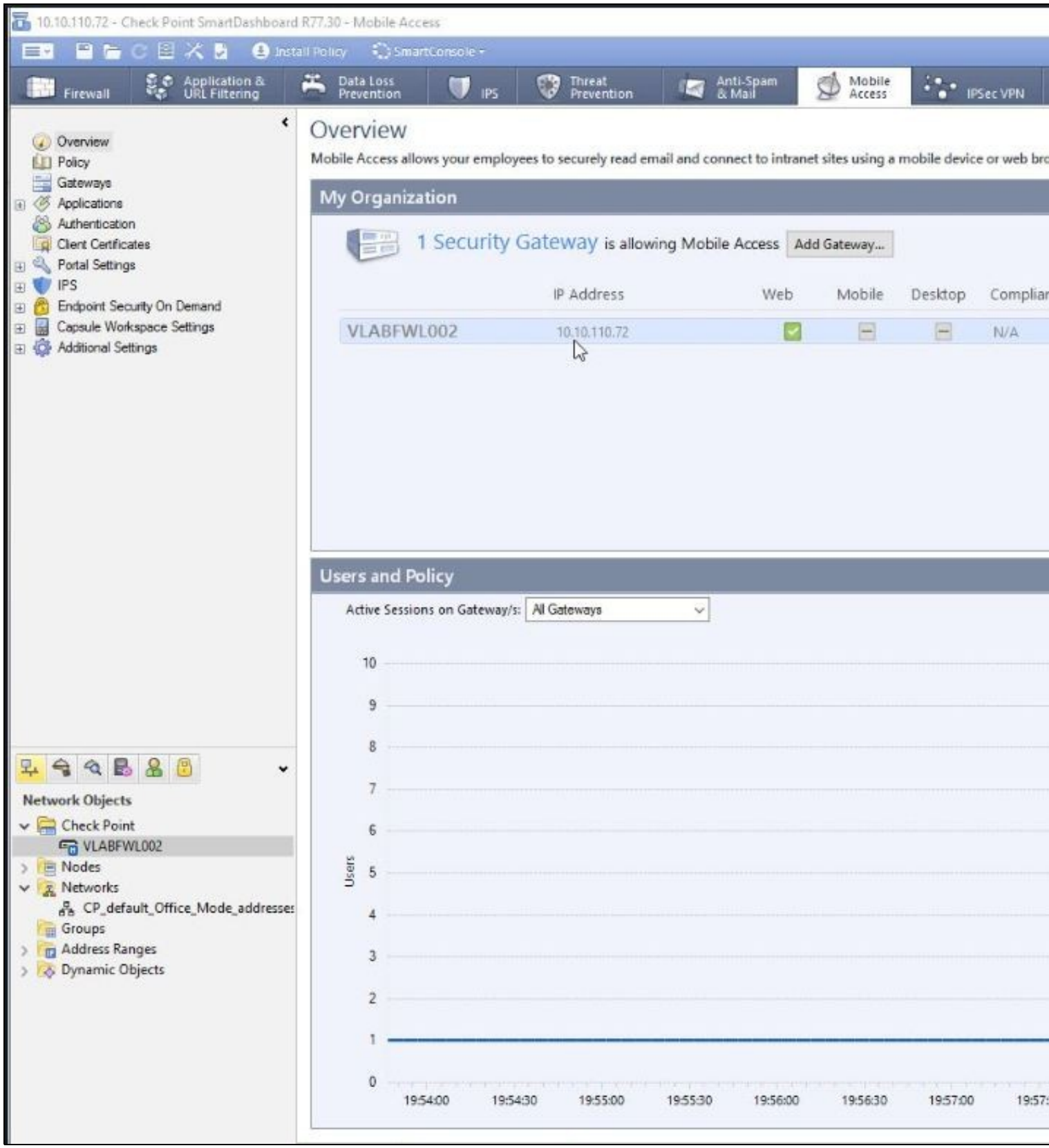
16 Customising the Gaia Login Page

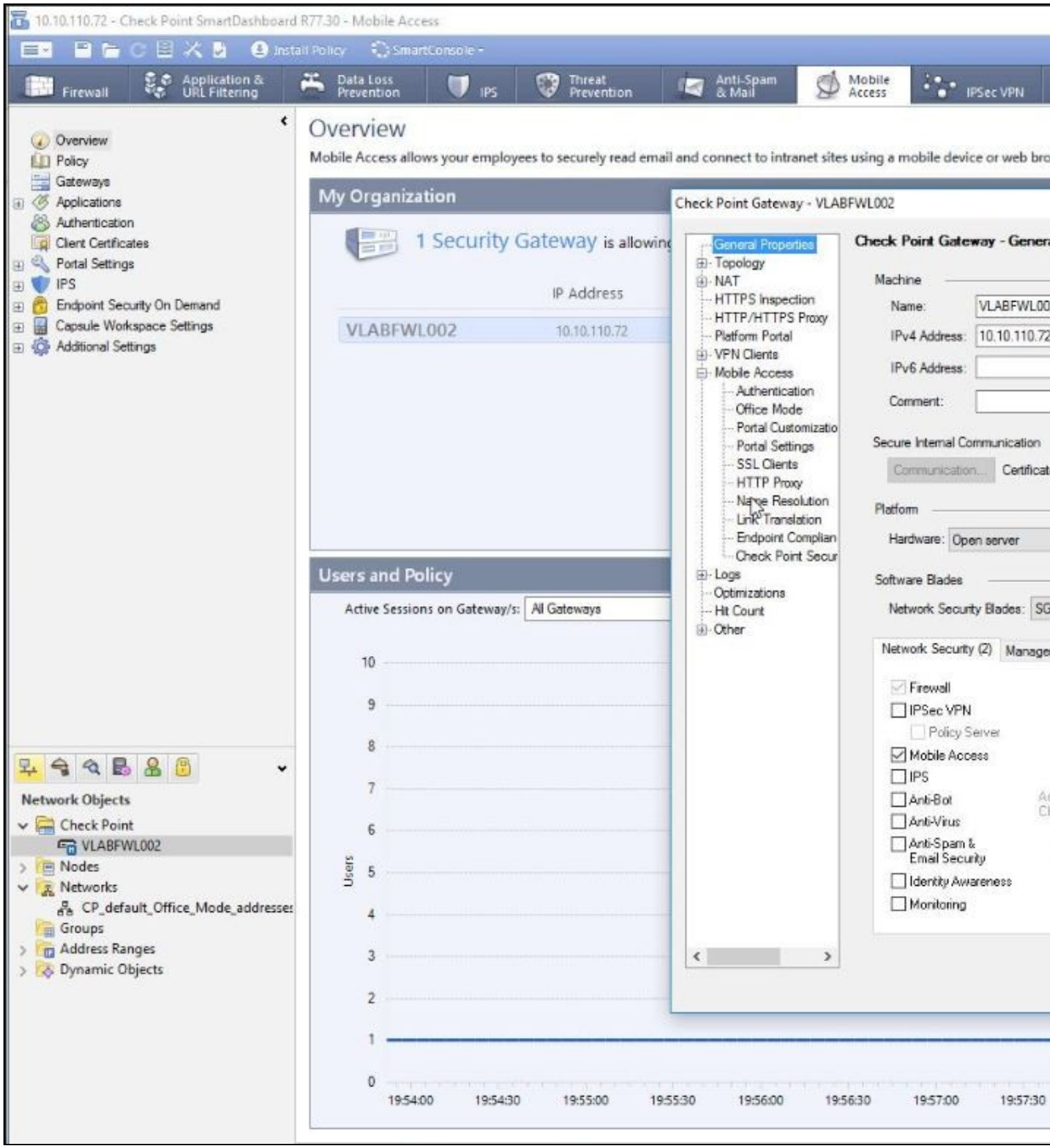
NOTE: it is assumed here that you are familiar with Unix commands, in particular with the vi editor, as you will need to edit a file.

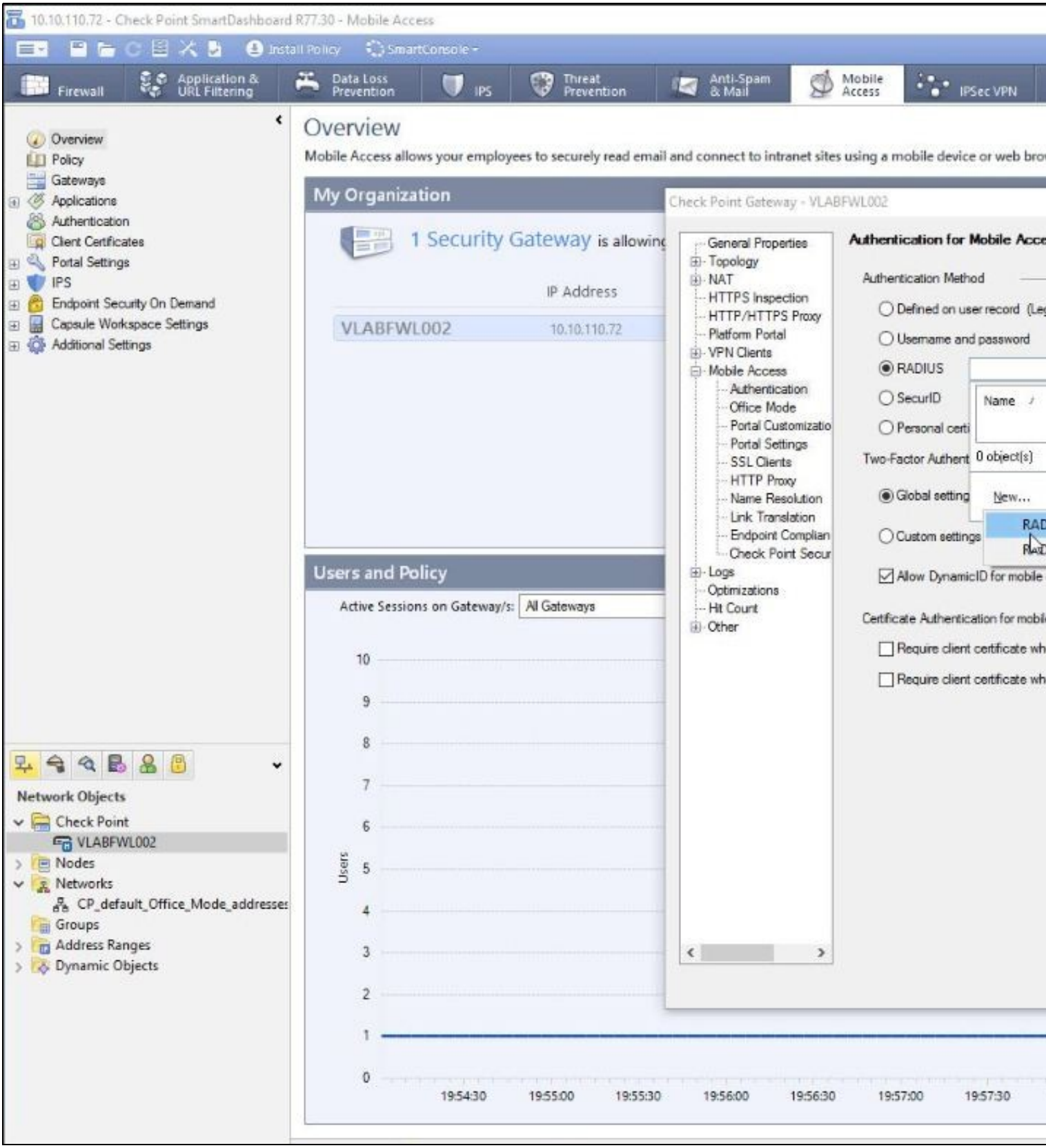
NOTE: There is an example LoginPage.php available which is the Login.php file with the modifications already included. This can be used for reference but may not be 100% suitable for specific installations and different Gaia versions.

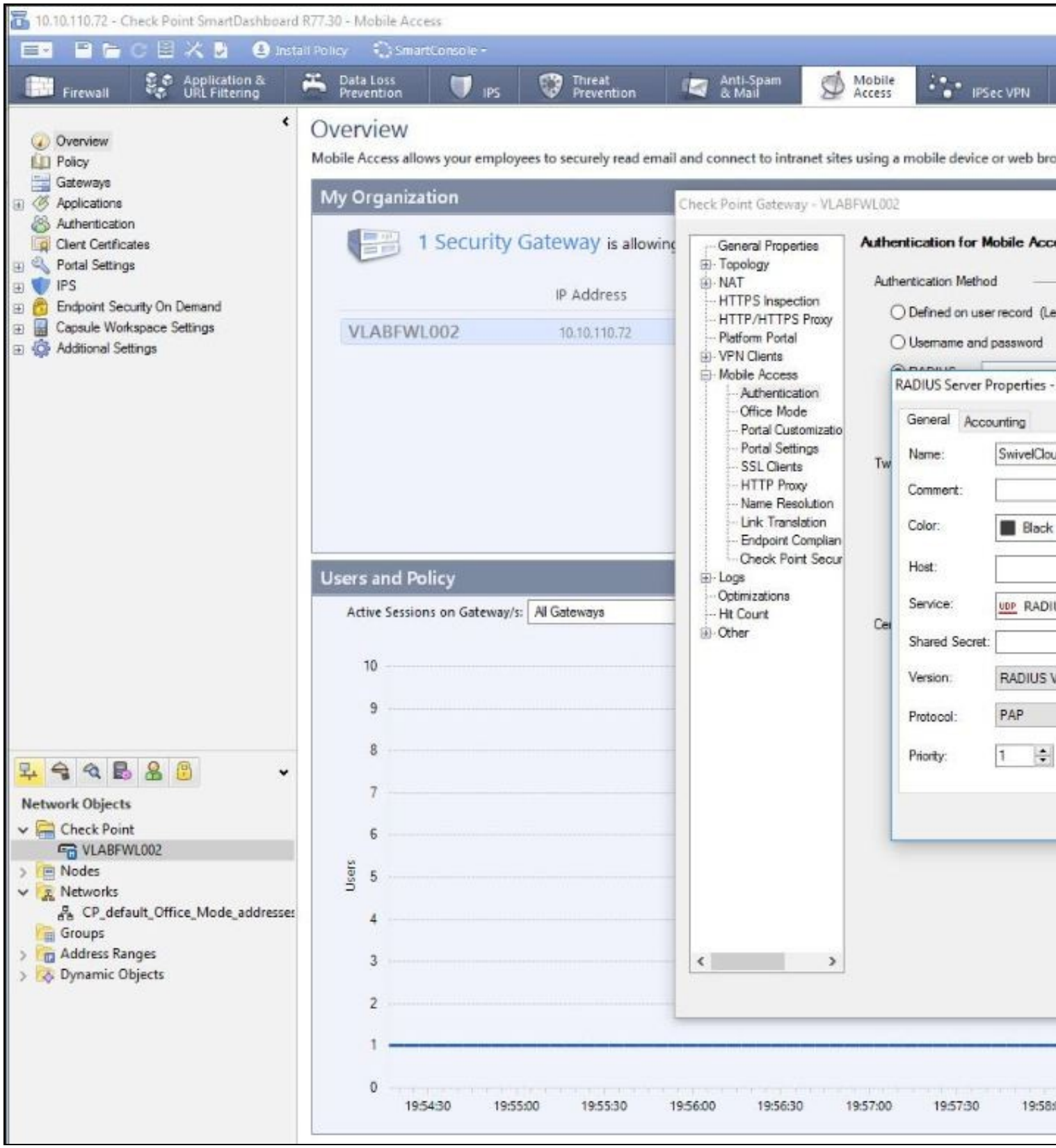
16.1 Test the RADIUS authentication

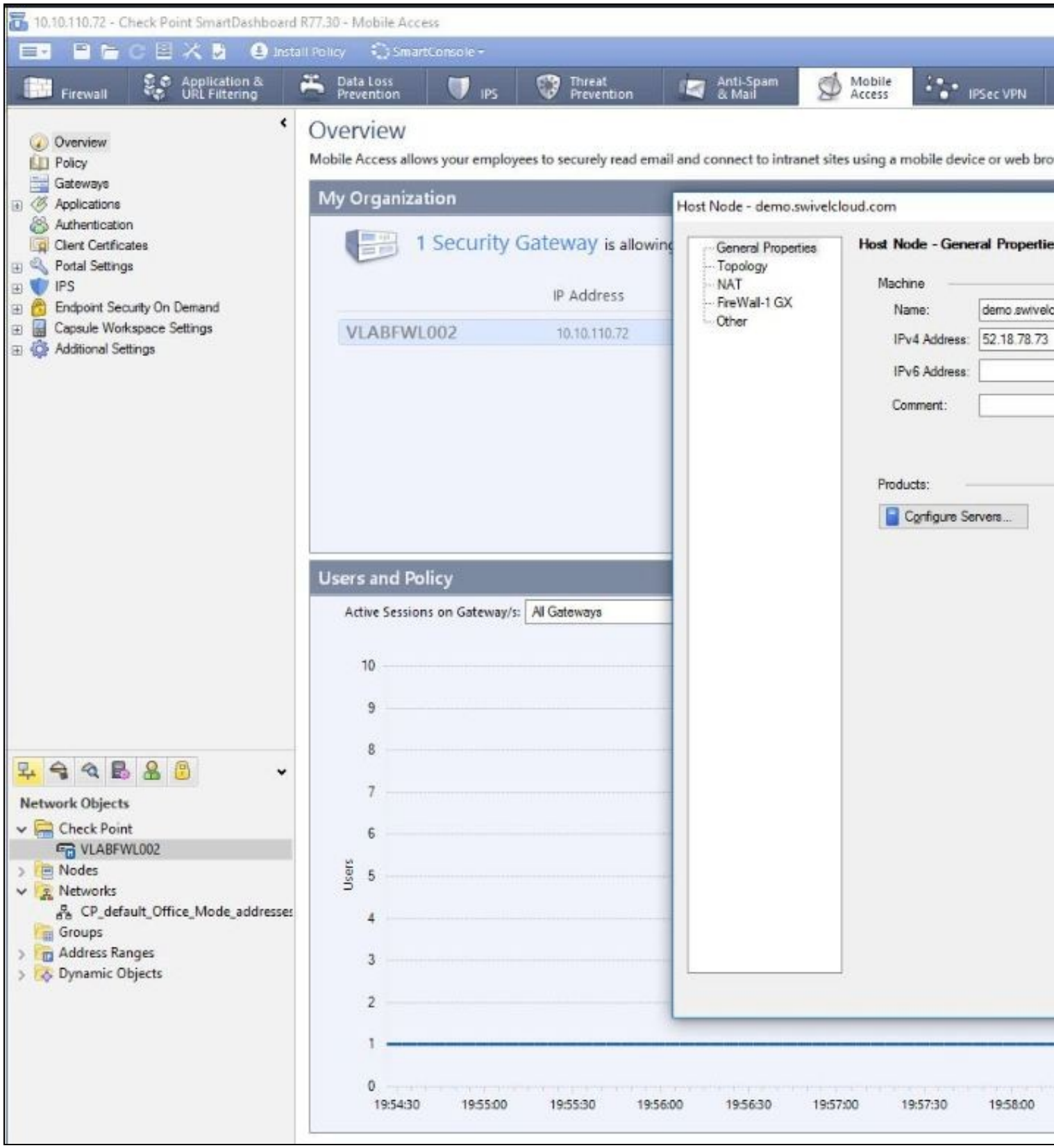
At this stage it should be possible to authenticate by SMS, hardware Token, Mobile Phone Client and Taskbar to verify that the RADIUS authentication is working for users. Browse to the SSL VPN login page, and enter Username and if being used, the password. From the Swivel Administration console select 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.

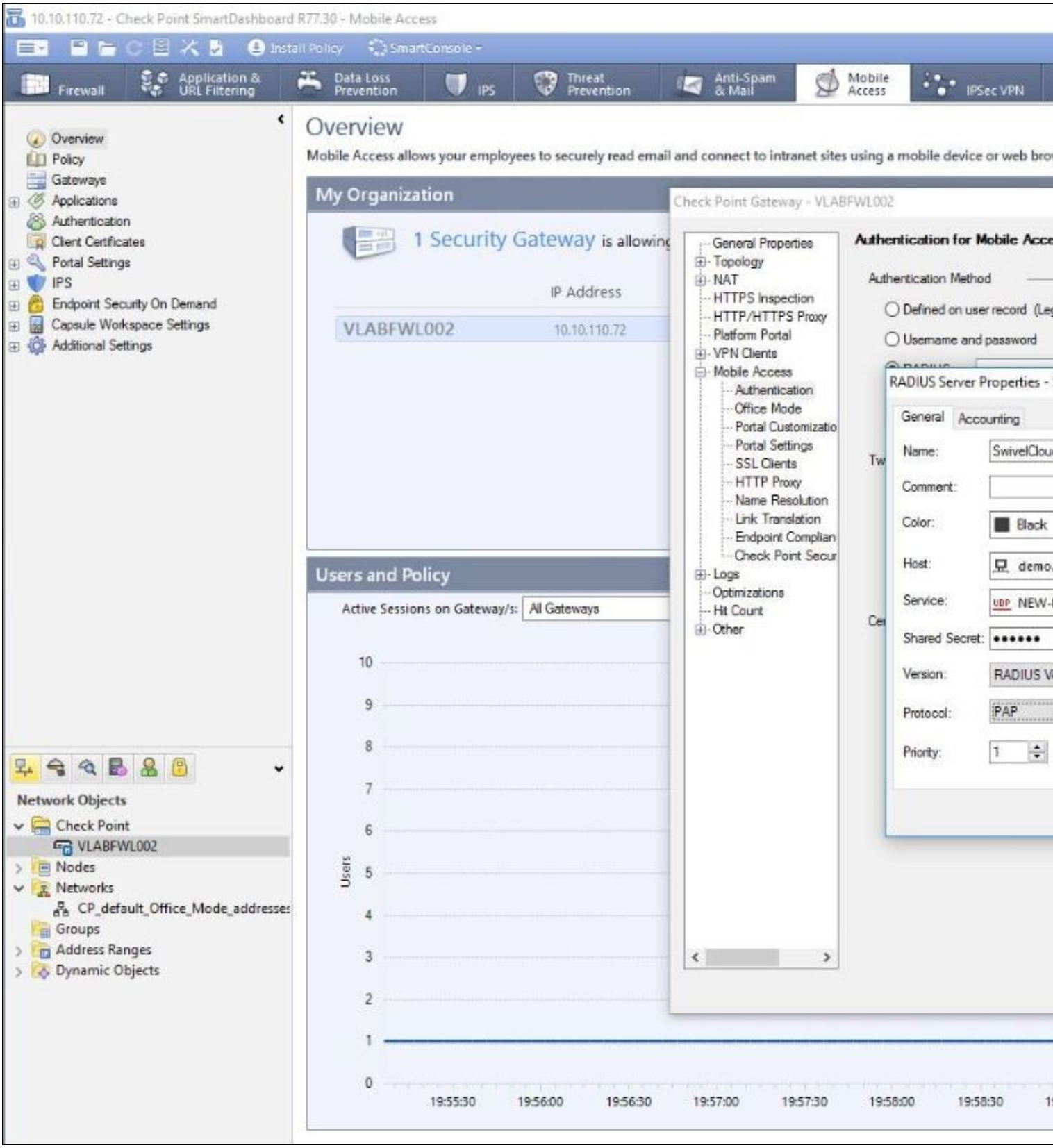

10.10.110.72 - Check Point SmartDashboard R77.30 - Mobile Access
Install Policy
SmartConsole
Firewall
Application & URL Filtering
Data Loss Prevention
IPS
Threat Prevention
Anti-Spam & Mail
Mobile Access
IPSec VPN
Overview
Policy
Gateways
Applications
Authentication
Client Certificates
Portal Settings
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 br
My Organization
1 Security Gateway is allowing Mobile Access
Add Gateway...
IP Address
Web
Mobile
Desktop
Compliar
VLABFWL002
10.10.110.72
N/A
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
Network Objects
Check Point
VLABFWL002
Nodes
Networks
CP_default_Office_Mode_addresses
Groups
Address Ranges
Dynamic Objects

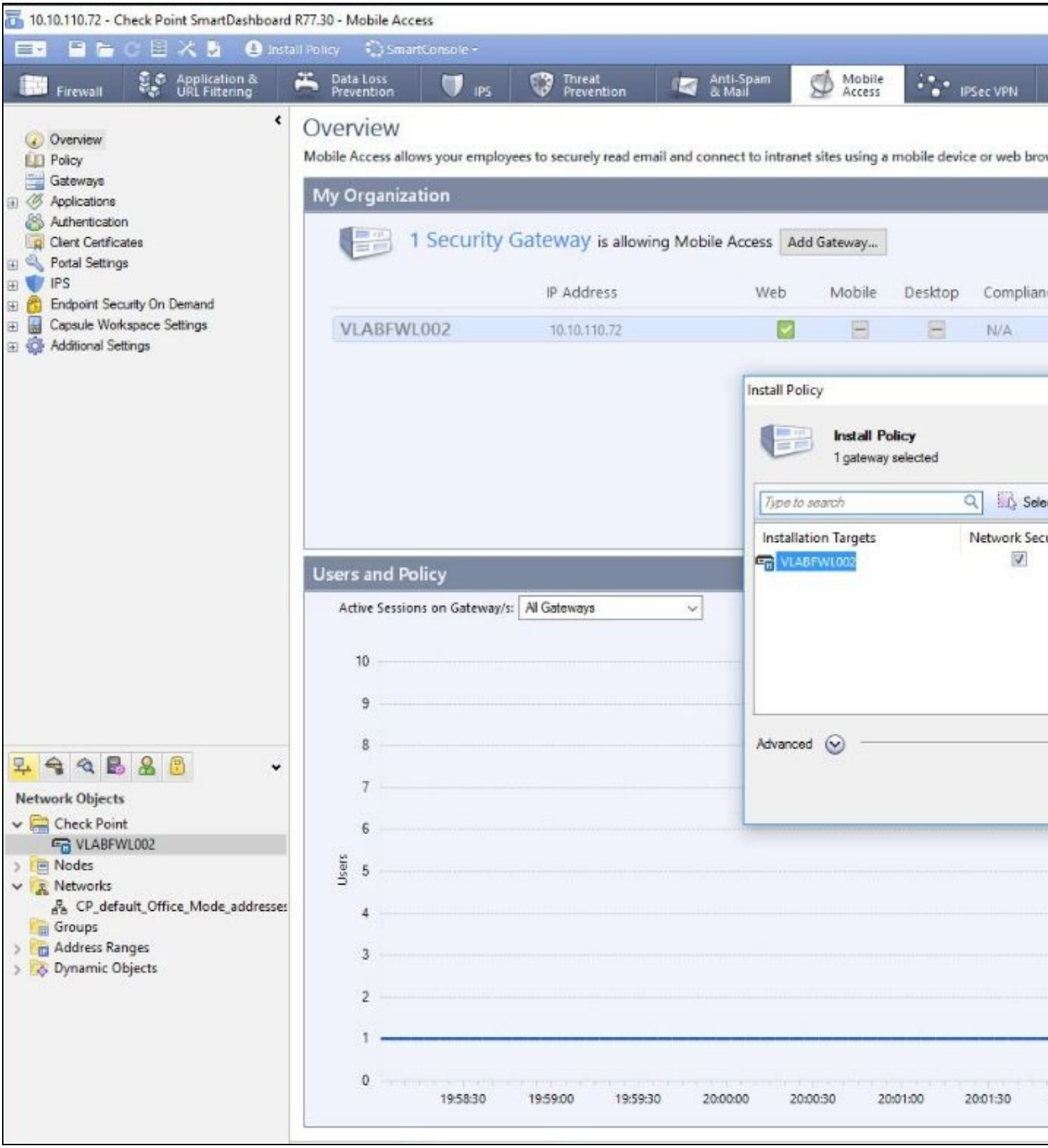

10.10.110.72 - Check Point SmartDashboard R77.30 - Mobile Access
Install Policy
SmartConsole
Firewall
Application & URL Filtering
Data Loss Prevention
IPS
Threat Prevention
Anti-Spam & Mail
Mobile Access
IPSec VPN
Overview
Policy
Gateways
Applications
Authentication
Client Certificates
Portal Settings
IPS
Endpoint Security On Demand
Capsule Workspace Settings
Additional Settings
Overview
Mobile Access allows your employees to securely read email and connect to intranet sites using a mobile device or web bro
My Organization
1 Security Gateway is allowin
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 Customizatio
Portal Settings
SSL Clients
HTTP Proxy
Name Resolution
Link Translation
Endpoint Complian
Check Point Secur
Logs
Optimizations
Hit Count
Other
Check Point Gateway - Gener
Machine
Name:
VLABFWL00
IPv4 Address:
10.10.110.72
IPv6 Address:
Comment:
Secure Internal Communication
Communication...
Certificat
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
Users and Policy
Active Sessions on Gateway/s:
All Gateways
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

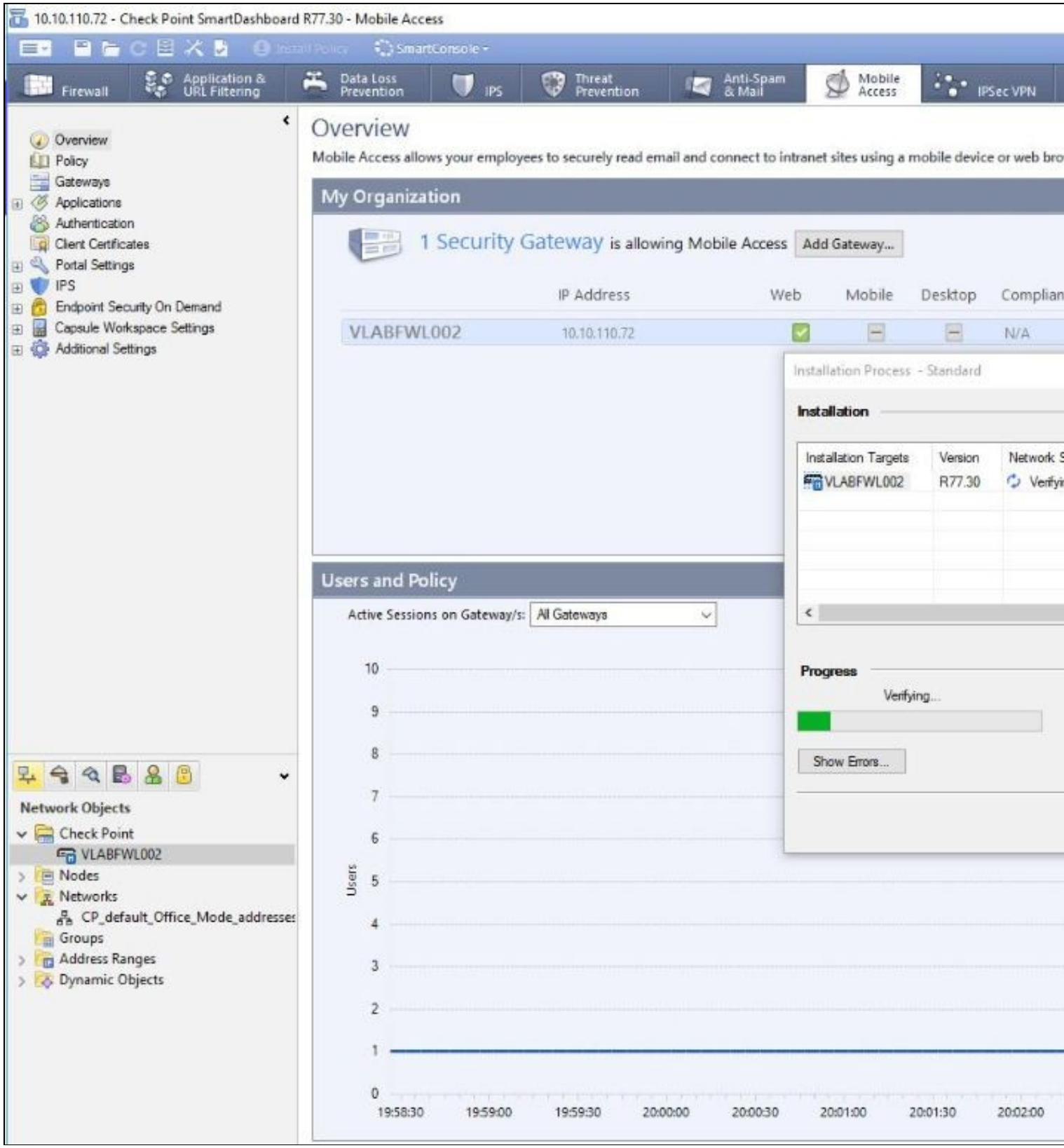

10.10.110.72 - Check Point SmartDashboard R77.30 - Mobile Access
Install Policy
SmartConsole
Firewall
Application & URL Filtering
Data Loss Prevention
IPS
Threat Prevention
Anti-Spam & Mail
Mobile Access
IPSec VPN
Overview
Policy
Gateways
Applications
Authentication
Client Certificates
Portal Settings
IPS
Endpoint Security On Demand
Capsule Workspace Settings
Additional Settings
Overview
Mobile Access allows your employees to securely read email and connect to intranet sites using a mobile device or web bro
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 Customizatio
Portal Settings
SSL Clients
HTTP Proxy
Name Resolution
Link Translation
Endpoint Complian
Check Point Secur
Logs
Optimizations
Hit Count
Other
Authentication for Mobile Acce
Authentication Method
Defined on user record (Le
Username and password
RADIUS
SecurID
Personal certi
Name
Two-Factor Authent
0 object(s)
Global setting
New...
Custom settings
Allow DynamicID for mobile
Certificate Authentication for mobi
Require client certificate wh
Require client certificate wh
Users and Policy
Active Sessions on Gateway/s:
All Gateways
Users
10
9
8
7
6
5
4
3
2
1
0
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

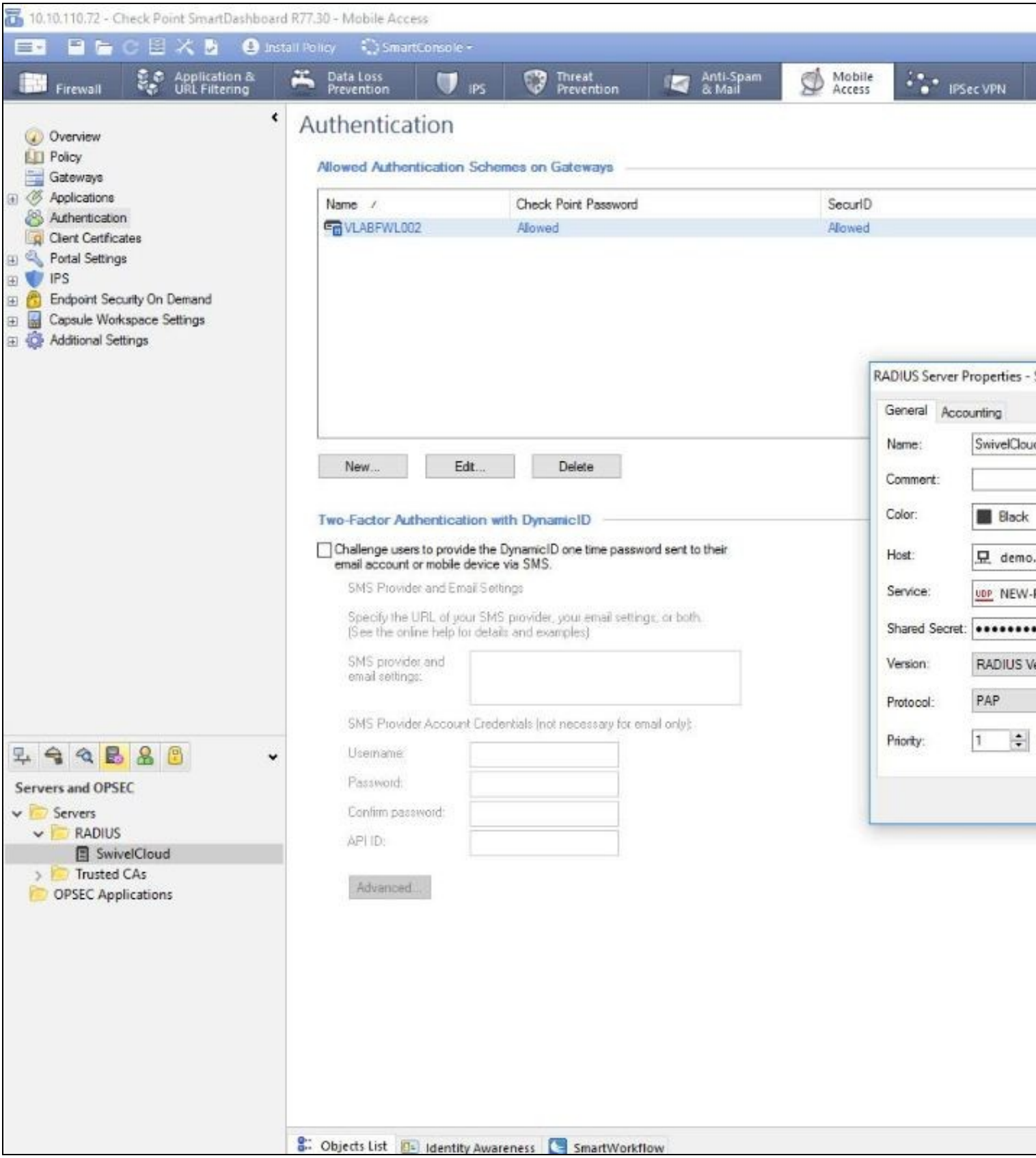

10.10.110.72 - Check Point SmartDashboard R77.30 - Mobile Access
Install Policy
SmartConsole
Firewall
Application & URL Filtering
Data Loss Prevention
IPS
Threat Prevention
Anti-Spam & Mail
Mobile Access
IPSec VPN
Overview
Policy
Gateways
Applications
Authentication
Client Certificates
Portal Settings
IPS
Endpoint Security On Demand
Capsule Workspace Settings
Additional Settings
Overview
Mobile Access allows your employees to securely read email and connect to intranet sites using a mobile device or web bro
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 Customizatio
Portal Settings
SSL Clients
HTTP Proxy
Name Resolution
Link Translation
Endpoint Complian
Check Point Secur
Logs
Optimizations
Hit Count
Other
Authentication for Mobile Acc
Authentication Method
Defined on user record (Le
Username and password
RADIUS Server Properties -
General
Accounting
Name:
SwivelClou
Comment:
Color:
Black
Host:
Service:
UDP RADIU
Shared Secret:
Version:
RADIUS V
Protocol:
PAP
Priority:
1
Users and Policy
Active Sessions on Gateway/s:
All Gateways
Users
10
9
8
7
6
5
4
3
2
1
0
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


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
Overview
Mobile Access allows your employees to securely read email and connect to intranet sites using a mobile device or web bro
My Organization
1 Security Gateway is allowin
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.swivelc
IPv4 Address:
52.18.78.73
IPv6 Address:
Comment:
Products:
Configure Servers...
Users and Policy
Active Sessions on Gateway/s:
All Gateways
Users
10
9
8
7
6
5
4
3
2
1
0
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


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
Overview
Mobile Access allows your employees to securely read email and connect to intranet sites using a mobile device or web bro
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 Customizatio
Portal Settings
SSL Clients
HTTP Proxy
Name Resolution
Link Translation
Endpoint Complian
Check Point Secur
Logs
Optimizations
Hit Count
Other
Authentication for Mobile Acce
Authentication Method
Defined on user record
Username and password
RADIUS Server Properties -
General
Accounting
Name:
Comment:
Color:
Black
Host:
Service:
Shared Secret:
Version:
Protocol:
PAP
Priority:
Users and Policy
Active Sessions on Gateway/s:
All Gateways
Users
10
9
8
7
6
5
4
3
2
1
0
19:55:30
19:56:00
19:56:30
19:57:00
19:57:30
19:58:00
19:58:30
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
Overview
Mobile Access allows your employees to securely read email and connect to intranet sites using a mobile device or web bro
My Organization
1 Security Gateway is allowing Mobile Access
Add Gateway...
IP Address
Web
Mobile
Desktop
Compliance
VLABFWL002
10.10.110.72
N/A
Install Policy
Install Policy
1 gateway selected
Type to search
Installation Targets
Network Sec
VLABFWL002
Advanced
Users and Policy
Active Sessions on Gateway/s:
All Gateways
Users
10
9
8
7
6
5
4
3
2
1
0
19:58:30
19:59:00
19:59:30
20:00:00
20:00:30
20:01:00
20:01:30
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
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
Overview
Mobile Access allows your employees to securely read email and connect to intranet sites using a mobile device or web bro
My Organization
1 Security Gateway is allowing Mobile Access
Add Gateway...
IP Address
Web
Mobile
Desktop
Complian
VLABFWL002
10.10.110.72
N/A
Installation Process - Standard
Installation
Installation Targets
Version
Network S
VLABFWL002
R77.30
Verifyi
Progress
Verifying...
Show Errors...
Users and Policy
Active Sessions on Gateway/s:
All Gateways
10
9
8
7
6
5
4
3
2
1
0
Users
19:58:30
19:59:00
19:59:30
20:00:00
20:00:30
20:01:00
20:01:30
20:02:00
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:
Comment:
Color:
Black
Host:
Service:
Shared Secret:
Version:
Protocol:
PAP
Priority:
1
Servers and OPSEC
Servers
RADIUS
SwivelCloud
Trusted CAs
OPSEC Applications
Objects List
Identity Awareness
SmartWorkflow

17 Swivel Configuration

17.1 Configuring the RADIUS server

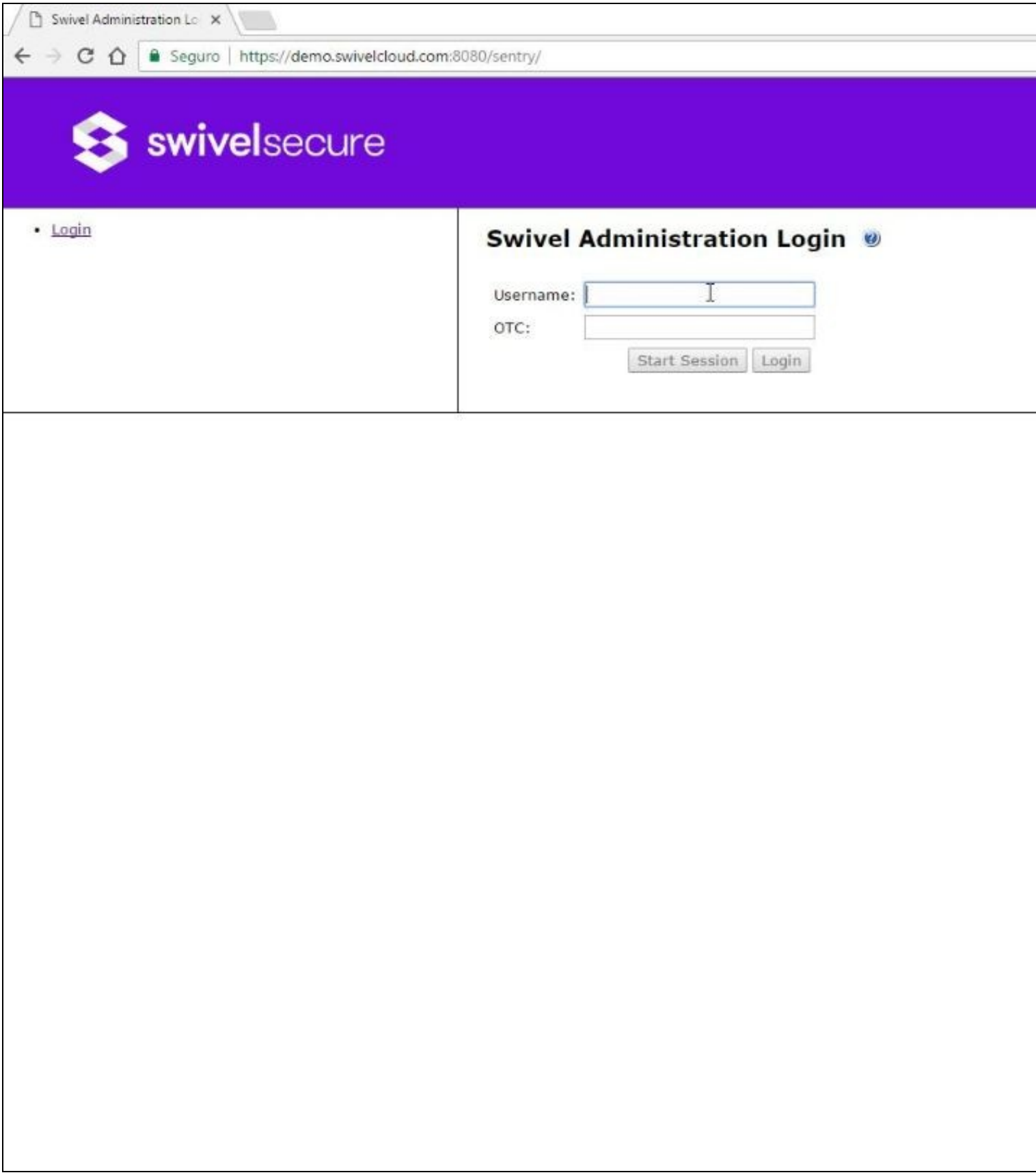
On the Swivel Administration console configure the RADIUS Server and NAS, see RADIUS Configuration

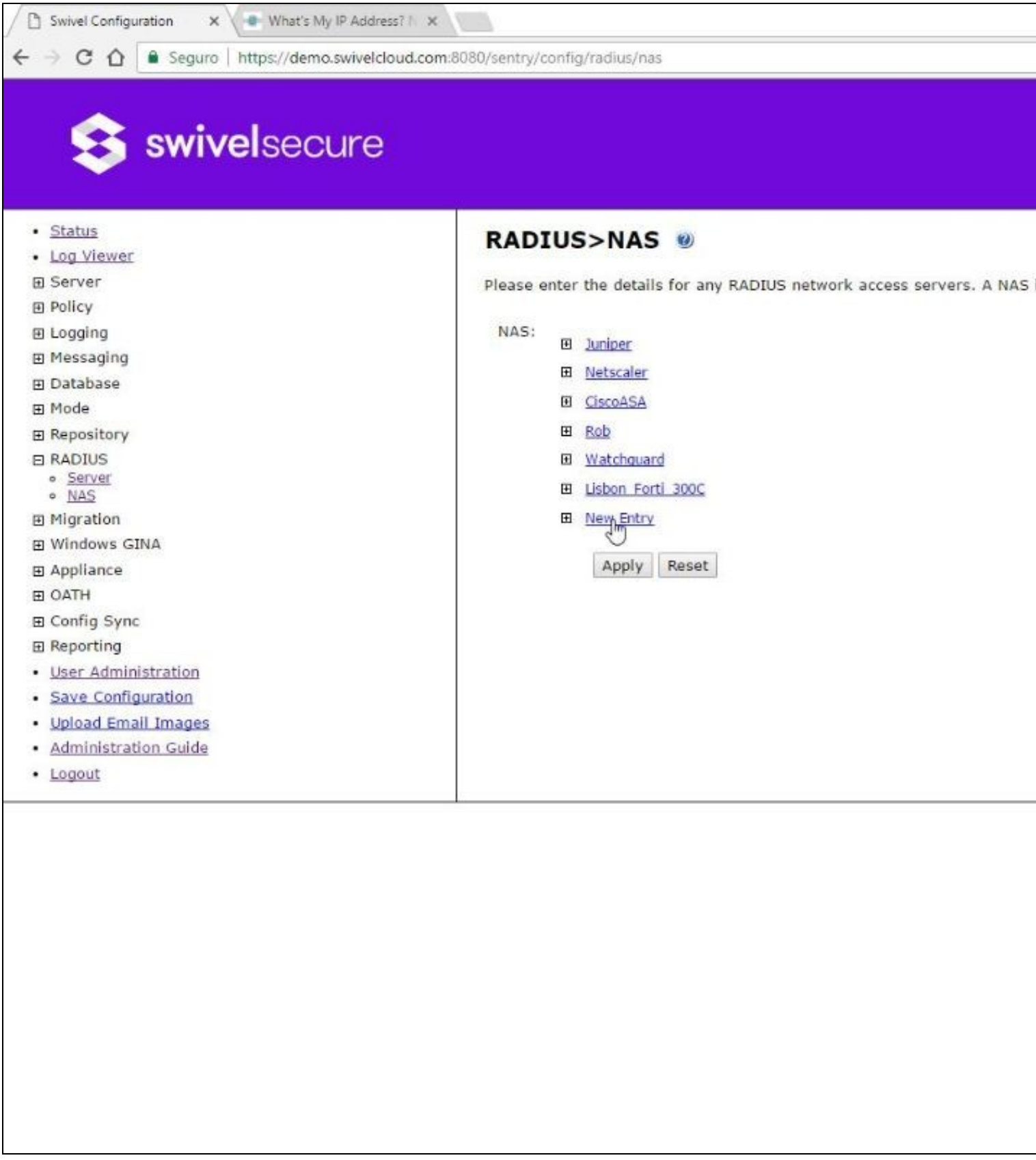
17.2 Enabling Session creation with username

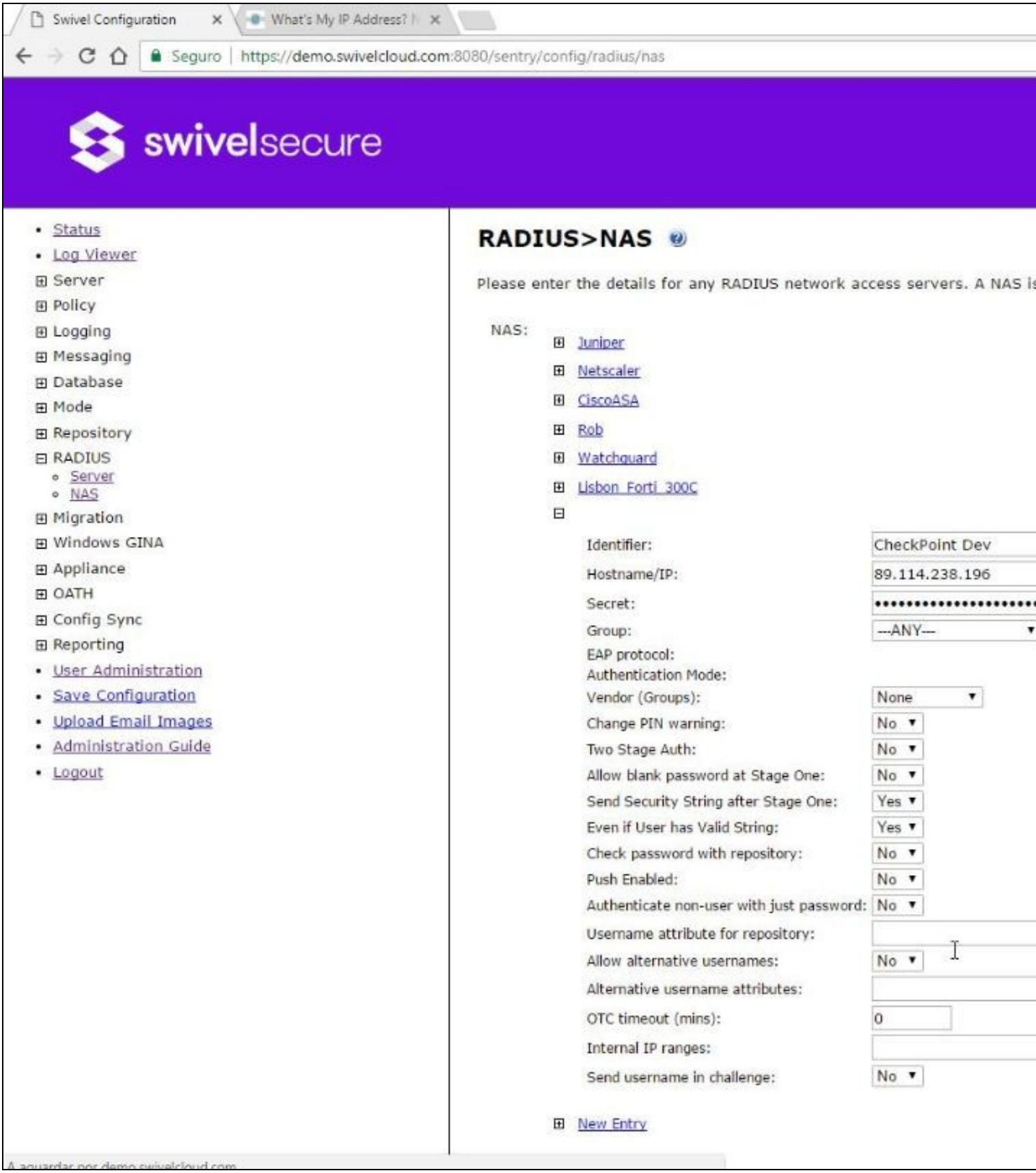
To allow the TURing image, Pinpad and other single channel images, under Server/Single Channel set Allow session request by username to Yes.

17.3 Setting up Swivel Dual Channel Transports

See Transport Configuration

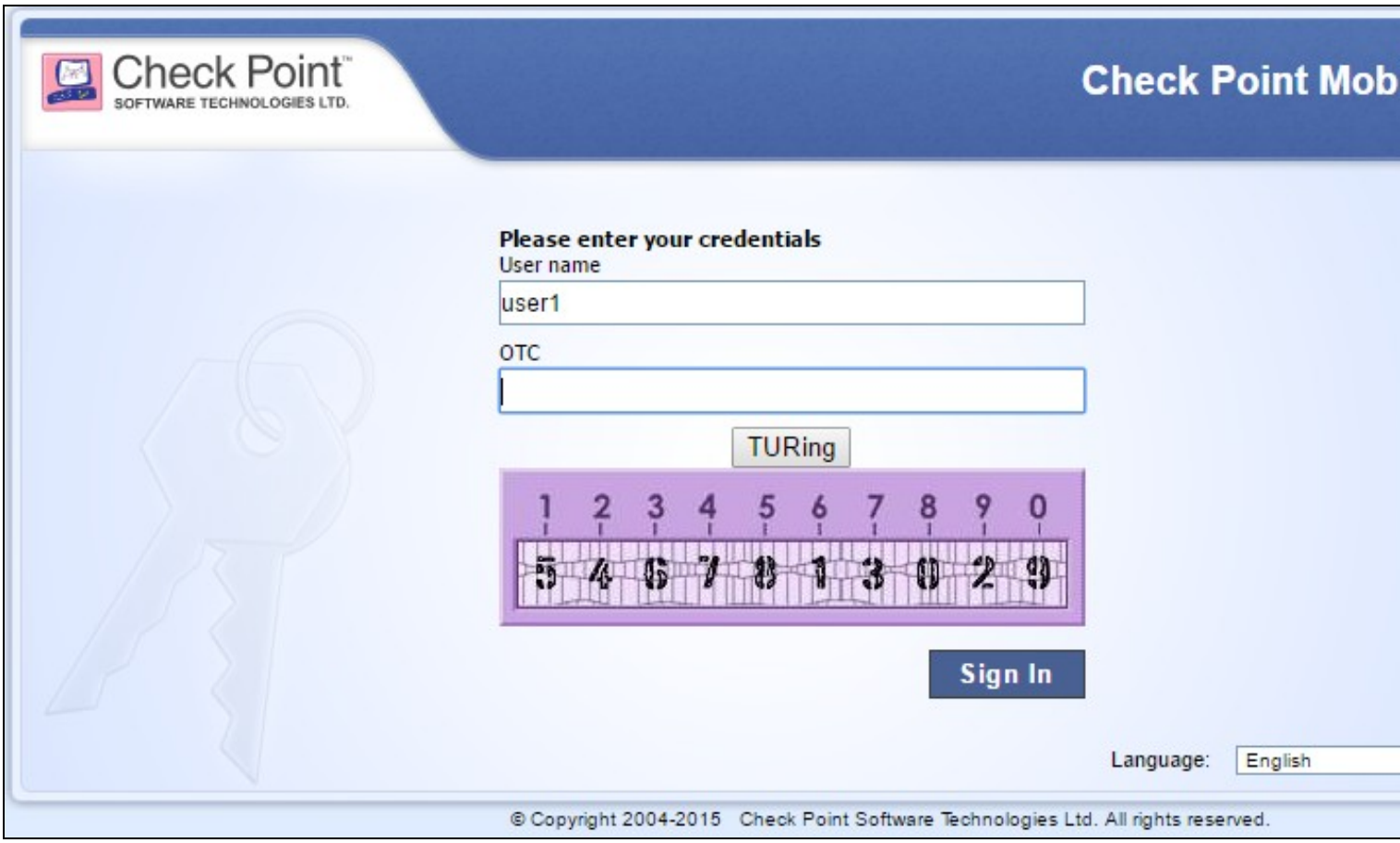

Swivel Administration Lo
Seguro | https://demo.swivelcloud.com:8080/sentry/
swivelsecure
Login
Swivel Administration Login
Username:
OTC:
Start Session
Login


Swivel Configuration
What's My IP Address?
Seguro
https://demo.swivelcloud.com:8080/sentry/config/radius/nas
swivelsecure
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
Apply
Reset


Swivel Configuration
What's My IP Address?
Seguro | https://demo.swivelcloud.com:8080/sentry/config/radius/nas
swivelsecure
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: 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
A aguardar por demo.swivelcloud.com...

18 Testing

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

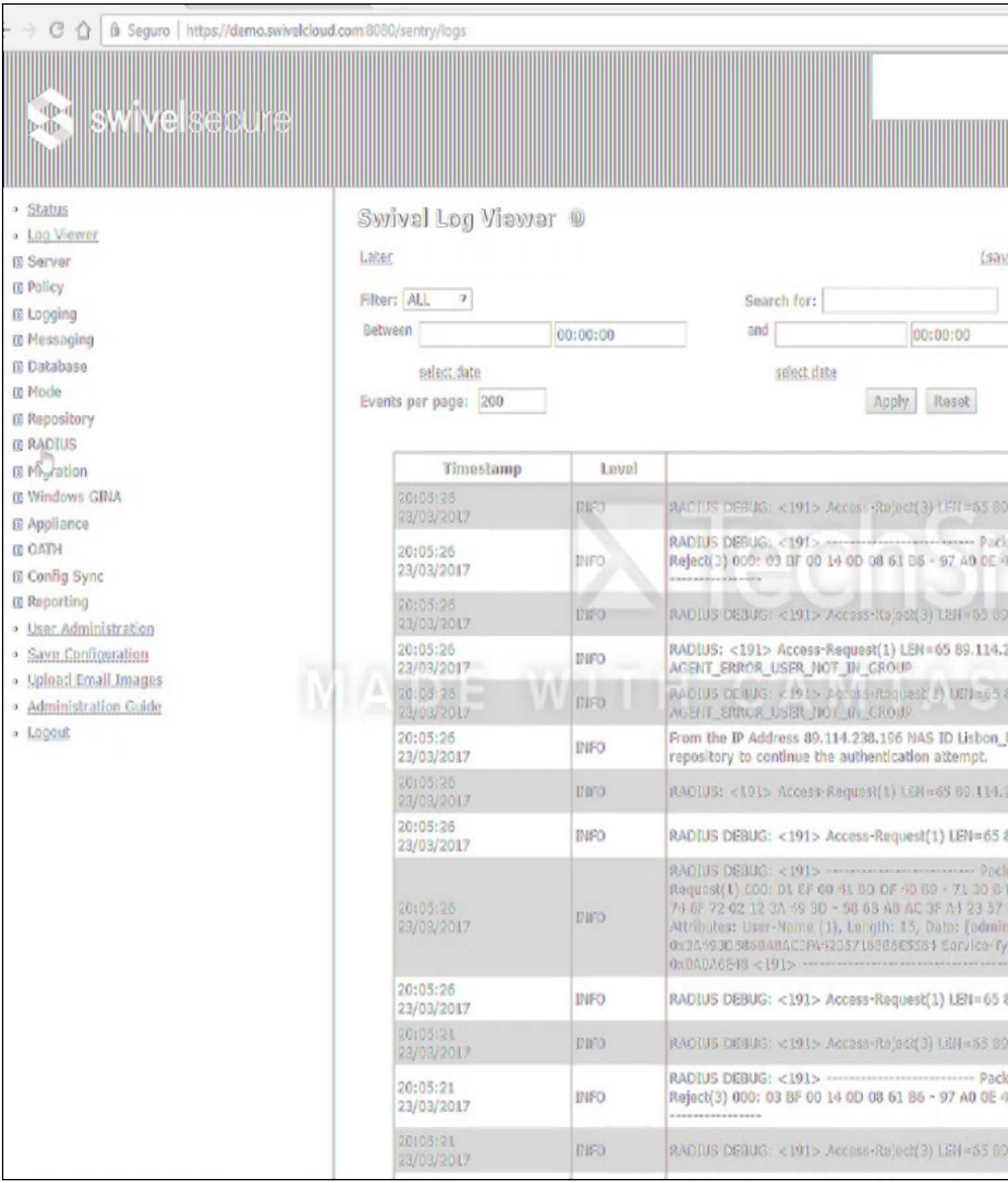


After entering their username and either tabbing away from the username field of clicking the TURing button they will be presented with a TURing image. The PINsafe log should record a session start for that user.

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.

19 Troubleshooting

Check the Swivel logs for Turing images and RADIUS requests.



20 Additional Information

For assistance in the Swivel Secure installation and configuration please firstly contact your reseller and then email Swivel Secure support at supportdesk@swivelsecure.com

21 Checkpoint EndPointSecurityVPN Integration

Place Holder

22 Checkpoint Mobile Access

Please refer to the Checkpoint Connectra Integration page.

23 Checkpoint Mobile Access Blade Integration

24 Overview

Swivel can provide strong and two factor authentication to the Check Point Mobile Access Blade. This document outlines the details required to carry this out.

25 Baseline

Swivel 3.x

Check Point CR75 Mobile Access Blade and newer

26 Prerequisites

Working Mobile Access Blade VPN

Swivel 3.x

Use of the TURing, 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.

27 Downloads

Customised login page

28 Demos

TURing	SMS	Mobile App.
Check Point MAB & Swivel TURing	Check Point MAB & Swivel SMS	Check Point MAB & Swivel Mobile App.

29 Swivel Configuration

29.1 Configuring the RADIUS server

On the Swivel Administration console configure the RADIUS Server and NAS, see RADIUS Configuration

29.2 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.

29.3 Setting up Swivel Dual Channel Transports

See Transport Configuration

30 Mobile Access Blade Configuration

30.1 Enabling RADIUS Authentication in Mobile Access Blade

You need to configure Swivel as an authentication server on the Mobile Access Blade

- Open Smart Dashboard and log in.
- Under Servers and OPSEC, locate the RADIUS folder and right click and select New RADIUS
- In the New RADIUS popup window click on 'New'
- Configure the Swivel server as a new host. You just need to give it a name and add the IP address.
- Select Swivel as the host, ?NEW-RADIUS? as the service, and enter the shared secret you previously set on the Swivel appliance. 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.

- 

New RADIUS

- 

New Host

- 

Configure New Host

- 

RADIUS Server Properties

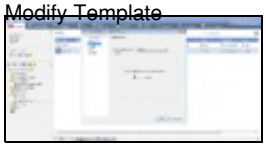
30.2 Configuring AD Templates to use RADIUS

- Modify AD user template and select RADIUS.

Don?t forget to save and install the policy once you have made all relevant changes.

- 

Modify Template

- 

Select RADIUS

30.3 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.

31 Customising the Mobile Access Blade Login Page

31.1 Modify custom LoginPage.php

Download the provided LoginPage.php

Modify the PHP file, and change the URL values to the site location (search for TURing)

31.2 Connect to the Check Point Appliance

Use WinSCP to connect to the Check Point Appliance, and retrieve a copy and keep safe keeping of the login page (LoginPage.php) from:

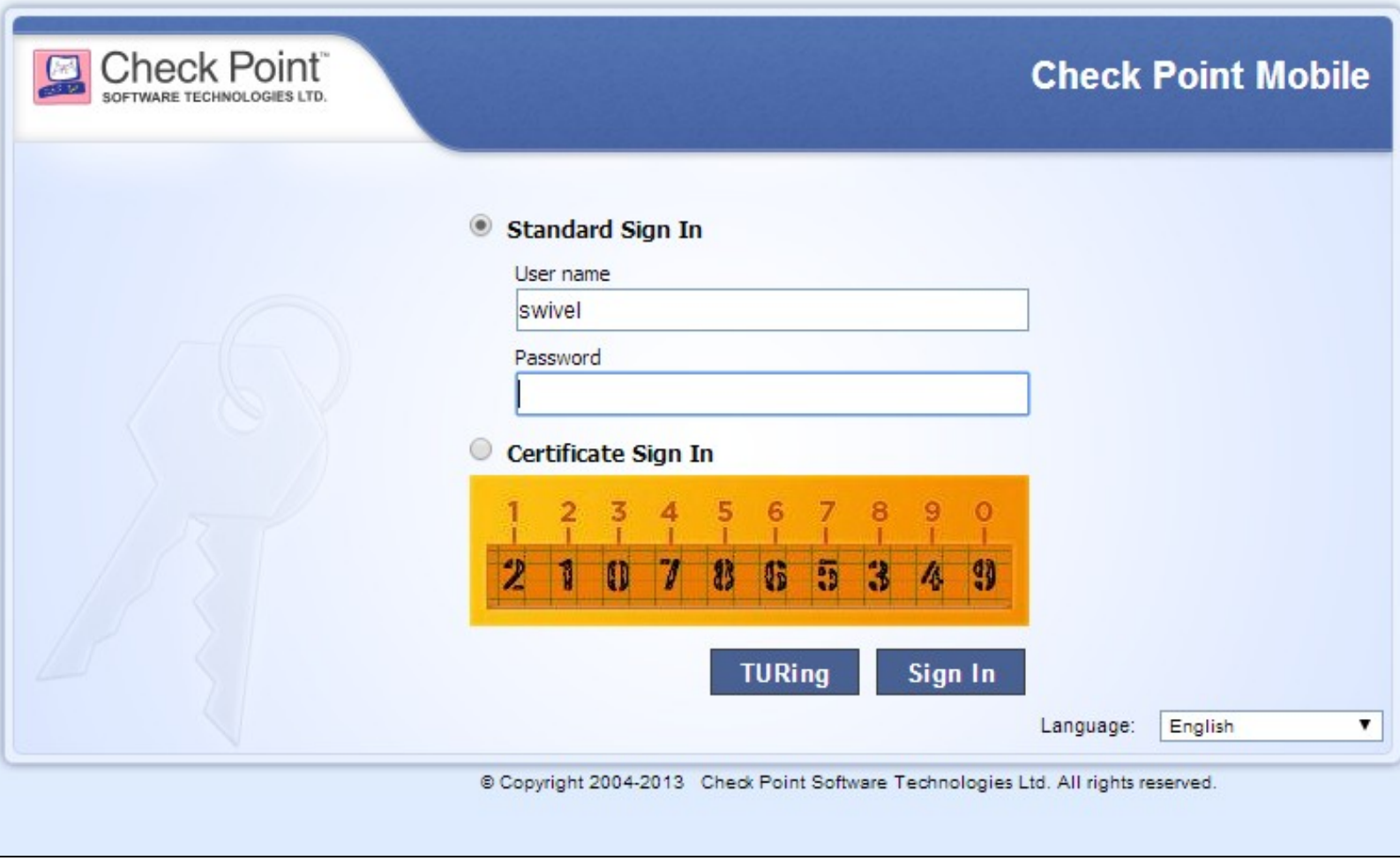
/opt/CPcvpn-R77/phpincs (note: the exact directory name CPcvpn-R** will vary depending on the Mobile Access Blade revision number).

31.3 Upload new Login Page

Use WinSCP to upload a copy of the provided LoginPage.php to the appliance.

32 Testing

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



After entering their username and either tabbing away from the username field of clicking the TURing button they will be presented with a TURing image.

The Swivel 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 Swivel log show record the RADIUS dialogue associated with this authentication.

33 Troubleshooting

Check the Swivel logs for TURing images and RADIUS requests.

Image from PINsafe server absent

34 Known Issues and Limitations

35 Checkpoint SecureClient Integration

Checkpoint SecureClient

Integration Guide

Version 1.1 March 2010, Updated March 2014

36 Introduction

This document outlines the steps required to integrate the Checkpoint SecureClient VPN software with Swivel.

Swivel users can use Swivel?s Token, SMS, Mobile Phone Client, as well as the single channel TURing and Pinpad methods to retrieve a One Time Code or a Security string.

With Single Channel methods, the user must be presented with a TURing or Pinpad at sign-in time, so they can extract their OTC such as the TURing using the Taskbar.

The settings and software can be configured for larger deployments within an msi file to ease installation.

36.1 Prerequisites

Checkpoint SecureClient E75. This solution is not compatible with E80.

Swivel 3.x. Where the Single Channel image is to be used, this should be presented to the user through a Network Address Translation to the Swivel server.

Swivel SecureClient software

- The file extensions have been changed to prevent them being blocked by filters etc .dll files to .dlx, and .reg to .rex. These need to be renamed back again.

36.2 Baseline

Checkpoint SecureClient R60 and R77,

Checkpoint SecureClient E75.10 (tested for Token, SMS, Mobile App, Taskbar)

Checkpoint VPN server R75.45 (tested for Token, SMS, Mobile App, Taskbar)

Swivel 3.6, 3.9.7, 3.10

36.3 Architecture

The user connects to the Checkpoint VPN by using the SecureClient software. The Checkpoint is configured to use a Swivel server for radius authentication. Users are stored and maintained in Swivel.

37 Swivel Configuration

37.1 Configuring the RADIUS server

On the Swivel Administration console configure the RADIUS Server and NAS, see RADIUS Configuration

37.2 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.

37.3 Setting up Swivel Dual Channel Transports

See Transport Configuration

38 Configuring the Checkpoint VPN-1/Firewall-1

38.1 Checkpoint VPN-1/Firewall-1 configuration Overview

The steps for enabling SecureClient users on the Checkpoint VPN-1/Firewall-1 is outlined below. For further details refer to the VPN-1/Firewall-1 Administration Guides.

1. Install the SecureClient license.

2. Create SecureClient users.

3. Define a SecureClient authentication method using PINsafe as a RADIUS server

4. Create a SecureClient group.

5. Add SecureClient users to the SecureClient group.

6. Define a Remote Access Community and participants.

7. Create SecureClient rule for the Remote Access Community.

8. Create the Desktop Security Policy rules.

9. Install Security Policy.

38.1.1 Configure Checkpoint VPN-1/Firewall-1 to use the Swivel RADIUS server

Create a RADIUS server entry on the Checkpoint Policy Editor

Select Manage/Network Objects' then Click on New then Workstation. In the Workstation Properties window, enter the, Swivel server IP Address, choose 'Host' for Type. For the Comment enter enter "PINsafe authentication". When complete, click OK. 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.

Select Manage/Servers then click on New and from the menu select Radius. In the RADIUS Server Properties window enter the following:

Name RADIUS server name

Comment information e.g. PINsafe RADIUS server

Colour A colour for the object (we like orange!)

Host hostname of the Swivel server created above

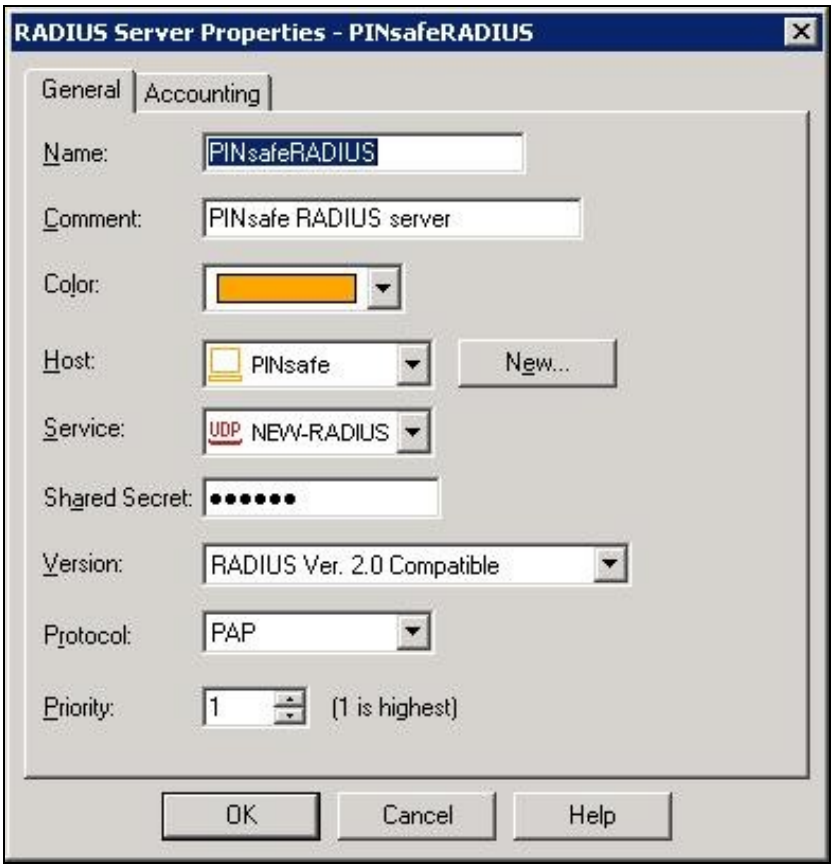
Service select New Radius (Uses port 1812)

Shared secret enter the shared secret that is also entered on the Swivel server

Version select the RADIUS version required

Protocol select the required RADIUS version

Priority The priority for authentication to multiple RADIUS devices



38.1.2 To configure External Checkpoint VPN-1/Firewall-1 users to authenticate by RADIUS

External User Profiles There are two different types of External User Profiles available in the Check Point VPN-1/Firewall-1 product, either match all users or match by domain, whereby users are differentiated by their domain name.

The steps below will configure an External Profile of Match All Users.

1. On the Checkpoint VPN-1/Firewall-1 configuration select Manage/Users and Administrators/New/Match All Users/Default.

2. The user generic* is created and greyed out.

3. Select the Authentication tab.

4. From the drop down box choose RADIUS as the user?s Authentication Method.

For further details on the available user authentication methods, configuration and setup, refer to the VPN-1/Firewall-1 Administration Guides.

The SecureClient is now ready for two factor authentication using standard SMS delivery or the Mobile Phone Client.

38.2 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. Open the Secureclient, 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 SecureClient 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. 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.

38.3 Modifying the Checkpoint SecureClient for Single Channel and Advanced SMS features

Note that all .dll files have been renamed to .dlx, and .reg files to .rex, to avoid problems with email filters. You will need to change the names back before deploying the files.

Stop the SecureClient or ensure it is not running.

Copy PINsafeAuthGUI.dll, and copy it to the SecuRemote\bin folder

Edit SecuRemote\database\userc.C. and add the below to the :options section

```
:guilibs (
: ("C:\Program Files\CheckPoint\SecuRemote\bin\PINsafeAuthGUI.dll")
)
```

Edit RegSettings.reg. to set the correct Swivel server and possibly the port and context. Double-click RegSettings.reg to install the registry settings the DLL needs.

The options are:

PINsafeServer: The IP address of the Swivel server. This should be a NAT address of the Swivel server and accessible from the client.

PINsafeProtocol: 1 for https, or 0 for http

PINsafePort: The port used to retrieve single channel images from the Swivel server, usually 8443 for a Swivel virtual or hardware appliance. For a software only install see Software Only Installation

PINsafeContext: The installation instance of the pinsafe server, usually pinsafe or proxy for a Swivel virtual or hardware appliance

PINsafeAllowSelfCert: 1 to allow self signed certificates on the Swivel server, 0 to not allow them to be used

PINsafeSecret:

PINsafeUser: The user for authentication can be pre-configured. Do not set this value if this is a template to be used for deployment to multiple users.

PINsafeChannelType: single or dual channel communications. Setting dual, requests an SMS security string by the on demand method. The On Demand authentication must be enabled on the Swivel server.

Default Values are:

```
Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\SOFTWARE\Swivel Secure\PINsafe SecureClient]
"PINsafeServer"="localhost"
"PINsafeProtocol"="1"
"PINsafePort"="8080"
"PINsafeContext"="pinsafe"
"PINsafeAllowSelfCert"="1"
"PINsafeSecret"="secret"
"PINsafeUser"=""
"PINsafeChannelType"="single"
```

Swivel virtual or hardware Appliance Values:

Default Values are:

```
Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\SOFTWARE\Swivel Secure\PINsafe SecureClient]
"PINsafeServer"="External NAT IP of PINsafe server"
"PINsafeProtocol"="1"
"PINsafePort"="8443"
"PINsafeContext"="proxy"
"PINsafeAllowSelfCert"="1"
"PINsafeSecret"="secret"
"PINsafeUser"=""
"PINsafeChannelType"="single"
```

Verify that winhttp.dll is present in C:\Windows\System32

Start SecureClient. Click connect. Under Options, Change Authentication to Secure Authentication API.

When you click Connect, you should now either see a dialog with a TURing on it, or "CONFIRMED" for dual channel, in which case a security string will be sent by the appropriate transport. The password field has been left in case you want a password as well as a OTC, but this can be removed if required. Enter the OTC, and hopefully it will authenticate.

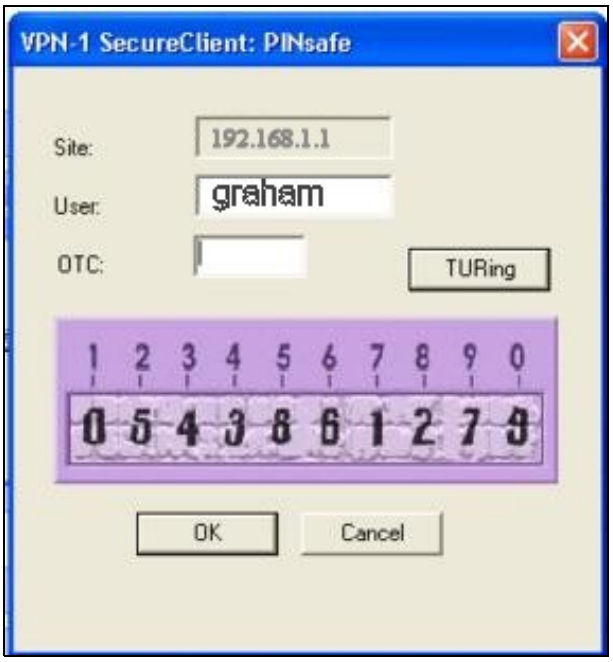
39 Removing the Swivel SecureClient

To remove the Swivel authentication remove the earlier added content in Edit SecuRemote\database\userc.C.

then restart the client

40 Verifying the Installation

Login using the Turing or SMS.



41 Bulk deployment

With a tested deployment, it is possible to take these settings and create a msi file that will install the Swivel SecureClient software.

For further information see [[1]]

42 Troubleshooting

Check the Swivel logs for Turing images and RADIUS requests.

Check the Checkpoint Firewall Logs

radius not supported

This can be seen when using local policies, switch to a Global Policy for RADIUS authentication and test, or for individual users use RADIUS authentication.

43 Known Issues and Limitations

Checkpoint will not accept RADIUS passwords greater than 16 characters in length. If check password with repository is used, then the PIN length will also need to be taken into account, i.e. for a 4 digit PIN, this restricts the length to 12 characters. Two stage RADIUS authentication will bring this back to 16 characters.

44 Additional Information

For assistance in the Swivel installation and configuration please firstly contact your reseller and then email Swivel Secure support at support@swivelsecure.com