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 Vesers 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							
Firewall	Data Loss Prevention	Indeconeole P	Threat Prevention	Anti-Spam & Mail	Mobile Access	44. J	PSec VPN
 Overview Policy Gatewaye Ø Applications Authentication Client Certificates 	Overview Mobile Access My Organ	allows your emplo		nail and connect to intra ring Mobile Access			
			IP Address	Web	Mobile	Desktop	Complia
 ☑ Gapsule Workspace Settings ☑	VLABF	WL002	10.10.110.72			Ξ	N/A
Image: Second Secon	10 9 8 7 6 9	sions on Gateway/	s: Al Gateways	¥ 19:55:30 19:56:00) 19:56:30	19:57:00) 19:57

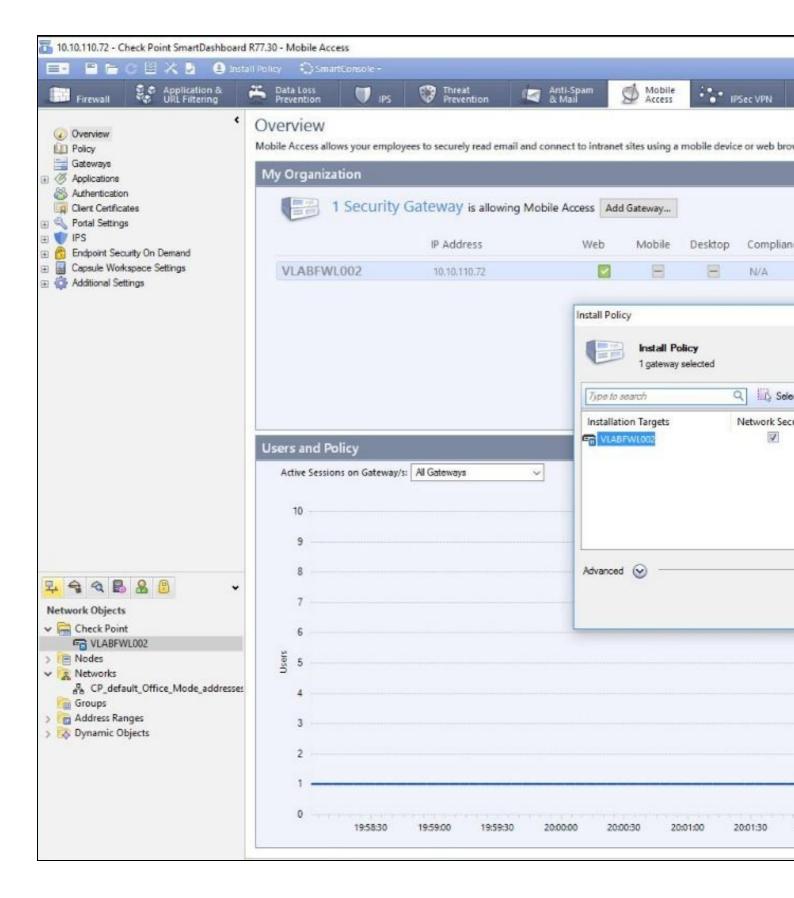
10.10.110.72 - Check Point SmartDashboard R	Policy 💮 Smart					
Firewall	Data Loss Prevention	🛡 ips	Prevention	🔄 Anti-Spam 💆	Mobile Access	PSec VPN
Verview	My Organiza	tion Security	Gateway is allowin IP Address 10.10.110.72	Topology NAT HTTPS Inspection HTTP/HTTPS Proxy Platform Portal	tes using a mobile devi	ce or web br
Additional Settings Additional Settings Network Objects Network Objects Check Point Check Point VLABFWL002 Nodes Networks Address Ranges Address Ranges Dynamic Objects	Users and Po Active Session 10 9 8 7 6 5 4 3 2	licy is on Gateway/s	E Al Gateways	VPN Clients Mobile Access Authentication Office Mode Portal Customizate Portal Settings SSL Clients HTTP Proxy Narve Resolution UnR Translation Endpoint Compliar Orbeck Point Secu Optimizations Ht Count Other	Secure Internal Communication Platform Hardware: Op Software Blades Network Secure Network Secure Policy S Mobile Acc IPS Anti-Bot Anti-Bot Anti-Spam Email Secu Identity Aw	nCertifica en server ity Blades: S y (2) Manag k server sess k trity

10.10.110.72 - Check Point SmartDashboard						
	Data Loss Prevention		Threat Prevention	Anti-Spam & Mail	Mobile Access	IPSec VPN
Firewall Policy Policy Gateways Gateways Authentication Clent Certificates Potal Settings Policy Endpoint Security On Demand Capsule Workspace Settings Additional Settings Additional Settings Additional Settings Additional Settings Solutional Settings Network Objects Solutional Settings	Overview Mobile Access allo My Organiza VLABFW	ws your employ ation 1 Security L002	yees to securely read ema Gateway is allowin IP Address 10.10.110.72	il and connect to intrane Check Point Gateway -	Access et sites using a VLABFWL002 Auther Cor Cettin Cetti	Becvpn
 Check Point VLABFWL002 Nodes Retworks CP_default_Office_Mode_addresses Groups Address Ranges Dynamic Objects 	6 5 4 3 2 1 0	19:54:30	19:55:00 19:55:30	2 19:56:00 19	56:30 19	57:00 19:57:30

💷 🖹 🖬 C 🗄 X 🖟 🕘 Instal		tConsole -		1	-			_
Firewall	Data Loss Prevention	U IPS	Prevention	anti-Spam & Mail		dobile	Par IB	Sec VPN
(Overview	Overview Mobile Access allo My Organiza	tion Security	Gateway is allowing IP Address 10.10.110.72	Check Point Gateway General Propertie Topology NAT HTTPS Inspecti HTTP/HTTPS Inspection Platform Potal Office Mobile Access Authentication Office Mode Portal Custon Portal Setting SSL Clients	- VLABP ss m roxy mizatio gs	WL002 Authenti O C O U RAI G Tw	ication for I ication for I tication Metho Defined on us Jeenand on us DIUS Server General Acc	e or web t Mobile Ar od – er record d password Propertie
Image: Second state Image: Second state	10 9 8 7 6 5 5 4 3 2 1 1	licy ns on Gateway/s		HTTP Proxy - HTTP Proxy - Name Resolution - Link Translation - Endpoint Complian - Check Point Secur ⊡ Logs - Optimizations - Ht Count		Cei S V P	Commerit: Color: Host: Service: Version. Protocol: PAP Priority: 1	

10.10.110.72 - Check Point SmartDashboard						
	II Policy 🕤 Smail A Data Loss Prevention	rtConsole -	Threat Prevention	Anti-Spam & Mail	Mobile Access	IPSec VPN
Overview Policy Gatewaye Ø Applications & Authentication	My Organiza	ition		Host Node - demo.swi		
 Glent Certificates Potal Settings ♥ IPS Capsule Workspace Settings Gasule Workspace Settings Additional Settings 	VLABFW		Gateway is allowin IP Address 10.10.110.72	General Properties Topology NAT FireWall-1 GX Other	s Host Node - Gen Machine Name: IPv4 Address IPv6 Address Comment: Products: Cgnfigure S	demo swivel
Retwork Objects Check Point VLABFWL002 Nodes Networks B CP_default_Office_Mode_addresses Groups Address Ranges Dynamic Objects	Users and Po Active Sessio 10 9 8 7 6 6 5 6 4 3 2 1 1 0	olicy ns on Gateway/	s: All Gateways			

Firewall	Cata Loss Prevention	U IPS	Threat Prevention	ன Anti-Spam		IPSec VPN
Firewall Poicy Gateways Applications Authentication Clent Certificates Potal Settings Pic Poicy Gateways Potal Settings Potal Settings <td>Coverview Mobile Access allo My Organiza VLABFWI</td> <td>tion Security .002</td> <td>rees to securely read email Gateway is allowing IP Address 10.10.110.72</td> <td>and connect to intranet</td> <td>Acce t sites usin VLABFWL Aut Avy tatio</td> <td>g a mobile device or web</td>	Coverview Mobile Access allo My Organiza VLABFWI	tion Security .002	rees to securely read email Gateway is allowing IP Address 10.10.110.72	and connect to intranet	Acce t sites usin VLABFWL Aut Avy tatio	g a mobile device or web
Groups Address Ranges Mynamic Objects	3			<	>	



10.10.110.72 - Check Point SmartDashboard R							
Firewall	Data Loss Prevention		Threat Prevention	Anti-Spam	Mobile Access	11 B	
<	Overview Mobile Access allo My Organiza	ws your employ tion	ees to securely read en	nail and connect to ir	ntranet sites using a r		PSec VPN
Client Certificates Client Certificates Client Certificates Portal Settings Client Security On Demand Client Security On De	VLABFWI		Gateway is allow IP Address 10.10.110.72	ing Mobile Access		Desktop	Complian N/A
CT. 201 , security on country the					Installation Process	- Standard	
					Installation Targets	Version R77.30	Network 🌣 Verify
	Users and Po	olicy ns on Gateway/s	Al Gateways	v	<		
	10 9				Progress Verify	ing	
Retwork Objects Check Point	8				Show Errors		
 VLABFWL002 Nodes Retworks CP_default_Office_Mode_addresses Groups Address Ranges Dynamic Objects 	6 5 4 3 2						
	0 19:58:30	19:59:00	19:59:30 20:	00:00 20:00:30	20:01:00 2	20:01:30	20:02:00

Firewall	Data Loss Prevention	IPS IPS Prevention	Anti-Spam 🖉 Mobile & Mail PSec VPN
 ✓ Overview ✓ Policy ✓ Gateways 	Authenticati	ion Ication Schemes on Gateways	
Applications Authentication Client Certificates Authenticates Authentication Client Certificates Vortal Settings Vortal Settings Portal Seturity On Demand Go Capsule Workspace Settings	Name /	Check Point Password Allowed	SecurID Allowed
π 🤯 Additional Settings	New	Edit Delete	RADIUS Server Properties - General Accounting Name: SwivelClos
	Challenge users t email account or SMS Provider Specify the UF (See the online SMS provider email settings:		oth. Service: UPP NEW Shared Secret: •••••••• Version: RADIUS V Protocol: PAP
Servers and OPSEC Servers Cartery Servers RADIUS SwivelCloud SwivelCloud OPSEC Applications	11000000000		Priority: 1

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

✓ B Swivel Administration Lo × ← → C A Seguro https://dem	no.swivelcloud.com:8080/sentry/	_
😒 swivelsed	oure	
• Login	Swivel Administration Login 🧶	
	Username:	
	OTC: Start Session Login	

🗅 Swivel Configuration 🛛 🗙 🔹 What's My	IP Address? N 🗶
- → C ☆ Seguro https://demo.	swivelcloud.com:8080/sentry/config/radius/nas
😂 swivelseci	ure
<u>Status</u> Log Viewer	RADIUS>NAS 🥹
E Server	Please enter the details for any RADIUS network access servers. A NAS
 Logging Messaging Database Mode Repository RADIUS <u>Server</u> <u>NAS</u> Migration Windows GINA Appliance OATH 	NAS: Metscaler SciscoASA Bob Watchouard Uisbon Forti 300C New Entry Apply Reset
 Config Sync Reporting <u>User Administration</u> <u>Save Configuration</u> <u>Upload Email Images</u> <u>Administration Guide</u> Logout 	

Status LogVilaver Server Ser	C C Seguro https://demo.sv	wivelcloud.com:8080/sentry/config/radius/nas	
Log Viewer 3 Gerver 9 Policy 9 Policy 9 Logging 9 Detabase 9 Mode 9 Repository 9 NAS: 9 NAS: 9 Nassang 9 Nassang <t< th=""><th></th><th>re</th><th></th></t<>		re	
g Berver Please enter the details for any RADIUS network access servers. A h g Holicy NAS: g Messaging NAS: g Database NAS: g Node NAS: g Repository NAS: g Windows GINA Watchouard g Windows GINA Identifier: g Windows GINA Identifier: g Windows GINA Identifier: g Config Sync Group: g Reporting Secret: g Config Sync Group: g Reporting Authentication Mode: y Upload Email Images Change PIN warning: No • Administration Security String after Stage One: Yes • y Logout Allow blank password at Stage One: Yes • Yes + Administration Guide No • Authenticate non-user with just password: No • Logout Allow thank password at Stage One: No • I Administration Authenticate non-user with just password: No • Logout Mo • Authenticate non-user with just password: No • Authenticate non-user with just password: No • I </th <th></th> <th>RADIUS>NAS 🥹</th> <th></th>		RADIUS>NAS 🥹	
B policy B Logging B Mode B Mode B Mode B Repository B RADIUS C RADIUS B NAS: B NAS: B RADIUS B NAS: B RADIUS B Vindows GINA B Appliance B Appliance B Config Sync Group: Change PIN warning: No * User Administration Save Configuration User Administratio			
B Logging NAS: B Luniper M Messaging Immessaging Metscaler G Database Immessaging Immessaging B Mode Immessaging Immessaging B Mode Immessaging Immessaging B Mode Immessaging Immessaging B Mode Immessaging Immessaging B Rob Immessaging Immessaging B Notes Immessaging Immessaging B Notes Immessaging Immessaging B Notes Immessaging Immessaging B Migration Immessaging Immessaging B Appliance Immessaging Immessaging B Apporting Immessaging Immessaging B Config Sync Immessaging Immessay B Noting Itali Images Change PIN warning: No Immessaword I		Please enter the details for any RADIUS networ	k access servers. A N
Junifier Messaging B Messaging B Database B Mode B Repository B RADIUS B RADIUS B Migration B Migration B Windows GINA B Appliance B Appliance B Config Sync B Reporting B Vert Configuration B Vert Configuration B User Administration Administration Administration Administration Guide Allow dark password at Stage One: No マ Administration Guide Allow dark password at Stage One: No マ <td></td> <td>MAC</td> <td></td>		MAC	
B Database Interscalar B Mode Interscalar B Repository Internal IP ranges: B RADIUS Internal IP ranges: B Note Internal IP ranges:		I Juniper	
a Mode B CiscoASA a Repository B & Bob a RADIUS B Watchouard a NASS B Watchouard a NASS B Watchouard a Nass B Usbon FortI 300C a Mindows GINA B a Vindows GINA B a Config Sync Group: a Reporting Secret: a Reporting EAP protocol: a Vuendor Groups): None y Undows Ginal Images Charge PIN warning: a Config Sync Charge PIN warning: a Reporting EAP protocol: Authentication Mode:		<u>Netscaler</u>	
Bepository Bob a RADIUS Watchouard a Saiver Usbon Forti 300C b Migration Iston Forti 300C g Windows GINA Identifier: g Windows GINA Identifier: g Windows GINA Identifier: g Windows GINA Identifier: g Appliance Hostname/IP: g Appliance Group: g Config Sync Group: g Reporting Liser Administration User Administration Authentication Mode: Save Configuration Vendor (Groups): None Upload Email Images Change PIN warning: No Administration Guide Two Stage Auth: No Logout Allow blank password at Stage One: No Vender (Groups): No Vender User Administration Guide No No Logout Allow blank password at Stage One: No Vender (Groups): No Vender User Administration Guide No Vender Logout Allow blank password at Stage One: No User Administratiou		E CiscoASA	
BADIUS B Watchquard • NAS B Usbon Forti 200C a Migration B g Windows GINA B g Appliance Hostname/IP: g Appliance Hostname/IP: g Appliance Group: g CATH Secret: g Config Sync Group: g Config Sync Group: g Config Learning EAP protocol: User Administration Vendor (Groups): Save Configuration Vendor (Groups): Vaload Email Images Change PIN warning: Administration Guide Two Stage Auth: Logout No * Logout Secret: Mile warning: No * Protocol: Vendor (Groups): User Administration Guide Two Stage Auth: Logout No * Allow blank password at Stage One: No * Venk Finabled: No * User Administration Guide No * Logout Allow alternative usernames: No * Allow alternative usernames: No * Authenticate non-user with just password:		E Rob	
 Server NASS Migration Appliance Appliance Config Sync Config Sync Config Sync Reporting User Administration Vendor (Group: Authentication Mode: Save Configuration User Administration Administration Guide Logout No ▼ Logout No ▼ Logout No ▼ Administration Guide Check password at Stage One: Ves ▼ Even if User has Valid String: Ves ▼ Check password with repository: No ▼ Authenticate non-user with just password: No ▼ Allow alternative usernames: No ▼ Alternative username attributes: OTC timeout (mins): O Internal IP ranges: 			
Migration □ a Migration □ a Windows GINA Identifier: CheckPoint Dev a Appliance Hostname/IP: 89.114.238.196 a Config Sync Group:			
a Windows GINA Identifier: CheckPoint Dev a Appliance Hostname/IP: 89.114.238.196 a OATH Secret: ••••••••••••••••••••••••••••••••••••			
a Appliance Hostname/IP: 89.114.238.196 a Config Sync Group:			
a OATH Config Sync Config Sync Reporting User Administration User Administration User Administration Upload Email Images Administration Guide Change PIN warning: No Administration Guide Two Stage Auth: No Administration Guide Change PIN warning: Yes Chack password at Stage One: Yes Ves Ves Ves Ves Ves Ves Ves Ves Ves V		Identifier:	CheckPoint Dev
a Config Sync Secret: ANY a Reporting EAP protocol: ANY User Administration Authentication Mode: ANY Save Configuration Vendor (Groups): None • Upload Email Images Change PIN warning: No • Administration Guide Two Stage Auth: No • Loggout Allow blank password at Stage One: No • Send Security String after Stage One: No • Push Enabled: No • Authenticate non-user with just password: No • Allow alternative usernames: No • I		Hostname/IP:	89.114.238.196
a Reporting EAP protocol: User Administration Authentication Mode: Save Configuration Vendor (Groups): None Upload Email Images Change PIN warning: No Administration Guide Two Stage Auth: No Logout Allow blank password at Stage One: Yes v Even if User has Valid String: Yes v Check password with repository: No Voit Authenticate non-user with just password: No v Internative usernames: Allow alternative usernames: No I I Alternative username attributes: OTC timeout (mins): O I		Secret:	•••••
User Administration Authentication Mode: Save Configuration Vendor (Groups): None • Upload Email Images Change PIN warning: No • Administration Guide Two Stage Auth: No • Logout Allow blank password at Stage One: Yes • Even if User has Valid String: Yes • Check password with repository: No • Push Enabled: No • Username attribute for repository: Image: Alternative username attributes: OTC timeout (mins): O Internal IP ranges: Images: Images:		Group:	ANY
Save Configuration Vendor (Groups): None Upload Email Images Change PIN warning: No Administration Guide Two Stage Auth: No Loggout Allow blank password at Stage One: No Loggout Send Security String after Stage One: Yes Even if User has Valid String: Yes Yes Even if User has Valid String: No Yes Push Enabled: No No Authenticate non-user with just password: No Image: Allow alternative username attributes: Image: Image: OTC timeout (mins): 0 Image: Image:			
Upload Email Images Change PIN warning: No ▼ Administration Guide Two Stage Auth: No ▼ Logout Allow blank password at Stage One: No ▼ Allow blank password at Stage One: Yes ▼ Even if User has Valid String: Yes ▼ Even if User has Valid String: No ▼ Push Enabled: No ▼ Authenticate non-user with just password: No ▼ Allow alternative usernames: No ▼ Allow alternative username attributes: I OTC timeout (mins): 0 Internal IP ranges: I			(11.000 (2.3)
Administration Guide Two Stage Auth: No ▼ Logout Allow blank password at Stage One: No ▼ Allow blank password at Stage One: Yes ▼ 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: I Allow alternative usernames: No ▼ OTC timeout (mins): 0 Internal IP ranges: I			Laborator A. P. C. States and States and
Logout 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: I Allow alternative usernames: No ▼ Allow alternative username attributes: O OTC timeout (mins): 0 Internal IP ranges: I		and the second se	
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:			
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: I Allow alternative usernames: No ▼ Alternative username attributes: I OTC timeout (mins): 0 Internal IP ranges: I	Logout		Land the second s
Check password with repository: No T Push Enabled: No T Authenticate non-user with just password: No T Username attribute for repository: Allow alternative usernames: No T Alternative username attributes: OTC timeout (mins): 0 Internal IP ranges:			
Push Enabled: No ▼ Authenticate non-user with just password: No ▼ Username attribute for repository: No ▼ Allow alternative usernames: No ▼ Alternative username attributes: OTC timeout (mins): 0 Internal IP ranges:			1
Authenticate non-user with just password: No Username attribute for repository: Image: Control (Control (Co			
Usemame attribute for repository: Allow alternative usernames: Alternative username attributes: OTC timeout (mins): Internal IP ranges:			the second s
Allow alternative usernames: No Alternative username attributes: OTC timeout (mins): 0 Internal IP ranges:		Authenticate non-user with just passy	vord: No 🔻
Alternative username attributes: OTC timeout (mins): 0 Internal IP ranges: 0		Username attribute for repository:	T
OTC timeout (mins): 0 Internal IP ranges:		Allow alternative usernames:	No 🔹 🔟
Internal IP ranges:		Alternative username attributes:	
Internal IP ranges:		OTC timeout (mins):	0
			No. T

Testing

in the second

ner dense suit

ald and a

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



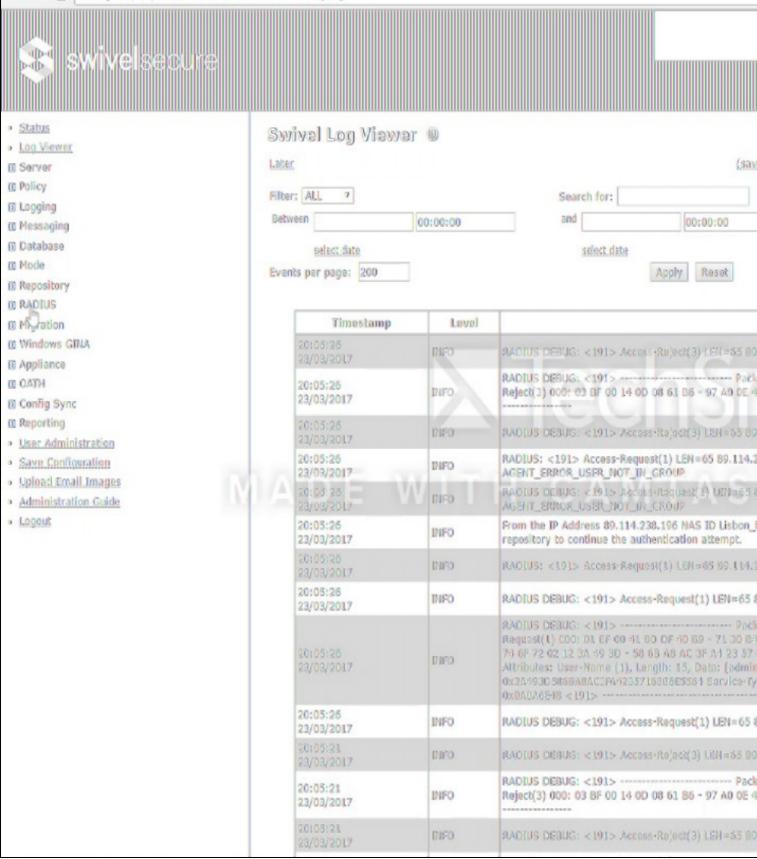
After entering their username and either tabbing away from the username field of clicking the TURing button they will be presented with a TURing image. The PINsafe log should record a session start for that user.

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.

Troubleshooting

Check the Swivel logs for Turing images and RADIUS requests.





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