Table of Contents

1 Bluecoat ProxySG Integration	1
2 Checkpoint Integration	2
3 Overview	
4 Baseline	4
5 Prerequisites	5
6 Gaia Configuration 6.1 Enabling RADIUS Authentication in Gaia	
7 Customising the Gaia Login Page 7.1 Test the RADIUS authentication	
8 Swivel Configuration 8.1 Configuring the RADIUS server	
9 Testing	
10 Troubleshooting	
11 Additional Information	
12 MobileIron Integration	
13 Overview	
14 Prerequisites	
15 How does it work	
16 SwivelSecure Configuration 16.1 Enabling Standard Federation - Sales Force 16.2 Enabling Standard Federation - Office 365	
17 Related Articles	41
18 Additional Information	
19 Symantec Secure Web Gateway Integration	43

1 Bluecoat ProxySG Integration

Bluecoat Proxy SG Guide

2 Checkpoint Integration

PINsafe to Checkpoint Gaia

Integration Notes

3 Overview

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

4 Baseline

Swivel 4.x

Checkpoint Gaia appliance version R77.30.

5 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.

6 Gaia Configuration

6.1 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.

7 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.

7.1 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 A/	ccess					
	l Policy 💮 Sm	iartConsole -	Threat	Anti-Spam	Mobile	12. J	Carlina
Overview Overview Gatewaye Gatewaye Clert Certificates Solution Potal Settings IPS	Overview Mobile Access al My Organiz	llows your emp zation 1 Security	loyees to securely read er y Gateway is allow	mail and connect to intra ving Mobile Access	add Gateway	mobile devic	e or web br
 Endpoint Security On Demand Gapsule Workspace Settings 	VLABEV	VL002	10.10.110.72	web	Mobile	Desktop	N/A
	Users and I	Policy					
	Active Sessi	ions on Gatewa	y/s: Al Gateways	~			
무숙 숙 🗟 🔒 🔋 🗸	8						
Check Point VLABFWL002 Nodes Variation Networks	6 5						
Groups Address Ranges Dynamic Objects	3						
	2						
	0 1	9:54:00 19	9:54:30 19:55:00	19:55:30 19:56:00	19:56:30	19:57:00	19:57

🛅 10.10.110.72 - Check Point SmartDashboard R	77.30 - Mobile Acc	ess			
🔲 🗎 🔚 C 🗏 🗶 🔒 Instati	Policy 🕠 Sma	rtConsole -			
Firewall	Data Loss Prevention	U IPS	Inreat Prevention	Anti-Spam & Mail	Mobile IPSec VPN
Overview Policy Gatewaye Applications Authoritophone	Overview Mobile Access allo My Organiza	ws your emplo	yees to securely read ema	il and connect to intranet : Check Point Gateway - V	sites using a mobile device or web br LABFWL002
 Glent Certificates 	VLABFW	1 Security	Gateway is allowin IP Address 10.10.110.72	Centeral Properties Content of the second s	Check Point Gateway - Gener Machine Name: VLABFWL0 IPv4 Address: 10.10.110.7 IPv6 Address: 10.10.110.7 Comment: Communication Communication Certifica
Retwork Objects Check Point Check Point VLABFWL002 Nodes Retworks Set CP_default_Office_Mode_addresses Groups	Users and Po Active Sessio 10	olicy ns on Gateway/	s All Gatewaya	Link Translation Endpoint Compli Check Point Sec Optimizations Ht Count Other	an Hardware: Open server Cur Software Blades Network Security Blades: S Network Security (2) Manag Firewall IPSec VPN Policy Server Mobile Access IPS Anti-Bot Anti-Virus Anti-Spam & Email Security Identity Awareness Moritoring
> Dynamic Objects	3 2 1 0 19:54:	00 19:54:3	0 19:55:00 19	55:30 19:56:00	> 19:56:30 19:57:00 19:57:30

Coverview Policy Gateways Applications	Overview Mobile Access allows your em My Organization	ployees to securely read email	and connect to intranet site	s using a mobile device or web bro BFWL002
 Authentication Client Certificates Portal Settings IPS Endpoint Security On Demand ECapsule Workspace Settings Additional Settings 	VLABFWL002	IP Address 10.10.110.72	General Properties Good States of the second state	Authentication for Mobile Accer Authentication Method Defined on user record (Le Usemame and password RADIUS SecurID Name / Personal cetti Two-Factor Authent 0 object(s) Global setting
Image: Second system Image: Second system Network Objects Image: Second system Image: Second system Image: Second system Image: Second syst	Users and Policy Active Sessions on Gatev 10 9 8 7 6 5 4 3	vay/s: Al Gateways	Endpoint Complian Check Point Secur Optimizations Hi Count Other	Custom settings

Firewall Strewall	Data Loss Prevention	U IPS	Threat Prevention	Anti-Spam & Mail		obile cess	• IPSec VPN
 Verview Policy Gateways Applications Authentication Clert Certificates Potal Settings Potal Settings Capsule Workspace Settings Capsule Workspace Settings Additional Settings Additional Settings Metwork Objects Check Point Check Point VLABFWL002 Nodes Retworks Retworks Check Point Check Point Check Point Check Point Check Point Retworks Retwork	Overview Mobile Access allo My Organiza VLABFW VLABFW Users and Po Active Sessio 10 9 8 7 6 8 7 6 6 4	ws your employ ntion 1 Security L002	vees to securely read email Gateway is allowing IP Address 10.10.110.72	And connect to intrane Check Point Gateway - General Properties Topology NAT HTTP/INTPS Inspection HTTP/INTPS Inspection Platform Portal VPN Clients Mobile Access Authentication Office Mode Portal Customit Portal Settings SSL Clients HTTP Proxy Name Resoluti Link Translatio Endpoint Comy Other Other	t sites us	sing a mobile of VL002 Authentication O Defined O Useman RADIUS S General Tw RADIUS S General Tw Commer Color: Host: Service: Shared Version Protocol Priority:	device or web bi
> 🐯 Dynamic Objects	2						
	1 <u> </u>	54:30 19:5	5:00 19:55:30 1	9:56:00 19:56:30	19:5	57:00 19:5	57:30 19:50

10.10.110.72 - Check Point SmartDashboard	R77.30 - Mobile Acc	ess rtConsole -				
Firewall	Cata Loss Prevention	U ips	Threat Prevention	Anti-Spam & Mail	Mobile Access	• IPSec VPN
 Overview Policy Gatewaye Applications Authentication Client Certificates Potal Settings Potal Settings Potal Setury On Demand Capsule Workspace Settings Additional Settings 	Overview Mobile Access allo My Organiza	ws your employ ation 1 Security 1002	Gateway is allowin IP Address 10.10.110.72	Host Node - demo.swi General Properties - Topology - NAT - FireWal-1 GX - Other	et sites using a mobile velcloud.com Host Node - C Machine Name: IPv4 Addr	device or web bro ieneral Propertie demo.swivel ess: 52.18.78.73
Image: Production of countrys Image: Product of country of cou	Users and Po Active Sessio 10 9 8 7 6 5 4 3 2 1 1 0 19:54:30	plicy ns on Gateway/ 1955:00	s: All Gateways	00 195630	IPv6 Addr Comment: Products: Cgrfigu 19:57:00 19:57:30	ess:

📑 🖬 🗁 😋 💥 🛃 🙆 Instal	l Policy 🔅 Sma 🏝 Data Loss	rtConsole -	💏 Threat	anti-Spam	A M	obile 1.	
Frewall Application & Weight Direction Policy Gateways Gateways Applications Authentication Clent Certficates Policy Endpoint Security On Demand Endpoint Security On Demand Capsule Workspace Settings Additional Settings	Data Loss Prevention Overview Mobile Access allo My Organiza VLABFW	I Security	vees to securely read email Gateway is allowing IP Address 10.10.110.72	Anti-Spam Check Point Gateway General Propertie Topology NAT HTTPS Inspection HTTP/HTTPS Pri- Platform Portal VPN Clients Mobile Access Authentication Office Mode Portal Custom Portal Setting SSL Clients HTTP Proxy Name Resolu Link Translati Endpoint Com Check Point 3	Market sites us VLABFV R N OXY N Izatio S Secur	abile sing a mobile device VL002 Authentication for I Authentication Metho O Defined on use O Usemame and RADIUS Server General Acc Name: Color: Host:	e or web brind Mobile Acceler ad er record (Lu password Properties ounting SwivelClo Black R dem
Network Objects Check Point Check Point VLABFWL002 Nodes Networks CP_default_Office_Mode_addresses Groups Address Ranges Dynamic Objects	Active Sessio 10 9 8 7 6 7 6 7 6 7 6 7 6 7 6 7 6 7 6 7 6 7 6 7 6 7 6 7 6 7 6 7 6 7 6 7 6 7 6 7 7 6 7 7 6 7 7 6 7 7 6 7 7 6 7 7 7 6 7	ns on Gateway/ 19:55:30	s: All Gateways	Optimizations Hit Count Other	30	Service: Shared Secret Version: Protocol: Priority:	UDP NEW RADIUS Image: state stat

To 10.10.110.72 - Check Point SmartDashboard F	77.30 - Mobile Acces						
💷 🗎 🗁 C 🗏 🗶 🤮 Instal	l Policy 🔹 🕄 Smarte	onsole -					
Firewall	Data Loss Prevention	U ips	Threat Prevention	Anti-Spam & Mail	Mobile Access	- 1P	Sec VPN
Overview Policy Gatewaye Gatewaye Clert Certificates Ortal Settings IPS Fodopiet Security On Demand	Overview Mobile Access allows My Organizati	s your employ on Security (ees to securely read er Gateway is allow IP Address	mail and connect to intr ving Mobile Access	anet sites using a Add Gateway Mobile	n mobile devic	e or web bro
Enclose Vorkspace Settings	VLABFWLO	02	10.10.110.72	E		8	N/A
				Install	Policy Install P 1 gateway	olicy / selected	A I A Sele
				- Inst	allation Taracte		Maturark Sec
	Users and Poli Active Sessions 10 9	cy on Gateway/s	Al Gateways		LABFWL002		
Image: Second	8 7 6 5 4 3 2			Adva	nced ⊙ —		
	0	19:58:30	19:59:00 19:59	:30 20:00:00	20:00:30 21	0:01:00 2	0:01:30

🛅 10.10.110.72 - Check Point SmartDashboard I	R77.30 - Mobile Acc	ess					
	u Polici 🛛 💭 Sma	rtConsole -					
Firewall	Data Loss Prevention	U ips	Prevention	Anti-Spam & Mail	Mobile Access	1 10 IP	Sec VPN
 Overview Policy Gatewaye Ø Applications Authentication Client Certificates Potal Settings IPS 	Overview Mobile Access allo My Organiza	ows your employ ation 1 Security (ees to securely read en Gateway is allow IP Address	nail and connect to in ring Mobile Access W	ntranet sites using a r	nobile devic Desktop	e or web bro Complia
Constant Security On Demand Capsule Workspace Settings	VIAREW	1.002	10 10 110 73			-	NZA
E 🙀 Additional Settings	VLADTV	1.002	10.10.110.72	1			N/A
					Installation Process	- Standard	
					Installation Targets	Version	Network
					TO VLABRIVLUUZ	R/7.30	Verry
	Users and P	olicy					
	Active Sessio	ns on Gateway/s	All Gateways	v	<		
	10			uuw saaraa	Progress		
	9				Verify	ing	
	o				_		
₽ € < B & B · ·	0				Show Errors		
Network Objects	7				-		
🗸 🔚 Check Point	6						
VLABFWL002	Si e						
V R Networks	SD 2						
Groups	4						
> Address Ranges	3						
> Co Dynamic Objects	2						
	-						
	1			dialities and the second			
	0						1.1.1.1.1
	19:58:30	1959:00	1909:30 20:	00:00 20:00:30	20:01:00	20:01:30	20:02:00

10.10.110.72 - Check Point SmartDashbo	erd R77.30 - Mobile Acc	:ess				
Firewall	istall Policy 🐑 Sma Data Loss Prevention	rtConsole -	Threat Prevention	🛛 🖉 Anti-Spam & Mail	Mobile Access	PSec VPN
Overview Delicy Gateways	Authentica Allowed Author	ation Intication Sche	mes on Gateways —			
Applications Authentication Clent Certificates Sector 2 Clent Settings Vortal Settings Vortal Settings Des Endpoint Security On Demand Endpoint Security On Demand Endpoint Security Settings	Name /	02	Check Point Password Allowed		SecuriD Allowed	
					G)IUS Server Properties - eneral Accounting lame: SwivelClou
	New Two-Factor Au Challenge uss email account	Edt	Delete th DynamicID DynamicID one time passw via SMS.	word sent to their	с с +	omment: olor: I Black lost: <u>R</u> demo
	SMS Provi Specify the (See the or SMS provi email settin	URL of your SMS line help for detail for and gs:	ings i provider, your email settir is and examples)	ngs, or both	S S V P	ervice: UDP NEW- hared Secret: ••••••• ersion: RADIUS V rotocol: PAP
Image: Servers and OPSEC Image: Servers Image: Servers	Usemame Password Confirm pa API ID: Advence	ssword:			P	iority: 1 🜩
	S:: Objects List	🖹 Identity Awa	eness 💽 SmartWork	flow		

8 Swivel Configuration

8.1 Configuring the RADIUS server

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

8.2 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.

8.3 Setting up Swivel Dual Channel Transports

See Transport Configuration

Swivel Administration Lo ×	
← → C ☆ Seguro https://demo.sw	vivelcloud.com:8080/sentry/
😒 swivelsecu	re
• Login	Swivel Administration Login 🥘
	Username:
	OTC: Start Session Login

C C Seguro https://demo.seguro.seguro https://demo.seguro.seguro https://demo.seguro.seguro https://demo.seguro.seguro https://demo.seguro https://de	wivelcloud.com:8080/sentry/config/radius/nas
😂 swivelsecu	ire
<u>Status</u>	RADIUS>NAS @
Log Viewer	
E Server	Please enter the details for any RADIUS network access servers. A NAS
9 Policy	
E Logging	NAS:
Messaging	
🗄 Database	H <u>Netscaler</u>
1 Mode	CiscoASA
E Repository	E Rob
RADIUS	Watchguard
<u>Server</u> <u>NAS</u>	E Lisbon Forti 300C
Migration	E New Entry
Windows GINA	
Appliance	Apply Reset
HTAO E	
E Config Sync	
Reporting	
 User Administration 	
 Save Configuration 	
Upload Email Images	
 Administration Guide 	
• Logout	

1943 - C			
😒 swivelsecu	ire		
<u>Status</u> Log Viewer	RADIUS	>NAS 🥹	
Server	Please enter t	the details for any RADIUS network ac	cess servers. A
Policy			
1 Logging	NAS:	Juniner	
Messaging	E .	Nakaalaa	
Database	±	IVELSCALEF	
9 Mode	•	CISCOASA	
Repository	E	Rob	
RADIUS	E	Watchquard	
<u>NAS</u>	E	Lisbon Forti 300C	
Migration			
g Windows GINA		Identifier:	CheckPoint De
Appliance		Hostname/IP:	89.114.238.19
HTAO E		Secret:	
Config Sync		Group:	ANY
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:	No •
		Send Security String after Stage One:	Yes V
		Even if User has Valid String:	Yes V
		Check password with repository:	No •
		Push Enabled:	No •
		Authenticate non-user with just password:	NO V
		Username attribute for repository:	T
		Allow alternative usernames:	No •
		Alternative username attributes:	
		OTC timeout (mins):	0
		Internal IP ranges:	
		Send username in challenge:	No •

9 Testing

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

SOFTWARE TECHNOLOGIES LTD.		Check I	Point Mot
	Please enter your credentials User name User1 OTC TURing 1 2 3 4 5 6 7 8 9 0 5 4 5 7 8 9 0 5 4 5 7 8 9 0	Language:	English
	© Copyright 2004-2015 Check Point Software Technologies L	td. All rights rese	erved.

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.

10 Troubleshooting

Check the Swivel logs for Turing images and RADIUS requests.

	om:8080/sentry/logs				
Swivelseoure					
• <u>Status</u> • <u>Log Viewer</u> © Server m Policy	Swivel Log View Later	27		(sa	
© Logging	Filter; ALL 7		Search for:		
m Messaging	Between	00:00:00	and	00:00:00	
D Database	select.date		select date		
II Mode II Repository	Events per page: 200			Apply Reset	
n RADIUS	Timestamp	Level			
I Windows GINA	20105:25	PU22	a12/112 a22/12		
Appliance	23/03/2017	Lor-3	RADIUS DEBUG: KIMID ACC	iss-surved 3) (En=00 B	
ID OATH ID Config Sync	20:05:26 23/03/2017	INFO	RADIUS DEBUG: <191> Reject(3) 000: 03 BF 00 14 0	0 08 61 B5 - 97 A0 0E	
Reporting User_Administration	20:05:26 23/03/2017	DIFO	RADIUS DEBUG: <191> Acc	ass-Rajact(3) LEN - 55 8	
Save Configuration	20:05:26 23/03/2017	INFO	RADIUS: <191> Access-Reg AGENT_ERROR_USER_NOT_I	uest(1) LEN=65 89.114. N_GROUP	
Administration Guide	20:03:25 23/03/2017	DIF0	RADIUS DEBUG: < 191> AC AGENT_ERROR_USER_NOT_L	sis Request(1) LENa65 N_GROUP	
 rodont 	20:05:26 23/03/2017	INFO	From the IP Address 89.114.238.196 NAS ID U repository to continue the authentication atten		
	20:05:26 23/03/2017	DIFO	RADIUS: <191> Access Reg	ues?(1) LEN=65 09.114.	
	20:05:26 23/03/2017	INFO	RADIUS DEBUG: <191> Acco	ess-Request(1) LEN=65	
	20:05:25 23/03/2017	EIFO	RADIUS DEBUG: <191> Request(1) COO: D1 EF CO 41 74 6F 72 02 12 3A 49 3D - 5 Attributes: User-Name (1), 1 0x3A493D5858A8AC3FA4235 0x0A0A6548 <191>	Pac 80 DF 40 B9 - 71 30 B 8 68 A8 AC 3F A4 23 57 angth: 15, Data: [admi 71588685584 Sarvice-T	
	20:05:26 23/03/2017	INFO	RADIUS DEBUG: <191> Acc	ess-Request(1) LEN=65	
	20:05:21 23/03/2017	DIFO	RADIUS DEBUG: <191> Acc	255+Reject(3) LEH=65 B	
	20:05:21 23/03/2017	INFO	RADIUS DEBUG: <191> Reject(3) 000: 03 BF 00 14 0	Pac D 08 61 86 - 97 A0 05	
	20105121 23/03/2017	0360	RADIUS DEBUG: <191> Acc	oss-Rojoct(3) LEH=65 B	

11 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

12 MobileIron Integration

AuthControl Sentry/Cloud to MobileIron

Integration Notes

13 Overview

Swivel Secure can provide strong and two factor authentication to the Mobile Iron. AuthControl Sentry is a linux based IdP for SAML federations. It is provided as on-prem or Cloud SaaS flavours, providing an adaptative authentication multifactor, managed by a system of points, depending on the factor used and the target app to access. This document outlines the details required to carry this out.

14 Prerequisites

Working MobileIron (MobileIron Sentry appliance) MobileIron Core 9.X and Connector 9.X AuthControl Sentry 4.x

15 How does it work

At App level we use conditional access to Cloud SaaS federated with SAMLv2. The Federated Identity works in 3-way trust with Access between Identity Provider (IDP), Service Provider (SP) and the Access provided by MobileIron AdminPortal/Access Gateway.

16 SwivelSecure Configuration

16.1 Enabling Standard Federation - Sales Force

The standard federation involves just this 3 fields:

• Portal URL: (this Endpoint URL can be found on the Setup -> Security Controls -> Single Sign-On

Settings page in Salesforce.com, listed as ?Salesforce Login URL? under the Endpoints section. It is unique to your Salesforce.com instance and domain.

- Entity ID:, Reflected on SalesForce SSO configuration for My Domain
 Federeated id: That needs to match with the attributed defined on Salesforce.com and Swivel

Rules		
Applications	SAML Applica	tion
Authentication Methods		
View IdP Metadata	Nata: The F	ndepaint UDL is used and u if the ACS (Assortio
Кеуз	i SAML (Secu	rity Assertion Markup Language) request.
Users Active Sessions		
User History	Name	Salesforce
Log Viewer		
General Configuration		
Application Images	Image	Salesforce.png 🗸 🗸
	Points	0
	Portal URL	https://yourdomain.salesforce.com?
	·	
	Endpoint URL	
	Entity ID	https://saml.sentry.salesforce.com
		C
	Federated Id	email

Once that we have a working federation from AuthControl Sentry and the SP, (in the example we will use SalesForce), this is just a standard SalesForce and Custom IdP federation on MI Access console, as the MFA part from Swivel will be triggered once the MI Access has approved the connection. AuthControl Sentry provides a metadata url to quickly get the XML from IdP. It uses POST method for federation.

swivelsecure

Rules

Applications

Authentication Method

View IdP Metadata

Keys

Users Active Sessions

User History

Log Viewer

General Configuration

Application Images

Swivel + SalesForce Demo No description Policy Name: Default Policy

SAML Customization of Mobile Iron settings, Portal URL, Entity ID and Federated ID:



SAML Customization in the Sales Force Side. Settings for Mobile Iron.

SAML Single Sign-On Settings

Back to Single Sign-On Settings

		Edit	Delete	Clone	Download Metadata	SAML
Name	SwivelAccess					
SAML Version	2.0					
Issuer	https://access.mi-labs.es/ e816bccc2905/idp	MobileIro	on/acc/9b	6d9547-	11f8-4a8f-b943-	
Identity Provider Certificate	C=US, ST=California, L= Expiration: 12 Jul 2047 0	Mountain 8:45:42 G	View, O	MobileIr	on, OU=Support, CN=	Signing
Request Signing Certificate	SelfSignedCert_12Jun20	17 17492	25			
Request Signature Method	RSA-SHA256					
Assertion Decryption Certificate	Assertion not encrypted					
SAML Identity Type	Username					
SAML Identity Location	Subject					
Service Provider Initiated Request Binding	HTTP POST					
Identity Provider Login URL	https://access.mi-labs.es/	MobileIro	n/acc/9b	6d9547-	11f8-4a8f-b943-e816b	ccc290
Identity Provider Logout URL	https://ssauth.mi-labs.es:	8443/sen	try/single	logout		
Custom Error URL						
Just-in-time User Provisioning						
User Provisioning Enabled						
Endpoints						
Salesforce Login URL	https://milabses-dev-ed.n	ny.salesfo	rce.com	so=00D	0Y000001ktKL	
OAuth 2.0 Token Endpoint	https://milabses-dev-ed.n	ny.salesfo	rce.com	services	oauth2/token?so=00D	000000
		Edit	Delete	Clone	Download Metadata	SAML

After the application settings definitions have been applied the aplications are available in AuthControl Sentry's web portal.



User Login in Authcontrol Sentry with SalesForce using the MI Account



SSO for SalesForce using Mobile Iron and Turing image from SwivelSecure. This means that the user logs in using the Swivel Secure credentials, by the selected method (in this case Turing image) into the Sales Force (without the need of using Sales Force Credentials).

See 1	sales.user@mi-labs.es		
	Password		
	btc	t~	
5	1 2 3 4 5 6 0 3 1 9 8 4	7 8 9 0	-
			1

Successfull login in Sales Force.



16.2 Enabling Standard Federation - Office 365

In the case of Office365, AuthControl requires that the main federation must be performed with ADFS. On a working federation, a complement has to be installed on ADFS 3.0 server.

	Swivel Authentication Provider Configuration
Settings Language	es Logging Advanced
Swivel URL:	https 🗸 :// ssauth.mi-labs.es : 8443 / proxy
Agent Secret:	Allow self-signed certificates
Confirm Secret:	нинининини
	Allow non-PINsafe users
	Ignore domain prefix
Image Type:	Turing V Auto-show Image
Image Source:	Pinpad
Turing URL:	https://ssauth.mi-labs.es:8443/proxy/SCImage
Pinpad URL:	https://ssauth.mi-labs.es:8443/proxy/SCPinPad
	OK Cancel Save
Swivel ADFS Auther	ntication Provider, version 1.0.6.2, Copyright © Swivel Secure Ltd 2015

There?s a couple of choices depending if the customer is using ADFS Proxy servers or not.

This plugin installs Swivel Secure product as an MFA to be applied via ADFS Authentication Policy Settings.

Set AuthControl Sentry / Swivel Secure as Authentication Provider

		Edit Glo	bal Aut	hentic	ation	Policy)) 		X
Primary	Multi-factor								
Configu Users MFA i	ure multi-factor /Groups s required for t	authentication he following us	(MFA) sett ers and gro	tings. oups:					
ES	Swivel-User-G	roup					[<u>A</u> dd <u>R</u> emove	
Devic MFA i V L	es s required for t Inregistered de legistered dev	he following de wices ices	vices:						
Local MFA i V E	ions s required whe xtranet ntranet	en accessing ap	plications	from the	followir	ng locatio	ins:		
Select to enal	additional auth ble MFA:	entication meth	nods. You	must sele	ect at le	ast one o	of the foll	owing metho	ods
Cer Sw	tificate Auther ivel Authentica	itication ation Provider	-						
What is	s multi-factor a	uthentication?							
				0)K] C.	ancel	Appl	y

On AuthControl Sentry side, we will create an Application configuration with MI Access, IdP and Office365 endpoints:

i Note: The Endpo SAML (Security A	int URL is used only if the ACS (Assertion Consumer Service) is not supplied in the Assertion Markup Language) request.
Name	Office365 secured by MI Access
Image	O365.png V Office 365
Points	100
Portal URL	https://login.microsoftonline.com/login.srf
Endpoint URL	https://access.mi-labs.es/MobileIron/acc/9b7ea0b6-e908-4111-8eb1-946
Entity ID	https://access.mi-labs.es/MobileIron/acc/9b7ea0b6-e908-4111-8eb1-946
Federated Id	userPrincipalName

This way, ADFS will require PINPAD or Turing image in order to validate and access Office365, in addition to ADFS primary authentication policy.

MI LABS ES Login
Welcome ES\office.user For security reasons, we require additional information to verify your account OTC: 1 2 3 4 5 6 7 8 9 0 8 5 1 6 9 3 7 2 0 4
Continue

17 Related Articles

• ADFS configuration

https://kb.swivelsecure.com/w/index.php/Microsoft_ADFS_3_Authentication

18 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

19 Symantec Secure Web Gateway Integration

Media:Swivel_Secure_Symantec_SWG_Integration.pdf