Check Point SandBlast Mobile

SandBlast Mobile Integration With Capsule Workspace – Step-by-Step guide



© 2016 Check PointSoftware Technologies Ltd.

All rights reserved. This product and related documentation are protected by copyright and distributed under licensing restricting their use, copying, distribution, and decompilation. No part of this product or related documentation may be reproduced in any form or by any means without prior written authorization of Check Point. While every precaution has been taken in the preparation of this book, Check Pointassumes no responsibility for errors or omissions. This publication and features described herein are subject to change without notice.

RESTRICTED RIGHTS LEGEND:

Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 and FAR 52.227-19.

TRADEMARKS:

Refer to the Copyright page http://www.Check Point.com/copyright.html for a list of our trademarks. Refer to the Third Party copyright notices http://www.Check Point.com/3rd_party_copyright.html for a list of relevant copyrights and third-party licenses.

SandBlast Mobile Integration With Capsule Workspace – Step-by-Step guide

I.	Intro	oduction	.1
1.	Step	o 1 - Prepare all the prerequisites	.3
2.	Step	2 – Install SANDBLAST MOBILE (SBM) & SANDBLAST MOBILE (SBM)	
Stat	us Te	ester	.4
3.	Step	o 3 – Install and Configure Check Point's Gateway & Management	.5
4.	Step	o 4 – Install Capsule Workspace	.9
5.	Step	5 – Demonstrate SANDBLAST MOBILE (SBM) & Capsule Workspace	
inte	gratic	on and mitigation	10
5	.1.	Test 1 – Wipe data from Capsule Workspace because the device is at High Risk	10
5	.2.	Test 2 – Block Access to Capsule Workspace because the device has no SANDBLAST MOB	ILE
(\$	SBM) in	nstalled	11



I. Introduction

This is a step-by-step guide on how to integrate **Capsule Workspace** with **SANDBLAST MOBILE** (SBM). The integration enables the user to add Check Point **SANDBLAST MOBILE** "Risk Level" as

another enforcement factor in Capsule Workspace.

The Policy enforcement is controlled by the Capsule Workspace administrator (in the Check Point management machine) and could be configured in **GuiDBEdit** (Check Point's Database tool).

I.1. The integration process

The guide will take the user through the following process:



I.2. Architecture

For this demonstration, the user will install SandBlast Mobile Protect & Capsule Workspace on the (2) device, and will connect Capsule Workspace to the (3) Gateway Machine with the Mobile Access Blade. The architecture below describes the entire eco-system of SandBlast Mobile Protect & Capsule Workspace.



I.3. Latest software & documentation

Check Point <u>Capsule Workspace</u> is enabled through connection of mobile devices with Capsule Workspace application to **R77.30 appliance** with activated **Mobile Access Blade**.

This guide explains how to integrate <u>SANDBLAST MOBILE (SBM)</u> & <u>Capsule Workspace</u> based on the assumptions that the user has available <u>Capsule Workspace environment</u>.

For more information on how to create a Capsule Workspace environment, please go to this <u>internal</u> <u>guide</u>.

I.4. Revision History of this document

Date	Ву	Description
26/03/2017	Daniel Dor	First release of the document – based on R77.30 Gateway release
28/05/2017	Daniel Dor	Second release of the document – based on R77.30 Gateway release

1. Step 1 - Prepare all the prerequisites

The following prerequisites should be ready before starting the integration process:

- 1.1. Item 1 SANDBLAST MOBILE (SBM) APK file (2.57 and above) this can be downloaded from SANDBLAST MOBILE (SBM) dashboard using the regular registration process or through the app stores.
- **1.2. Item 2 –** Capsule Workspace APK File (7.1.40 and above) this can be downloaded from the app stores
- **1.3. Item 3 SANDBLAST MOBILE (SBM) Status Tester** (this is optional for testing and relevant only for Android)
- 1.4. Item 4 SANDBLAST MOBILE (SBM) Dashboard
- 1.5. Item 5 GAIA R77.30 with Mobile Access Blade enabled
- **1.6. Item 6 –** Android Device (you can run the same process on iOS, but this guide describes only Android)
- 1.7. Item 7 A Malware

2. Step 2 – Install SANDBLAST MOBILE (SBM) & SANDBLAST MOBILE (SBM) Status Tester

- 2.1. On the device -> Install SandBlast Mobile Protect
 - 2.1.1. On SANDBLAST MOBILE (SBM) Dashboard -> Devices -> "Add new device" -> add your device
 - 2.1.2. ⁽¹⁾ On the device -> get the registration email and download the protect application
 - 2.1.3. \square On the Device -> Activate the protect application
 - 2.1.4. ^(I) On the Device -> Validate that you have no threats on the device and risk level is "No Risk"
- 2.2. ^(S) On the Device -> Install <u>SANDBLAST MOBILE (SBM) Status Tester</u> (this is optional, and will be used to check what is the current status of the SANDBLAST MOBILE (SBM) client)
- 2.3. ^(G) On the Device -> Enter SANDBLAST MOBILE (SBM) Status Tester -> Click on "Get SANDBLAST MOBILE (SBM) Status" -> you should get: "device_risk":"NN" -> This means that the device has no risk



- 3. Step 3 Install and Configure Check Point's Gateway & Management
 - 3.1. On your laptop -> install SmartDashboard (so you will be able to connect to the Check Point Gateway)
 - 3.2. On your laptop -> create a Capsule Workspace environment using this <u>internal guide</u>. You can create the Capsule Workspace environment on **your laptop** or on a **cloud service**. During the installation you will install a GW machine, you will enable Mobile Access Blade, and you will add Active Directory user to the Mobile Access Blade (this user will be used later inside Capsule Workspace).
 - 3.3. On your laptop -> Open the GuiDBedit.exe tool (should be in the following path after you installed SmartDashboard "C:\Program Files (x86)\CheckPoint\SmartConsole\R77.30\PROGRAM\GuiDBedit.exe")
 - 3.4. On GuiDBedit -> Connect to the Gateway with the Mobile Access Blade:



3.4.1. On GuiDBedit -> Click on "Table" -> Click on "Other":



3.4.2. On GuiDBedit -> Click on "Mobile Profiles" -> Click on "Default Profiles":

le View Objects Fields Search Ou	eries Help						
0							
ables Queries	Object	Name	Class Name L	ast Modify Time			
[and a second se	Shoel	ault Profile	mobile profile	un Mar 26 09-09-33 2017			
ips_signatures	- Bill Par	d	parronde policy scheme	Ion Dec 26 15:06:00 2016			
languages	ith nor	uncuve -	passcude_policy_scheme h	ten Dec 20 15:00:00 2010			
log_actions	Envir	missive	passcode_policy_scheme h	ton Dec 20 15:00:00 2010			
log_tield_client_types	LE reor	mai	passcode_policy_scheme h	ton Dec 20 15:06:00 2010			
log_field_server_types							
log_neds							
log_product_objects	120						
ingcious_com	5						
man_security_poncy							
mail_servers							
mgmt_versions_contig							
mime_types_db							
mimes							
mobile_profiles							
mobile_profiles_ruleba	se *						
	<u> </u>						
eld Name	Туре	Value	Valid Values	Default Value	Field description		
contact_fields_to_sync_from_app_to	owned object	contact_fields_to_sync	(contact_fields_to_sync)		Contacts fields to synchronize from applica		
sync_all_contact_fields	boolean	false		true	Synchronize all contact fields		
sync company field	boolean	false			Synchronize company field		
sync email field	boolean	false		true	Synchronize email field		
sync first name field	hoolean	true		true	Sunchronize first name field		
purchase address field	hoolean	false			Sumphropping home address field		
sync_home_address_ned	hoolean	test		Ince	Synchronize home analess need		
synciaschane eventer field	boolean	true		true	Synchronize last name new field		
sync_phone_nomber_nea	boolean	tide	Annual and a state of the second	true	Synchronize phone number neid		
contact_tields_to_sync_from_mail_sr_	owned object	contact_heids_to_sync	(contact_neids_to_sync)		Contacts fields to synchronize mail server t		
sync_all_contact_fields	boolean	true		true	Synchronize all contact fields		
sync_company_field	boolean	false			Synchronize company field		
sync_email_field	boolean	true		true	Synchronize email field		
sync_first_name_field	boolean	true		true	Synchronize first name field		
sync_home_address_field	boolean	false			Synchronize home address field		
sync_last_name_field	boolean	true		true	Synchronize last name field		
sync_phone_number_field	boolean	true		true	Synchronize phone number field		
contacts synchronizetion method	string	mail sry to app	(mail sry to app mail sry to app and devi-	mail sry to app	Contacts synchronizetion method		
future compatibility fields	Rontainer		(future compatibility field NULL)		future compatibility fields		
mail offine interval	unumber	14	1-9999	14	Mail offline interval		
mail offline interval unit	string	Davs	(Davs Weeks Months)	Davs	Unit for mail offline interval numeric value		
max allowed attachments size	unumber	5	1000000	5	Maximum size of attachments allowed for		
may allowed attachments unit	string	MBs	(Butes KBs MBs GBs)	MRc	Unit for sure of maximum allowed attachm		
reminder they location	hoolean	toue	Inling'und'und'anal	toue	Location		
THE REPORT OF THE PARTY OF THE	hasless	tion the second se		true	Charle and Engl Sime		
cominders about shad and 5	puolean	arue		uue	asans anno 200 time		
reminders_show_start_end_time	Doolean	true		true	subject		
reminders_show_start_end_time reminders_show_subject	boolean	true		true	Issue log when device is detected as jail bro		
reminders_show_start_end_time reminders_show_subject report_jail_break_detection		faise			Request the user to send geographic loaction		
reminders_show_start_end_time reminders_show_subject report_jail_break_detection request_user_to_send_geo_location	boolean				Require nerroads to the application		
reminders_show_start_end_time reminders_show_subject report_jail_break_detection request_user_to_send_geo_location require_app_passcode	boolean boolean	true		true	negure passeoue to the application		
reminders_show_start_end_time reminders_show_subject report_ail_break_detection request_user_to_send_geo_location require_app_passcode restrict_attachments_size	boolean boolean boolean	true true		true	Restricts the size of allowed attachments fo		
reminders, show, start_end, time reminders, show, subject report_jail_break_detection request_user_to_send_grea_location require, app_passcode restrict_attachments_size session_timeout	boolean boolean boolean unumber	true true 1	1-43200	true 1	Restricts the size of allowed attachments fo Session timeout		
reminders, show, start, end, time reminders, show, subject report, jail, break, detection request, user, to, send, geo_location require, app, passcode restrict, attachments, size session, timeout session, timeout, unit	boolean boolean boolean unumber string	true true 1 Weeks	1-43200 (Minutes, Hours, Days, Weeks)	true true 1 Weeks	Restricts the size of allowed attachments fo Session timeout Unit for session timeout numeric value		

3.4.3. On GuiDBedit -> Double Click on "Future_compataibility_fields" -> in the opened box click "ok" -> repeat this action 4 times (to create 4 different fields):

1 IF	ave root			C. Strategierer	and the second s	- 9
e view Objects Fields Search	Queries Help					
Ð						
ables Queries			Object Name	Class Name	Last Modify Time	
identity roles			Default_Profile	mobile_profile	Mon Dec 26 15:06:00 2016	
inspect			Restrictive	passcode_policy_scheme	Mon Dec 26 15:06:00 2016	
inspect logs			Permissive	passcode_policy_scheme	Mon Dec 26 15:06:00 2016	
inspect streaming			Normal	passcode_policy_scheme	Mon Dec 26 15:06:00 2016	
install_contracts						
install_state_details						
install_statuses						
ips_attribute_exten	sions					
ips_contexts						
ips_exceptions						
ips_implied_except	tions_tbl					
ips_protections_per	r_profile					
ips_signatures						
tanguages		-				
log_actions		1				
log field rener by	Del .					
ing fields	PIC .					
log product phier	ts					
legcloud conf						
mail security polic	w.					
mail_servers						
mgmt_versions_co	infig					
mime_types_db						
mimes						
mobile_profiles						
mobile_profiles_rul	lebase					
mac_agents						
ncode	105	-				
ncode network annlicatio	Time	*	Valid Valuer	Default Value	Eith devolution	
Id Name	Туре	* Value	Valid Values	Default Value	Field description	
Id Name sync_home_address_field	Type boolean	+ Value false	Valid Values	Default Value	Field description Synchronize home address field	
Id Name sync_home_address_field sync_last_name_field	Type boolean boolean	+ Value faise true	Valid Values	Default Value true	Field description Synchronice home address field Synchronice last name field	
Id Name sync_home_address_field sync_last_mame_field sync_phone_number_field	Type boolean boolean boolean	- Value faise true true	Valid Values	Default Value true true	Field description Synchronica home address field Synchronica pane number field Synchronica pane number field	
id Name sync, home, and dress, field sync, labone, number, field sync, shone, number, field	Type boolean boolean boolean string	value faise true true mail_snc_to_app	Valid Values	Default Value true true true true true true	Field description Synchronice home address field Synchronice that start mer field Synchronice phone number field Centests: andressides method	
Id Name sync, home, address, field sync, jast, name, field sync, phone, number, field entritis, sync, branizetion, northold future compatibility, fields	Type boolean boolean string container ounset obj*	Value false true true mail.or.to.app future future future false future fut fut fut fut fut fut fut	Valid Values (mail_snc_to_app.mail_snc (future_compatibility_field	Default Value true true true true true true true tr	Field description Synchronize home address find Synchronize task name field Synchronize phone monker field Cartesta senschweizelisten Fahrer zerompstänglig fields	;
d Name sync, home, address, field sync, bhome, address, field sync, bhome, umber, field emross, sync, phone, umber, field emross, sync, phone, umber, field sync, phone, umber, field sync, phone, umber, field statute, compatibility, fields	Type boolean boolean boolean string container owned object	value false true true mail_on_to_app future_competibility_field	Valid Values (mail_soc_to_app mail_soc (future_compatibility_field	Default Value true true true true to app and devi mail so: to app (NULL)	Field description Synchronics home address field Synchronics last nume field Synchronics phone number field Contacts, anotheristics method future_competibility_fields	/
dd Name sync, home, address, field sync, bhome, underst, field sync, bhome, underst, field sync, bhome, underst, field sentPits, uncheanizetion, method future, compatibility, fields field, name field under	Type boolean boolean boolean string container owned object string	value faise true true mail_cru_to_app future_compatibility_field	Valid Values (mail_soc_to_app mail_soc (future_compatibility_field	Default Value true true true true (NULL)	Field description Synchrenize home address field Synchrenize home modered Synchrenize photo-modere field Synchrenize photo-modere field Contrals sunchreating for mothered Field synchrenize photomethy field Field synchrenize Fiel	/
d Name sync, home, address, field sync, home, address, field sync, home, number, field emtBs synchronizeison method, future compatibility, fields field yake	Type boolean boolean string container owned object string string	Value false true true true future_competibility_field	Valid Values (mail_src, to_app mail_src (future_compatibility_field	Default Value true true to app and devi- NNUL)	Field description Synchronics home address field Synchronics last name field Synchronics phone number field Cetatest: synchronics on mithod future, compatibility, fields field, name field, name	
d Name sync, loome, address, field sync, last, name, field future compatibility, fields field, name field value	Type boolean boolean boolean string container owned object string string owned object	Value false true true mail_sec_to_app future_compatibility_field future_compatibility_field	Valid Values [mail_crc_to_app_mail_src_ [future_compatibility_field	Default Value true true to app and decimel sv to app (NRLI)	Field description Synchrenize home address field Synchrenize home medier field Synchrenize (home member field Contrals, sunchrenizetion method field, ramme Field, rubut	
d Name sync, home, address, field sync, banwe, field sync, banwe, field sync, banwe, field sync, banwe, field sync, banwe, field sync, banwe, field value field value field value	Type boolean boolean boolean tring container owned object string string owned object string string owned object	Value false true mail.cor.fo.ppp future_compatibility_field future_compatibility_field	Valid Values (mail_sec_to_app mail_sec_ (future_compatibility_field	Default Value true true to app and deimell ov. to app INULL)	Field description Synchronics home arate field Synchronics home number field Centests: supervision method future, compatibility, fields field, sname field, sname field, sname	
d Name neode metanot andiates field sync, bar, and for the second and second sync, bar, and second and second second sync, bar, and second	Type Type boolean boolean boolean string container owned object string owned object string string owned object	Value false true true mail.co.to.app. future_compatibility_field future_compatibility_field	Valid Values (mail_sey, to .app mail_sey (future_compatibility_field	Default Value true true true to app and days, mell sor to app	Field description Synchrenize home address field Synchrenize home moder field Synchrenize phote momber field Contracts sunchrenize(icio momber field, runne Field	
with neede with Name sync, Johne, and east, field sync, Johne, Junne, field sync, Johne, Junne field, Junne field, Junne field, Junne field, Junne field, Junne field, Junne	Type boolean boolean boolean tring container owned object string string owned object string string owned object	Value false true mail.cm.fo.app future_compatibility_field future_compatibility_field	Valid Values (mail_sec_to_app mail_sec (future_compatibility_field	Default Value true true to app and devmail or to app (NULL)	Field decorption Synchronics home address field Synchronics home anderess field Synchronics phone number field Contacts uncertainties method future_compatibility_fields field_runne field_value field	
the second secon	Type boolean boolean string container owned object string string string string tring tring string tring tring	Value false true true mail.cs.to.app future_competibility_field future_competibility_field	Vald Values (mail_sey, to app mail_sey (future_compatibility_field	Default Value true to acc and docmail on to acc (NOLL)	Field description Synchronice home address field Synchronice last runne field Synchronice phone number field Context: Junctionation method Reduct compatibility, fields Field, runne Field,	
with a second se	Type boolean boolean boolean string container owned object string owned object string string string string string	Value false true true mail to to app future_compatibility.field future_compatibility.field future_compatibility.field	Valid Values (mail, so, to, app mail so: (future_compatibility_field	Default Value true true to age and devi mell on to age (NULL)	Field decorption Synchronics home address field Synchronics home address field Synchronics phome number field Contacts any optimisties on mithod future_compatibility_fields field_runne field_vulue field_runne field_vulue field_runne field_vulue	
The secole secol	Ver Type boolean boolean boolean string container owned object string owned object string string owned object string owned object	Value false true true false, competibility, field fature, competibility, field fature, competibility, field fature, competibility, field	Valid Values Imail_orc_to_app.mail_soc (future_compatibility_field	Default Value true true true true true true true tr	Field description Synchronics tast and/res field Synchronics tast and/res field Synchronics phone number field Contests: another field Contests: another field Contests: another field Field, some Fie	
the secole secol	Type boolean boolean boolean dring container owned object string string owned object string string owned object string string owned object string	Value false toue toue malanstan, app. Reture, compatibility, field fature, compatibility, field fature, compatibility, field fature, compatibility, field	Valid Values (mail, ice to app mail re- (haure, compatibility, bird	Default Value true true to age and devi_ mail or to age (NULL)	Field description Synchronics home address field Synchronics home multicered Synchronics phone number field Contacts asynchronics home field Mutrer_compatibility_fields field_runne	
the second secon	VIE Type boolean boolean boolean tring container owned object string strin	Value faite faite toue toue toue toue faiture_competibility_faid faiture_competibility_faid faiture_competibility_faid faiture_competibility_faid	Valid Values (mail.coc.to.ado.mail.coc (Roture, compatibility, field	Default Value true true to area and deci NNRL)	Field description Synchronics home address field Synchronics home address field Synchronics phone number field Contacts anotheristics method Auture competibility_Fields Field_runne Field	
node wroken andress field ync, hone, address, field ync, hone, address, field ync, hone, address, field ync, hone, andress, field ync, hone, andress, field mark, anne, field field, ynne field, ynne	Type boolsan boolsan boolsan container container owned object string owned object string string owned object string owned object string string tring owned object tring owned object tring owned object	Value Value faite faite faiture, compatibility, field faiture, compatibility, field faiture, compatibility, field faiture, compatibility, field faiture, compatibility, field faiture, compatibility, field	Valid Values (mul or, to upp mail or, (feature, compatibility, field	Default Value true to app and defair (NREL)	Field description Synchronics have address field Synchronics have address field Synchronics have more field Contract.ascontinisties method Adure, compatibility, fields field, runne field,	

3.4.4. On GuiDBedit -> Configure the Policy enforcement behavior for Capsule Workspace (The user can enter between 4-9 policy rules):

Rule ID	Is this rule	Field name	Field value	Description of the rule
	mandatory?		(few options)	
0	Mandatory rule	protect_policy_enabled	(1) true	(1) This rule enables the integration between protect & CWS
			(2) false	(2) This rule disables the integration between protect & CWS
1	Mandatory rule	protect_not_activated_action	(1) none	(1) In this case when Protect is not activated, CWS will allow access
			(2) block	(2) In this case when Protect is not activated, CWS will block access
2	Mandatory rule	protect_medium_risk_action	(1) none	(1) In this case when Protect find that the device is at medium risk,
			(2) block	CWS will allow access
			(3) wipe	(2) In this case when Protect find that the device is at medium risk,
				CWS will block access
				(3) In this case when Protect find that the device is at medium risk,
				CWS will wipe the data from the container
3	Mandatory rule	protect_high_risk_action	(1) none	(1) In this case when Protect find that the device is at high risk, CWS
			(2) block	will allow access
			(3) wipe	(2) In this case when Protect find that the device is at high risk, CWS
				will block access
				(3) In this case when Protect find that the device is at high risk, CWS
				will wipe the data from the container
4	Non-Mandatory	protect_not_activated_report	(1) true	(1) In this case when Protect is not activated, CWS will send a report to
	rule		(2) false	the admin
				(2) In this case when Protect is not activated, CWS will not send a
				report to the admin
5	Non-Mandatory	protect_medium_risk_report	(1) true	(1) In this case when Protect find that the device is at medium risk,
	rule		(2) false	CWS will send a report to the admin
				(2) In this case when Protect find that the device is at medium risk,
				CWS will not send a report to the admin
6	Non-Mandatory	protect_high_risk_report	(1) true	(1) In this case when Protect find that the device is at high risk, CWS
	rule		(2) false	will send a report to the admin
				(2) In this case when Protect find that the device is at high risk, CWS
				will not send a report to the admin
7	Non-Mandatory	protect_not_activated_message	(1) free text	(1) In this case when Protect is not activated, CWS will send a custom
	rule			message (with "free text" inside)
8	Non-Mandatory	protect_medium_risk_message	(1) free text	(1) In this case when Protect find that the device is at medium risk,
	rule			CWS will send a custom message (with "free text" inside)
9	Non-Mandatory	protect_high_risk_message	(1) free text	(1) In this case when Protect find that the device is at high risk, CWS
	rule			will send a custom message (with "free text" inside)

3.4.4.1. **Phase 1** – Understand the different types of rules the user can enter

- 3.4.4.2. Phase 2 Adding policy rules For each rule, you will need to add a new field. On the first place, add 4 fields (at minimum you must enter the 4 first rules) -> these are the 4 rules you need to insert (green is the rule, red is the explanation):
 - 3.4.4.2.1. Rule 0 -> protect_policy_enabled -> true -> this enable the SANDBLAST MOBILE (SBM) & CWS Integration

- 3.4.4.2.2. Rule 1 -> protect_not_activated_action -> block -> In this case when Protect is not activated, CWS will block access
- 3.4.4.2.3. Rule 2 -> protect_medium_risk_action -> none -> In this case when Protect find that the device is at medium risk, CWS will allow access
- 3.4.4.2.4. Rule 3 -> protect_high_risk_action -> wipe -> In this case when Protect find that the device is at high risk, CWS will wipe the data from the container:

2.10.100.100 - Cneck Point Database	2 1001			Marrison Rockspace	Const. 1998, 1 and the second lines.		Total No. Supervised	
View Objects Fields Search Q	ueries Hel	2						
tt Queries		Object Name	Class Name I	ast Modify Time				
international	141	Default Profile	mobile profile	un Mar 26 09:09:33 2017				
languager	<u></u>	Restrictive	passcode policy scheme	Mon Dec 26 15:06:00 2016				
log actions		Permissive	passonde policy scheme	Ann Dec 25 15:06:00 2016				
log field client types		Normal	passcode policy scheme	Mon Dec 2615:06:00 2016				
lon field server types								
log fields								
log product objects								
logcloud conf	120							
mail security policy	100							
mail servers								
mamt versions confi	a							
mime types db	·							
mimes								
mobile profiles								
mobile profiles ruleb	ase •							
m								
lame	Type	Value	Valid Values	Default Value	Field description			
sunc all contact fields	hoolean	Inte		true	Synchronize all contact fields			
nunc company field	hoolean	false			Sunchronize company field			
sync_company_nerd	boolean	raise		land.	Synchronize company new			
sync_email/neu	buolean	tibe		uue tees	Synchronize emailmeid			
sync_rist_name_rield	boolean	true		true	synchronize first name field			
sync_home_address_field	boolean	false			Synchronize home address field			
sync_last_name_field	boolean	true		true	Synchronize last name field			
sync_phone_number_field	boolean	true		true	Synchronize phone number field			
ontacts_synchronizetion_method	string	mail_srv_to_app	(mail_srv_to_app,mail_srv_to_app_and_devi.	. mail_srv_to_app	Contacts_synchronizetion method			
ture_compatibility_fields	container		(future_compatibility_field,NULL)		future_compatibility_fields			
	owned of	oject future_compatibility_field						
field_name	string	protect_policy_enabled	0		field_name			
field_value	string	true	V		field_value			
	owned of	ject future_compatibility_field						
field name	string	protect not activated action			field name			
field value	string	block			field value			
	owned of	siect future compatibility field						
field name	string	protect medium risk action	-		field name			
Gald using	stains		2		field ushes			
new_rout	owned of	viert future compatibility field			inda state			
field assess	thing a	sector black side setion			field arms			
neid_name	string	protect_nigh_risk_action	2	1 m	neid_name			
all affiliant internal	Tannig	1 Alexandre	1 0000	-	Mail affine internal			
an_onnine_interval	unumber	14	(Deco Martin Marthal)	Development of the second seco	Wan online interval			
an_omane_incerval_Unit	sung	Days	(Days, weeks, months)	Days	Unit for mail offline interval numeric value			
ax_alloweg_attacnments_size	unumber	3	1~3999999	3	maximum size or attachments allowed for			
ax allowed attachments unit	string	MBS	(Bytes, KBS, MBS, GBS)	MBS	Unit for suze of maximum allowed attachm			
	boolean	true		true	Location			
minders_show_location	boolean	true		true	Start and End time			
minders_show_location minders_show_start_end_time		true		true	Subject			
minders_show_location minders_show_start_end_time minders_show_subject	boolean				ferrors from only one of an interface should be in the little base			
minders_show_location minders_show_start_end_time minders_show_subject port_jail_break_detection	boolean boolean	true		true	Essue log when device is detected as jail bro			
minders_show_location minders_show_start_end_time minders_show_subject uport_jail_break_detection rquest_user_to_send_geo_location	boolean boolean boolean	true faise		true	Request the user to send geographic loaction			
minders_show_location minders_show_start_end_time minders_show_subject port_jail_break_detection quest_user_to_send_geo_location quire_app_passcode	boolean boolean boolean boolean	true false true		true	Request the user to send geographic loaction Require passcode to the application			

3.4.4.3. **Phase 3** – File -> Save all

3.4.5. On your computer -> connect to SmartDashboard -> install policy

- 4. Step 4 Install Capsule Workspace
 - 4.1. ^(G) On the device -> Install Capsule Workspace on the device
 - 4.1.1. Get <u>Capsule Workspace APK File</u> (this version can integrate with SANDBLAST MOBILE (SBM))
 - 4.1.2. Install Capsule Workspace on the device
 - 4.2. ^(S) On the device -> Connect to the Gateway site (with the Mobile Access Blade) -> then access Capsule Workspace using the Active Directory user you've created in step 2 (Mobile Access blade)



4.3. ^(G) On the device -> Validate that you can use Capsule Workspace and all of its applications

5. Step 5 – Demonstrate SANDBLAST MOBILE (SBM) & Capsule Workspace integration and mitigation

- 5.1. Test 1 Wipe data from Capsule Workspace because the device is at High Risk
 - 5.1.1. \bigcirc On the device -> Install a Malware on the device
 - 5.1.2. ^(G) On the device -> SANDBLAST MOBILE (SBM) detects the malware
 - 5.1.3. ⁽⁾ On the device -> Enter SANDBLAST MOBILE (SBM) Status Tester -> Click on "Get SANDBLAST MOBILE (SBM) Status" -> you should get: "device_risk":"HI" -> This means that the device risk is "High"
 - 5.1.4. ^(S) On the device -> Try to enter Capsule Workspace -> Capsule Workspace will not be able to access, and the site will be wiped:

New	/ Connectio	on
(
	OR	
Enter Server Name		
	CONNECT	

- 5.1.5. \bigcirc On the device -> Remove the malware
- 5.1.6. ^(G) On the device -> SANDBLAST MOBILE (SBM) should indicate that the device is clean
- 5.1.7. ^(G) On the device -> Enter SANDBLAST MOBILE (SBM) Status Tester -> Click on "Get SANDBLAST MOBILE (SBM) Status" -> you should get: "device_risk":"NN" -> This means that the device has "no risk"
- 5.1.8. ^(G) On the device -> Connect to the Gateway site (with the Mobile Access Blade) -> then Enter Capsule Workspace using the Active Directory user you've created in step 2 (Mobile Access blade)



5.1.9. ⁽³⁾ On the device -> Capsule Workspace will allow you to get in

5.2. Test 2 – Block Access to Capsule Workspace because the device has no SANDBLAST MOBILE (SBM) installed

- 5.2.1. \bigcirc On the device -> remove SANDBLAST MOBILE (SBM) from the device
- 5.2.2. \bigcirc On the device -> try to enter Capsule Workspace
- 5.2.3. \bigcirc On the device -> Capsule Workspace will block the user from accessing CWS:



- 5.2.4. ^(G) On the device -> install and configure SANDBLAST MOBILE (SBM) again
- 5.2.5. \bigcirc On the device -> try and succeed to enter Capsule Workspace

5.3. Test 3 – Block Access to Capsule Workspace because the device is not registered to SANDBLAST MOBILE (SBM) Dashboard anymore

- 5.3.1. ^(B) On the device -> remove the device from SANDBLAST MOBILE (SBM) Dashboard
- 5.3.2. ^(S) On the device -> try to access SANDBLAST MOBILE (SBM) on the device. You shouldn't be able because the device was deleted from the dashboard:



- 5.3.3. β On the device -> try to enter Capsule Workspace
- 5.3.4. \bigcirc On the device -> Capsule Workspace will block the user from accessing CWS:



- 5.3.5. ^(B) On the device -> install and configure SANDBLAST MOBILE (SBM) again
- 5.3.6. \bigcirc On the device -> try and succeed to enter Capsule Workspace