

# Check Point SandBlast Mobile

---

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

---

Classification: [Confidential]



**Check Point**  
SOFTWARE TECHNOLOGIES LTD.

© 2016 Check Point Software 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 Point assumes 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](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. Introduction ..... 1**
- 1. Step 1 - Prepare all the prerequisites ..... 3**
- 2. Step 2 – Install SANDBLAST MOBILE (SBM) & SANDBLAST MOBILE (SBM) Status Tester ..... 4**
- 3. Step 3 – Install and Configure Check Point’s Gateway & Management ..... 5**
- 4. Step 4 – Install Capsule Workspace ..... 9**
- 5. Step 5 – Demonstrate SANDBLAST MOBILE (SBM) & Capsule Workspace integration 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 MOBILE (SBM) installed ..... 11

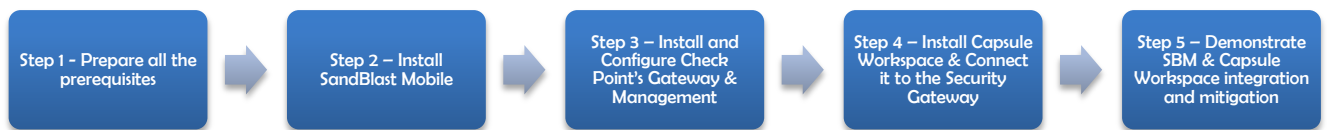
## I. Introduction

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).

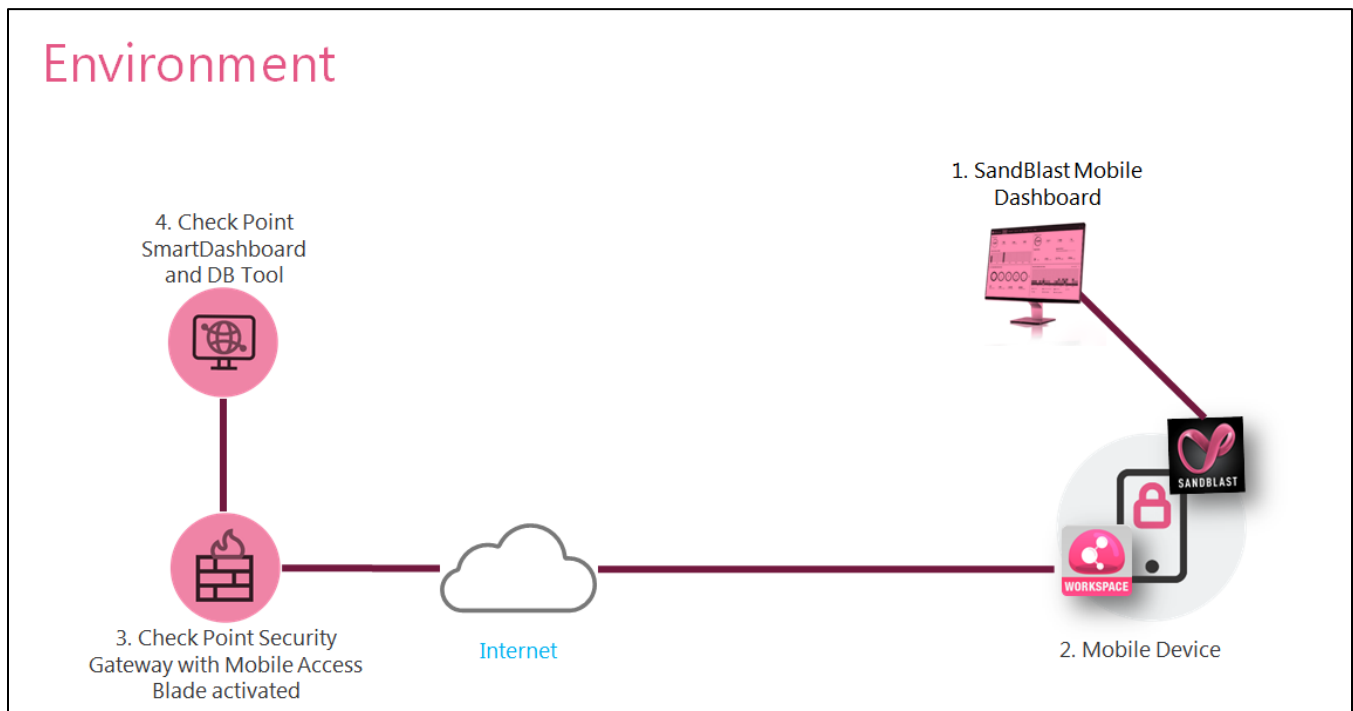
### I.1. The integration process

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 Capsule Workspace 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 SANDBLAST MOBILE (SBM) & Capsule Workspace based on the assumptions that the user has available Capsule Workspace environment.

For more information on how to create a Capsule Workspace environment, please go to this [internal guide](#).

### I.4. Revision History of this document

Date	By	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

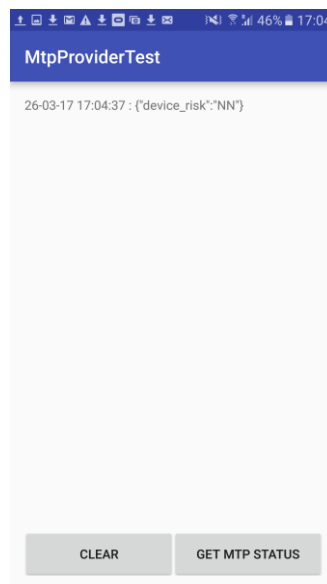
2.1.2.  On the device -> get the registration email and download the protect application

2.1.3.  On the Device -> Activate the protect application





2.1.4.  On the Device -> Validate that you have no threats on the device and risk level is “No Risk”

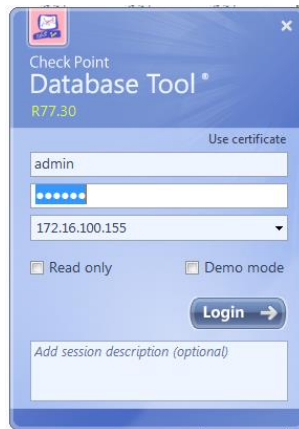
2.2.  On the Device -> Install [SANDBLAST MOBILE \(SBM\) Status Tester](#) (this is optional, and will be used to check what is the current status of the SANDBLAST MOBILE (SBM) client)

2.3.  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

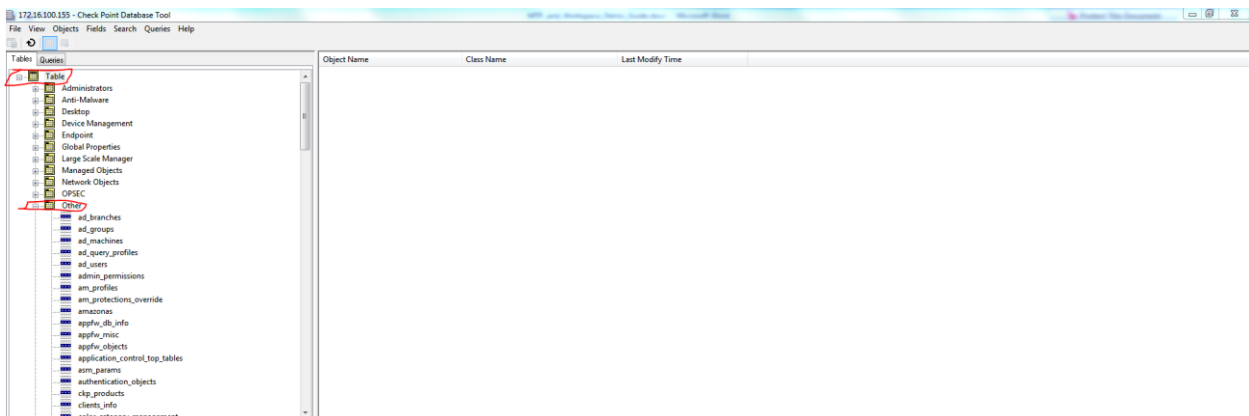


### 3. Step 3 – Install and Configure Check Point’s Gateway & Management

- 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 [internal guide](#). 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:

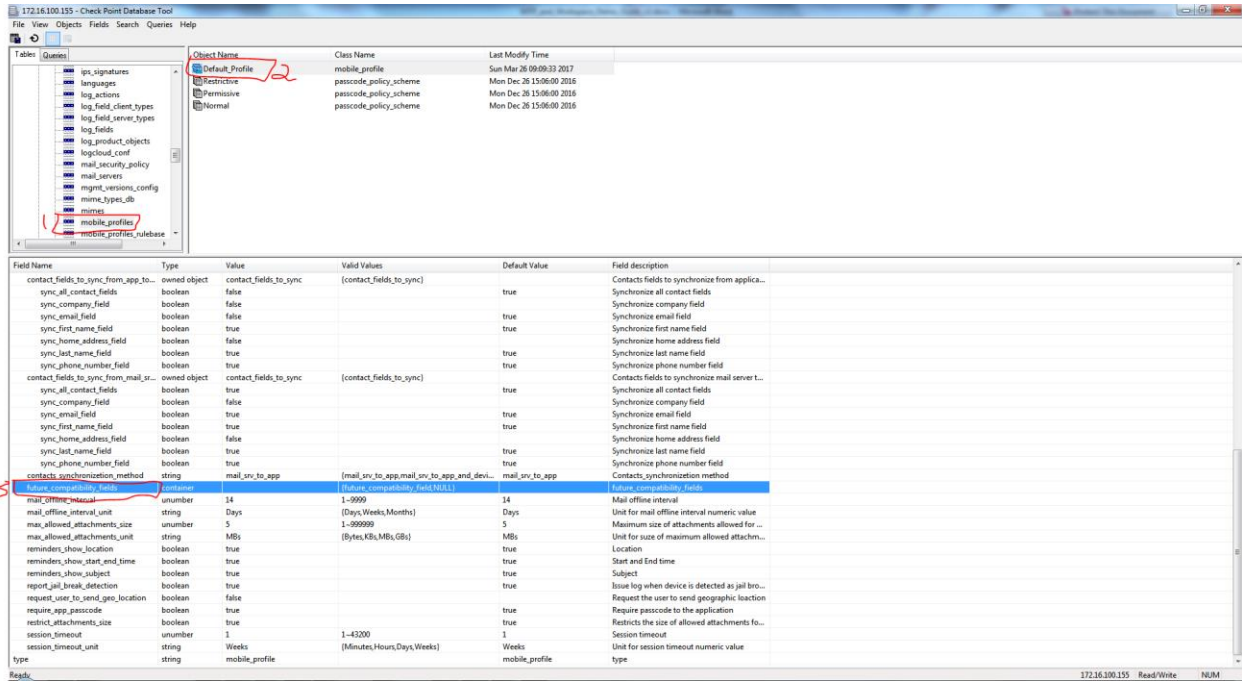


- 3.4.1.  On GuiDBedit -> Click on “Table” -> Click on “Other”:

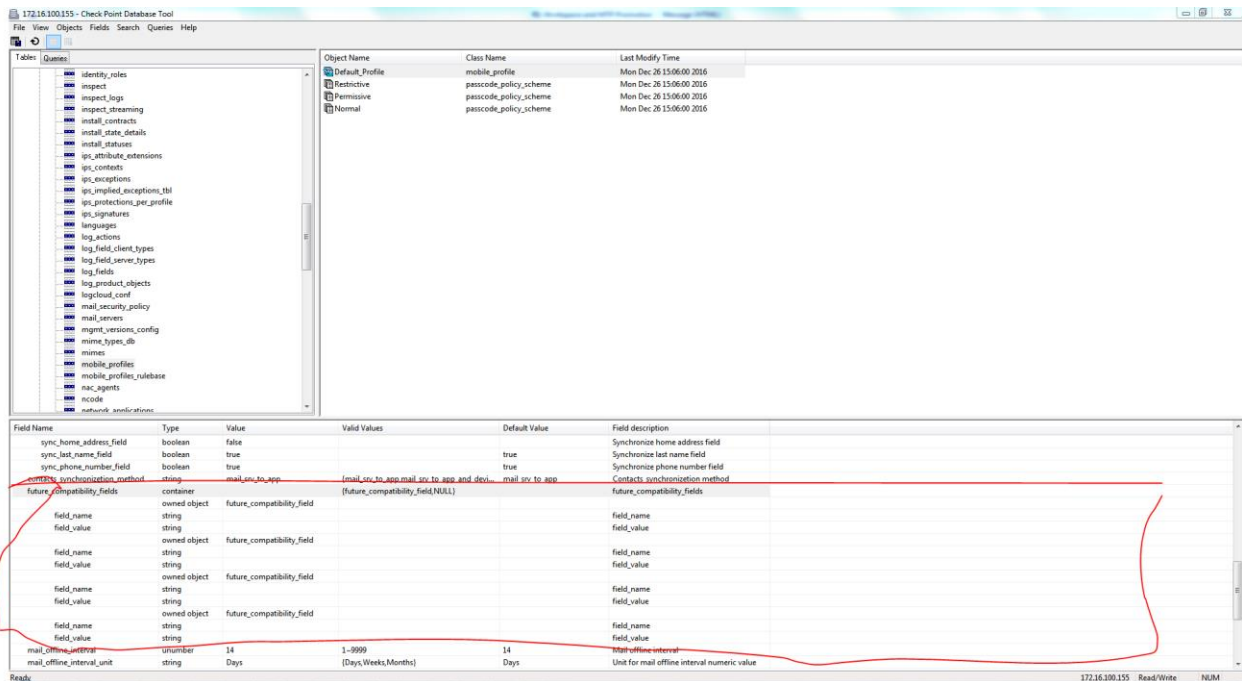


- 3.4.2.  On GuiDBedit -> Click on “Mobile Profiles” -> Click on “Default Profiles”:





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



### 3.4.4. On GuiDBedit -> Configure the Policy enforcement behavior for Capsule Workspace

(The user can enter between 4-9 policy rules):

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

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

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:

Field Name	Type	Value	Valid Values	Default Value	Field description
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_synchronization_method	string	mail_srv_to_app	{mail_srv_to_app,mail_srv_to_app_and_dev... {future_compatibility_field,NULL}	mail_srv_to_app	Contacts_synchronization method
future_compatibility_fields	container	future_compatibility_field			future_compatibility_fields
field_name	string	protect_policy_enabled	0		field_name
field_value	string	true			field_value
field_name	string	protect_not_activated_action	1		field_name
field_value	string	block			field_value
field_name	string	protect_medium_risk_action	2		field_name
field_value	string	none			field_value
field_name	string	protect_high_risk_action	3		field_name
mail_offline_interval	number	14	1-9999	14	Mail offline interval
mail_offline_interval_unit	string	Days	{Days,Weeks,Months}	Days	Unit for mail offline interval numeric value
max_allowed_attachments_size	unumber	5	1-999999	5	Maximum size of attachments allowed for ...
max_allowed_attachments_unit	string	MbS	{Bytes,KbS,MbS,GbS}	MbS	Unit for size of maximum allowed attachm...
reminders_show_location	boolean	true		true	Location
reminders_show_start_end_time	boolean	true		true	Start and End time
reminders_show_subject	boolean	true		true	Subject
report_jail_break_detection	boolean	true		true	Issue log when device is detected as jail bro...
request_user_to_send_geo_location	boolean	false			Request the user to send geographic location
require_app_password	boolean	true		true	Require password to the application
restrict_attachments_size	boolean	true		true	Restricts the size of allowed attachments fo...

3.4.4.3. Phase 3 – File -> Save all

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

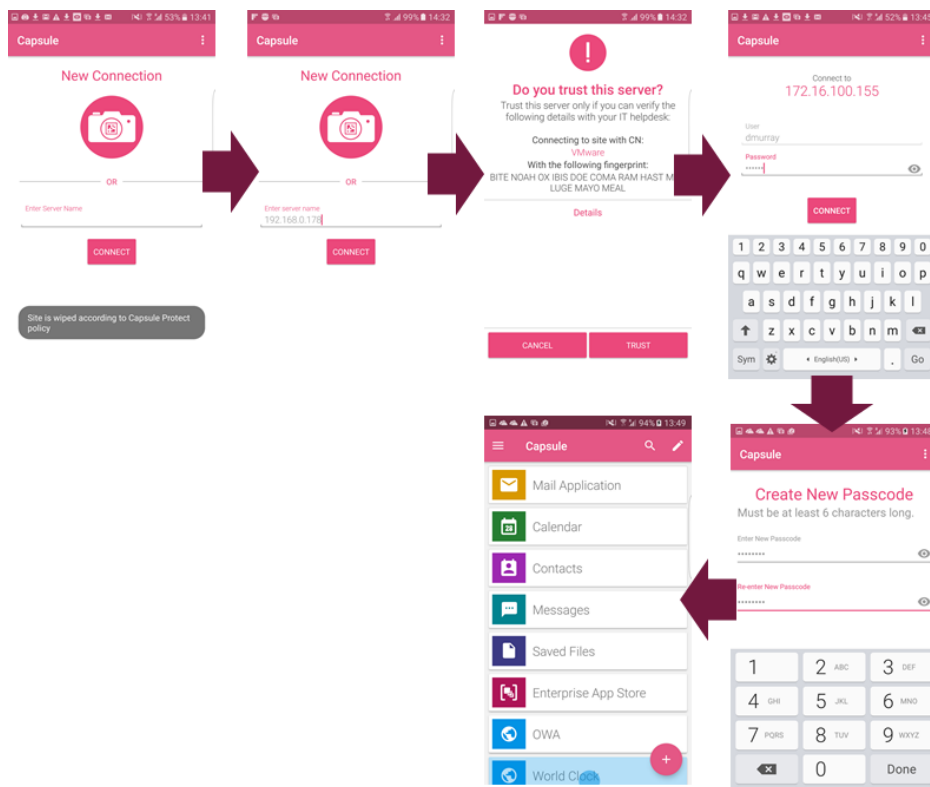
#### 4. Step 4 – Install Capsule Workspace

##### 4.1. On the device -> Install Capsule Workspace on the device

4.1.1. Get [Capsule Workspace APK File](#) (this version can integrate with SANDBLAST MOBILE (SBM))

4.1.2. Install Capsule Workspace on the device

##### 4.2. 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)

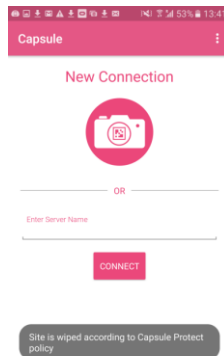


##### 4.3. On the device -> Validate that you can use Capsule Workspace and all of its applications

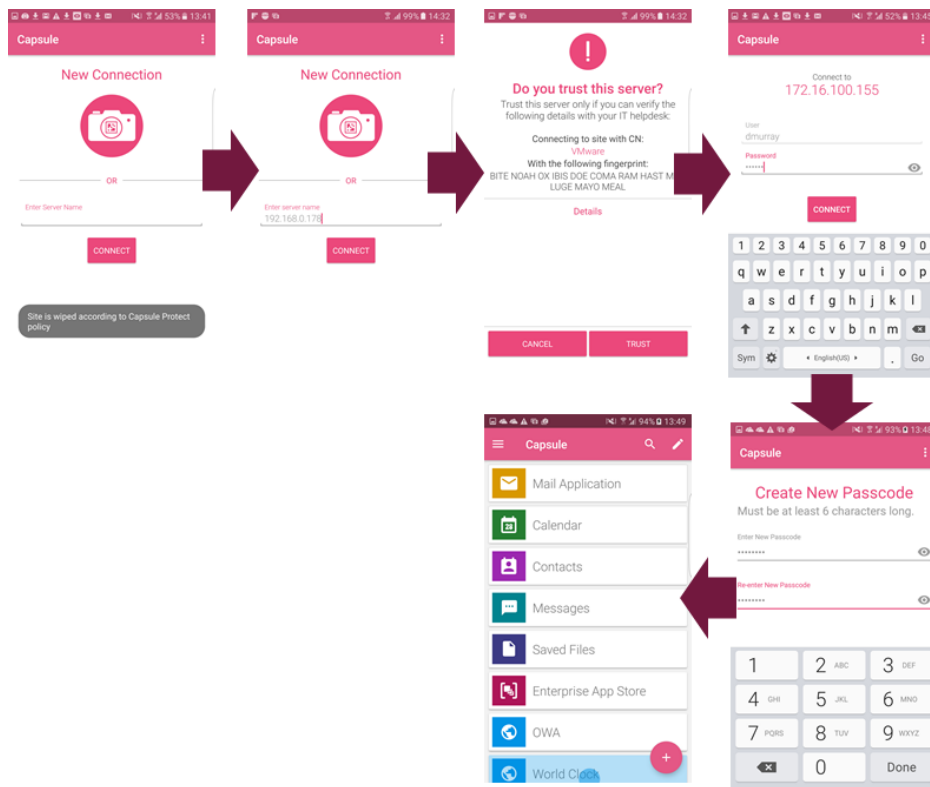
## 5. Step 5 – Demonstrate SANDBLAST MOBILE (SBM) & Capsule Workspace integration and mitigation

### 5.1. Test 1 – Wipe data from Capsule Workspace because the device is at High Risk

- 5.1.1. 🕒 On the device -> Install a Malware on the device
- 5.1.2. 🕒 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. 🕒 On the device -> Try to enter Capsule Workspace -> Capsule Workspace will not be able to access, and the site will be wiped:



- 5.1.5. 🕒 On the device -> Remove the malware
- 5.1.6. 🕒 On the device -> SANDBLAST MOBILE (SBM) should indicate that the device is clean
- 5.1.7. 🕒 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. 🕒 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)



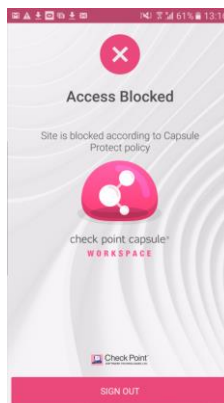
5.1.9. On the device -> Capsule Workspace will allow you to get in

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

5.2.1. On the device -> remove SANDBLAST MOBILE (SBM) from the device

5.2.2. On the device -> try to enter Capsule Workspace

5.2.3. On the device -> Capsule Workspace will block the user from accessing CWS:



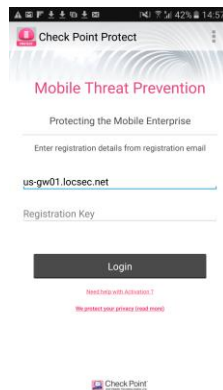
5.2.4. On the device -> install and configure SANDBLAST MOBILE (SBM) again

5.2.5. 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

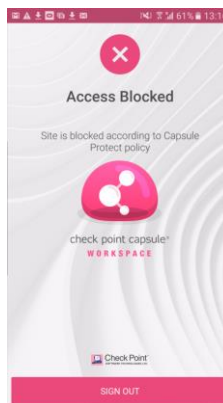
5.3.1. 🕒 On the device -> remove the device from SANDBLAST MOBILE (SBM) Dashboard

5.3.2. 🕒 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. 🕒 On the device -> try to enter Capsule Workspace

5.3.4. 🕒 On the device -> Capsule Workspace will block the user from accessing CWS:



5.3.5. 🕒 On the device -> install and configure SANDBLAST MOBILE (SBM) again

5.3.6. 🕒 On the device -> try and succeed to enter Capsule Workspace