23 July 2020

ENDPOINT SECURITY
VDI

E83.10

Administration Guide
Check Point Copyright Notice

© 2020 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 for a list of our trademarks.
Refer to the Third Party copyright notices for a list of relevant copyrights and third-party licenses.
Important Information

Latest Software
We recommend that you install the most recent software release to stay up-to-date with the latest functional improvements, stability fixes, security enhancements and protection against new and evolving attacks.

Certifications
For third party independent certification of Check Point products, see the Check Point Certifications page.

Check Point E83.10
For more about this release, see the E83.10 home page.

Latest Version of this Document
Open the latest version of this document in a Web browser.

Feedback
Check Point is engaged in a continuous effort to improve its documentation. Please help us by sending your comments.

Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>23 July 2020</td>
<td>Adds executable scripts for Golden Image and Shared Signature Server configurations</td>
</tr>
<tr>
<td>26 May 2020</td>
<td>First release of this document</td>
</tr>
</tbody>
</table>
# Table of Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>5</td>
</tr>
<tr>
<td>Minimal Requirements for Virtual Machines</td>
<td>6</td>
</tr>
<tr>
<td><strong>Configuring Clients for Persistent Desktops</strong></td>
<td>7</td>
</tr>
<tr>
<td>Software Blades for Persistent Desktops</td>
<td>7</td>
</tr>
<tr>
<td>Creating a Basic Golden Image for Persistent Desktops</td>
<td>7</td>
</tr>
<tr>
<td>Client Machine Configuration for Persistent Desktops</td>
<td>7</td>
</tr>
<tr>
<td>Creating a Pool for Persistent Desktops</td>
<td>11</td>
</tr>
<tr>
<td>Assigning Policies to VDI Pools</td>
<td>13</td>
</tr>
<tr>
<td><strong>Configuring Clients for Non-Persistent Desktops</strong></td>
<td>14</td>
</tr>
<tr>
<td>Shared Signatures Server</td>
<td>15</td>
</tr>
<tr>
<td>Set Up the Signatures Server</td>
<td>16</td>
</tr>
<tr>
<td>Manual Setup</td>
<td>16</td>
</tr>
<tr>
<td>Script Setup</td>
<td>16</td>
</tr>
<tr>
<td>Policy Setup</td>
<td>16</td>
</tr>
<tr>
<td>Creating a Basic Golden Image for Non-Persistent Desktops</td>
<td>17</td>
</tr>
<tr>
<td>Client Machine Configuration for Non-Persistent Desktops</td>
<td>18</td>
</tr>
<tr>
<td>Manual Setup</td>
<td>18</td>
</tr>
<tr>
<td>Script Setup</td>
<td>21</td>
</tr>
<tr>
<td>Policy Setup</td>
<td>21</td>
</tr>
<tr>
<td>Creating a Pool for Non-Persistent Desktops</td>
<td>21</td>
</tr>
<tr>
<td>Assigning Policies to VDI Pools</td>
<td>24</td>
</tr>
<tr>
<td>Software Blades for Non-Persistent Desktops</td>
<td>25</td>
</tr>
<tr>
<td><strong>Basic Golden Image Settings</strong></td>
<td>26</td>
</tr>
<tr>
<td><strong>Known Issues</strong></td>
<td>27</td>
</tr>
</tbody>
</table>
Introduction

Virtual Desktop Infrastructure (VDI) is the technology to create and manage virtual desktops. VDI is available as a feature on Check Point's Endpoint Security Client Releases E81.00 (and higher) for Persistent Mode and as a feature on E83.10 (and higher) for Non-Persistent Mode.

A virtual machine monitor (the hypervisor) controls the virtual machine that creates the virtual desktops. All the activity on the deployed virtual desktops occurs on the centralized server.

The "Golden Image" is the base ("Master") desktop image and the model for clone images. Desktop Pools define the server resources for the virtual desktops and solutions to hold the latest Anti-Malware signatures on all the virtual desktops.

Virtual desktop software applications support two modes.

- **Persistent Mode:**
  - Each user has a single specific desktop for their solitary use.
  - Each user’s desktop retains data on the desktop itself between logins and reboots.
  - The user’s machine is not "refreshed" for other users.

- **Non-Persistent Mode:**
  - Each user has a desktop from a pool of resources. The desktop contains the user’s profile.
  - Each user’s desktop reverts to its initial state when the user logs out.
  - The user’s machine is fresh in each instance.

**Note** - Non-Persistent virtual desktops access Anti-Malware signatures in a shared folder in the Shared Signatures Solution.

VMware Horizon 7 version 7.6 and 7.10 are the tested versions. The VMware software between and after these versions should work. Earlier versions may work. Contact Check Point Support for assistance with earlier VMware versions.

The Check Point Management Servers must run on Version R80.10 and higher. See the version support tables in the Persistent and Non-Persistent sections for more information.
Minimal Requirements for Virtual Machines

The Microsoft Windows image must be optimal for VDI.

See the System requirements for installing Windows 10 section on Microsoft's How to Find Windows 10 Computer Specifications & Systems Requirements.

Best Practice - Use an extra 1GHZ "CPU Power" for each scanning machine.
Configuring Clients for Persistent Desktops

**Supported Versions for Persistent Desktops**

- Endpoint Security Client E81.00 (and higher)
- Endpoint Security Server

<table>
<thead>
<tr>
<th>Basic Functionality</th>
<th>Servers Before R80.40</th>
<th>Servers R80.40 and Higher</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disable Periodic Scan</td>
<td>Use Registry</td>
<td>Use Registry</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Use SmartEndpoint + GuiDBedit Tool</td>
</tr>
<tr>
<td>Randomize Periodic Scan</td>
<td>[Not supported]</td>
<td>Use SmartEndpoint + GuiDBedit Tool</td>
</tr>
</tbody>
</table>

**Software Blades for Persistent Desktops**

Persistent virtual desktops have the same Endpoint Security client capabilities as non-virtual desktops.

**Creating a Basic Golden Image for Persistent Desktops**

See [The Golden Image](#) section for the procedure to create a basic golden image.

**Client Machine Configuration for Persistent Desktops**

Configurations for client machines are part of the creation of the Golden Image.

We recommend that you disable Periodic Scan to avoid "Scan Storms".

"Anti-Malware Scan Storms" can occur when anti-virus scans run at the same time on multiple virtual machines on the same physical server. A degradation of system performance is possible that can affect disk I/O and CPU usage.
Setting up the Client Machine for Persistent Desktops

1. We recommend that you disable the Anti-Malware periodic scan. Do it in one of these ways:
   - Manually use registry settings.
     a. Disable Self-Protection.
     b. Disable the scheduled scan in the registry:
        - x64: HKLM\SOFTWARE\Wow6432Node\CheckPoint\EndPoint Security\Anti-Malware\AVSchedOf=(DWORD)0x0b
        - x86: HKLM\SOFTWARE\CheckPoint\EndPoint Security\Anti-Malware\AVSchedOf=(DWORD)0x0b
     c. Restart the machine to restore Self-Protection.
   - Use the Compliance blade to change the registry. See sk132932.
   - Use the SmartEndpoint application R80.40 (or higher).
     Click on the Selected action option.
     Select “Perform periodic anti-malware scan every month” to clear the Perform Periodic Scan box.
- Use the GuiDBedit Application (R80.40 or higher).

2. Enable the Anti-Malware Randomized Scan if you do not disable the Anti-Malware Periodic Scan.

- Use the SmartEndpoint Application (R80.40 or higher).
- Use the GuiDBedit Application (R80.40 or higher).

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Type</th>
<th>Value</th>
<th>Valid Value</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>allow_scan, cancel</td>
<td>boolean</td>
<td>true</td>
<td>true</td>
<td>false</td>
</tr>
<tr>
<td>cover</td>
<td>string</td>
<td>Black</td>
<td>Black</td>
<td>Black</td>
</tr>
<tr>
<td>comments</td>
<td>string</td>
<td>Control Time/periodic...</td>
<td></td>
<td></td>
</tr>
<tr>
<td>randomize scan, interval</td>
<td>boolean</td>
<td>true</td>
<td>true</td>
<td>true</td>
</tr>
<tr>
<td>max scan, cancel, days</td>
<td>number</td>
<td>30</td>
<td>30</td>
<td></td>
</tr>
<tr>
<td>randomize, scan hour, from</td>
<td>string</td>
<td>12:00</td>
<td>(00:00-23:59)</td>
<td>12:00</td>
</tr>
<tr>
<td>randomize, scan hour, to</td>
<td>string</td>
<td>12:00</td>
<td>(00:00-23:59)</td>
<td>12:00</td>
</tr>
<tr>
<td>scan, day, month</td>
<td>number</td>
<td>1</td>
<td>1-28</td>
<td></td>
</tr>
<tr>
<td>scan, day, week</td>
<td>string</td>
<td>Sunday</td>
<td>Sunday,Mond...</td>
<td>Sunday</td>
</tr>
<tr>
<td>scan, hour</td>
<td>string</td>
<td>12:00</td>
<td>00:00-23:59</td>
<td>12:00</td>
</tr>
<tr>
<td>scan, interval</td>
<td>string</td>
<td>month</td>
<td>(month, week)</td>
<td>week</td>
</tr>
<tr>
<td>set, max, scan, cancel, days</td>
<td>boolean</td>
<td>true</td>
<td>true</td>
<td>true</td>
</tr>
</tbody>
</table>
Creating a Pool for Persistent Desktops

This procedure is mandatory to create supported Horizon pools for Persistent Virtual Desktops:

1. In **VMware Horizon**, select **Automated Desktop Pool** in the **Type** panel of **Add Desktop Pool**.

   - **Type**
     - [ ] Automated Desktop Pool
     - [ ] Manual Desktop Pool
     - [ ] RDS Desktop Pool

2. In the **User Assignment** panel, select **Dedicated**.
   
   Check **Enable automatic assignment**.
3. In the **vCenter Server** panel, select **Instant Clones** or **View Composer Linked Clone**. **Full Clones** are not currently supported.

4. In **Guest Customization** panel, select **Allow reuse of pre-existing computer account**.
Assigning Policies to VDI Pools

To assign specific behaviors to blades, you must configure policies. Some policies assign by default to users, not machines. Provision all VDI machines ahead to add them to a policy.

Create a new Computer Group:

- Select the Users and Computers Tab.
- In the Global Action pane, select New Virtual Group.
- Select Computer Group.
- Enter the Group Name and continue.
- Select the relevant machines and click Finish.

Create a policy and assign it to the Computer Group:

- Select the Policy tab.
- Select the relevant policy.
- Select a rule and perform the clone rule operation.
- Select the Connection option.
- Click Next.
- Under the Virtual Directory Structure folder, check the Computer Group newly created.
- Select Next.
- Set the rule action settings.
- Select Next.
- Enter the rule name and comments.
- Select Finish.
Configuring Clients for Non-Persistent Desktops

- Anti-Malware signatures load from the signature server according to policy.
- If the policy server is not available, the client uses signatures from the golden image.
Supported Versions for Non-Persistent Desktops

- Endpoint Security Client E83.10 and higher
- Endpoint Security Server

<table>
<thead>
<tr>
<th>Basic Functionality</th>
<th>Servers Before R80.40</th>
<th>Server R80.40</th>
<th>Servers after R81.00</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disable Periodic Scan</td>
<td>Use Registry</td>
<td>Use Registry</td>
<td>Use Registry</td>
</tr>
<tr>
<td>Configure Shared Signature</td>
<td>Use Registry</td>
<td>Use Registry</td>
<td>Use SmartEndpoint + GuiDBedit Tool</td>
</tr>
</tbody>
</table>

Shared Signatures Server

- Installs as a regular Endpoint Client and becomes a "signature server" later.
  
  **Note** - Create a specific policy in the Endpoint Management Server to configure it.

- Responsible for holding the latest Anti-Malware signatures.
  
  The signatures store in a read-only shared folder and update according to policy.

- Must run on a persistent virtual machine, preferably on the same storage as the clients.

- Must connect to the Endpoint Policy Server or the internet to update signatures.
Set Up the Signatures Server

You can set up the Signature Server as a manual procedure or with a script.

Manual Setup

Create a Shared Folder

- Create a folder to store the shared signatures.
- Share the folder and grant read access to members of the Domain Computers’ group.

Note - On Work-group machines, the SYSTEM account does not have network login rights. This configuration is not supported.

Perform Registry Changes

1. Set the machine as "Shared Signatures Server".
   
   x64: HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\CheckPoint\Endpoint Security\Anti-Malware\VdiSignatureServer=(DWORD)0x01
   
   x86: HKEY_LOCAL_MACHINE\SOFTWARE\CheckPoint\Endpoint Security\Anti-Malware\VdiSignatureServer=(DWORD)0x01

2. Set path to the shared signatures folder.
   
   x64: HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\CheckPoint\Endpoint Security\Anti-Malware\AVSharedBases=(SZ)"C:\Folder\to\share"
   
   x86: HKEY_LOCAL_MACHINE\SOFTWARE\CheckPoint\Endpoint Security\Anti-Malware\AVSharedBases=(SZ)"C:\Folder\to\share"

   Note:
   
   - If the path is not specified, the default shared folder will be:
     "C:\ProgramData\CheckPoint\Endpoint Security\Anti-Malware\bases\shared".
   
   - The folder exists after first successful update.

3. Reboot the machine to restart the Anti-Malware blade.

Script Setup

- Download the Shared Signatures Server Configuration script file.
- Execute the script on the Signature Server and follow the instructions.

Policy Setup

The policy setup is a plan for the future.

Note – Signature Validation: After the machine reboots, wait 20 minutes and make sure the shared signatures folder is populated with Anti-Malware signatures.
Creating a Basic Golden Image for Non-Persistent Desktops

See [The Golden Image](#) section for the procedure to create a basic golden image.
Client Machine Configuration for Non-Persistent Desktops

Configurations for client machines are part of the creation of the Golden Image.
You can set up the client machines (the golden image) as a manual procedure or with a script.

Manual Setup

You can set up the client machines (the golden image) as a manual procedure or with a script.

Setting up the Client Machine for Non-Persistent Desktops

1. We recommend that you disable the Anti-Malware periodic scan. Do it in one of these ways:

   Note - "Anti-Malware Scan Storms" may occur when anti-virus scans run at the same time on multiple virtual machines on the same physical server. A degradation of system performance is possible that can affect disk I/O and CPU usage.

   - Manually use registry settings.
     a. Disable the scheduled scan in the registry:

        x64: HKLM\SOFTWARE\Wow6432Node\CheckPoint\EndPoint Security\Anti-Malware\AVSchedOf=(DWORD)0x0b

        x86: HKLM\SOFTWARE\CheckPoint\EndPoint Security\Anti-Malware\AVSchedOf=(DWORD)0x0b

     b. Restart the machine to restore Self-Protection.

   - Use the Compliance blade to change the registry. See sk132932.
Use the SmartEndpoint application:

Click on the **Selected action** option.

Choose "**Perform periodic anti-malware scan every month**" to clear the **Perform Periodic Scan** box.
Use the GuiDBedit Application

2. Enable "Shared Signatures" scheme.
   
   **x64:** HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\CheckPoint\Endpoint Security\Anti-Malware\AVBasesScheme=(DWORD)0x01
   
   **x86:** HKEY_LOCAL_MACHINE\SOFTWARE\CheckPoint\Endpoint Security\Anti-Malware\AVBasesScheme=(DWORD)0x01
   
3. Setting "Shared Signatures" path.
   
   **x64:** HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\CheckPoint\Endpoint Security\Anti-Malware\AVSharedBases=(SZ)"\\server\sharedsignatures"
   
   **x86:** HKEY_LOCAL_MACHINE\SOFTWARE\CheckPoint\Endpoint Security\Anti-Malware\AVSharedBases=(SZ)"\\server\sharedsignatures"

   **Note** - If the path is not specified, the default shared folder is:
   
   C:\ProgramData\CheckPoint\EndpointSecurity\Anti-Malware\bases\shared
   
   The folder exists after the first successful update.
4. Reboot the machine or restart the Anti-Malware process.

Script Setup

- Download the Golden Image Configuration script file.
- Execute the script on the Golden Image and follow the instructions.

Policy Setup

The policy setup is a plan for the future.

Note - Signatures Recovery:

- When the signatures folder corrupts, you must delete the entire folder.
- After the next signatures update (scheduled or manual), the signatures refresh.

Creating a Pool for Non-Persistent Desktops

This procedure is mandatory to create supported Horizon pools for Non-Persistent Virtual Desktops:

1. In VMware Horizon, choose Automated Desktop Pool in the Type panel of Add Desktop Pool.

<table>
<thead>
<tr>
<th>Add Desktop Pool</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Desktop Pool Definition</strong></td>
<td><strong>Type</strong></td>
</tr>
<tr>
<td>User Assignment</td>
<td>Automated Desktop Pool</td>
</tr>
<tr>
<td>vCenter Server</td>
<td>Manual Desktop Pool</td>
</tr>
</tbody>
</table>

Setting

- Desktop Pool Identification
- Desktop Pool Settings
- Provisioning Settings
- Storage Optimization
- vCenter Settings
- Guest Customization
- Ready to Complete
2. In the **User Assignment** panel, choose **Floating**.
3. In the vCenter Server panel, choose Instant Clones or Linked Clones.

4. In the Provisioning Settings panel, choose Provision all machines up front.

Note - This allows you to assign policies to VDI machines. After the machines are provisioned and assigned to policies, you can reduce provisions.

5. In the Guest Customization panel, select Allow reuse of pre-existing computer account.
Assigning Policies to VDI Pools

To assign specific behaviors to blades, you must configure policies. Some policies assign by default to users, not machines. Provision all VDI machines ahead to add them to a policy.

Create a new Computer Group:
- Select the Users and Computers Tab.
- In the Global Action pane, select New Virtual Group.
- Choose Computer Group.
- Enter the Group Name and continue.
- Select the relevant machines and click Finish.

Create a policy and assign it to the Computer Group:
- Select the Policy tab.
- Select the relevant policy.
- Select a rule and perform the clone rule operation.
- Select the Connection option.
- Click Next.
- Under the Virtual Directory Structure folder, check the Computer Group newly created.
- Select Next.
- Set the rule action settings.
- Select Next.
- Enter the rule name and comments.
- Select Finish.
Software Blades for Non-Persistent Desktops

The Endpoint Security client capabilities for non-persistent virtual desktops are:

- **Anti-Malware**
  - Fully supported when configured with the Shared Signatures Server.

- **Compliance, Firewall and Application Control, Remote Access VPN, and URL Filtering**
  - Fully supported.

- **Forensics**
  - Partially supported.
  - The Forensics database contains data for the current session.
  - Forensics Reports generate as usual.

- **Threat Emulation and Anti-Exploit**
  - Signatures are not in cache.
  - Signatures download for each new instance.

- **Anti-Bot**
  - Signatures are not in cache.
  - Signatures download for each new instance.
  - Cached data (such as the URLs checked against Threat-Cloud and Detection List) are lost on logoff.

- **Ransomware "Honeypots"**
  - Part of the Golden Image.

- **Behavioral Guard**
  - Signatures are not in cache.
  - Signatures download for each new instance.

- **Full Disk Encryption and Capsule Docs**
  - Not supported for non-persistent desktops.
Basic Golden Image Settings

A "Golden Image" is the base ("Master") desktop image. It is the model for clone images.

To Create the Golden Image:
1. Install the OS.
2. Configure the network settings.
   a. Configure the network settings to match your environment settings (DNS, Proxy).
   b. To verify that the configuration is correct, add it to your domain.
   c. Make sure you can ping <domain FQDN>.
   d. Make sure you can ping <Connection Server FQDN>
3. Install software and tools.
4. Install latest Windows updates.
5. Optimize Guest machine in one of two ways:
   a. Optimize master image according to the MS VDI Recommendation.
   b. Download and use the VMware OS Optimization Tool.
6. Install "VMWare Horizon Agent".
   a. Version 7.10 supports up to 19H1.
   b. Make sure that during installation you choose the correct settings (Linked clones or Instant Clones)
7. Endpoint Client.
   Create an exported Endpoint client package and install it as administrator.
   a. The latest Anti-Malware signatures.
      **Recommended** - Update manually with **Update Now** from the Endpoint tray icon at least once a day.
   b. Scan for malwares using the latest Anti-Malware signatures.
      **Recommended** - Scan manually with **Scan System Now** from the Endpoint tray icon for every signature update.
8. Shut Down VM.
9. Save the snapshot.
Known Issues

The current known issues:

- VDI Clients must be part of a domain. Work-group configurations are not supported.
- FDE capability is not supported. Do not install on Non-Persistent VDI machines.
- Tested on Horizon 7.6 and 7.10.
- "Anti-Malware Scanning Storms" may occur when anti-virus scans run at the same time on multiple virtual machines on the same physical server. A serious degradation of system performance is possible that can affect disk I/O and CPU usage.
- To set the policies for VDI clients, provision all of them ahead of time.
- "Repair" push operation does not work for the Non-persistent VDI machine.