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.

Check Point E80.62
For more about this release, see the E80.62 home page http://supportcontent.checkpoint.com/solutions?id=sk108375.

Latest Version of this Document
Download the latest version of this document http://supportcontent.checkpoint.com/documentation_download?ID=47284.
To learn more, visit the Check Point Support Center http://supportcenter.checkpoint.com.

Feedback
Check Point is engaged in a continuous effort to improve its documentation.
Please help us by sending your comments mailto:cp_techpub_feedback@checkpoint.com?subject=Feedback on Endpoint Security Client for Mac E80.62 Release Notes.

Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>10 February 2016</td>
<td>First release of this document</td>
</tr>
</tbody>
</table>
# Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Important Information</td>
<td>3</td>
</tr>
<tr>
<td>Introduction</td>
<td>5</td>
</tr>
<tr>
<td>What’s New</td>
<td>5</td>
</tr>
<tr>
<td>System Requirements</td>
<td>5</td>
</tr>
<tr>
<td>Management Requirements</td>
<td>5</td>
</tr>
<tr>
<td>Supported Product Upgrade Paths</td>
<td>6</td>
</tr>
<tr>
<td>Client Requirements</td>
<td>6</td>
</tr>
<tr>
<td>VPN Server and Gateway Requirements</td>
<td>6</td>
</tr>
<tr>
<td>Build Numbers</td>
<td>6</td>
</tr>
<tr>
<td>Deploying the New Client</td>
<td>7</td>
</tr>
<tr>
<td>Installing the Client</td>
<td>7</td>
</tr>
<tr>
<td>Notes on Installation</td>
<td>8</td>
</tr>
<tr>
<td>Upgrading to OS X 10.11</td>
<td>8</td>
</tr>
<tr>
<td>Uninstalling the Client on Mac</td>
<td>8</td>
</tr>
<tr>
<td>Uninstalling the Media Encryption Offline Tool</td>
<td>9</td>
</tr>
<tr>
<td>Known Limitations</td>
<td>9</td>
</tr>
</tbody>
</table>
Introduction

Check Point Endpoint Security client secures endpoints running OS X. The client secures the endpoint using these software blades:

- Firewall for desktop security
- Compliance
- Full Disk Encryption
- VPN for transparent remote access to corporate resources
- Media Encryption
- Capsule Docs (alpha), from E80.60

The Capsule Docs, Firewall, Compliance, Media Encryption, and Full Disk Encryption blades are centrally managed from SmartEndpoint. The VPN blade is managed by the policy created in SmartDashboard and installed on the gateway.

What's New

This release adds these new features:

- Support for the Endpoint Security client on OS X 10.11 El Capitan
- Support for the Media Encryption Offline Access utility on OS X 10.11 El Capitan
- Support for TLS 1.2

System Requirements

This section describes client, management, and gateway requirements.

Management Requirements

E80.62 Endpoint Security clients for Mac work with these Security Management Servers and Endpoint Security Management Server versions:

- R77.30.01
- R77.30 (not supported for Capsule Docs)
- R77.20.01

Upgrade your servers and SmartConsole to the required version before you deploy E80.62 clients.
Supported Product Upgrade Paths

This release is an upgrade for:

- E80.50.03, E80.60, E80.61, and E80.62 EA for Mac
- Endpoint Security VPN for Mac E75 and higher
- Full Disk Encryption 3.4.4 for Mac and higher

Client Requirements

E80.62 can be installed on these OS X platforms in 64-bit:

- OS X 10.11 El Capitan
- OS X 10.10 Yosemite
- OS X 10.9 Mavericks

VPN Server and Gateway Requirements

<table>
<thead>
<tr>
<th>E80.62 Client Type</th>
<th>Supported Security Management Server</th>
<th>Supported VPN Gateway</th>
</tr>
</thead>
<tbody>
<tr>
<td>Endpoint Security Suite with Remote Access VPN Blade</td>
<td>R77.30.01 - Supports all features</td>
<td>R77 and higher</td>
</tr>
<tr>
<td></td>
<td>R77.20, R77.20.01, R77.30 - Does not support new E80.62 features</td>
<td>R76 and higher</td>
</tr>
<tr>
<td></td>
<td></td>
<td>R71.30 and higher</td>
</tr>
<tr>
<td></td>
<td></td>
<td>R71.50 and higher</td>
</tr>
<tr>
<td>Standalone Endpoint Security VPN for OS X</td>
<td>R77 and higher</td>
<td></td>
</tr>
<tr>
<td></td>
<td>R76 and higher</td>
<td></td>
</tr>
<tr>
<td></td>
<td>R75 and higher</td>
<td></td>
</tr>
<tr>
<td></td>
<td>R71.30 and higher</td>
<td></td>
</tr>
<tr>
<td></td>
<td>R71.50 and higher</td>
<td></td>
</tr>
</tbody>
</table>

For the most up-to-date list of supported operating systems, server and gateway requirements, see: sk67820 http://supportcontent.checkpoint.com/solutions?id=sk67820.

Build Numbers

Build numbers for this release:

- Endpoint Security Client - 860200336
- Media Encryption Offline Access Utility - 860200307

Note - To see the build on your computer, click the client icon on the Menu bar and select Help > About.
Deploying the New Client

Client packages for Mac clients must be distributed manually and do not use Software Deployment.

To get the Mac client package:
2. In SmartEndpoint, in the Deployment tab, select an entity in the Action column and click Load client installer file.
3. Browse to the new client package.
   - For R77.20.01 or R77.30.01: EPS_E80.62_app.zip
   - For R77.30: EPS_E80.62_NC_app.zip
   The selected package is put in the Package Repository.
4. Click Mac Client > Download.
5. In the window that opens, select which blades to include in the package and click OK.
6. Optional: If Remote Access VPN is part of the package, you can configure a VPN site.
7. Select the location to save the package.
   The selected package starts to download.
8. The package shows in the configured location.
   Use a third party distribution method to distribute the ZIP file to endpoint users.

Installing the Client

Make sure users know how to install the client.

To install the Mac client package on client computers:
1. Double-click the ZIP file to expand it.
2. Click the APP file that shows next to the zip file.
   The Check Point Endpoint Security Installer opens.
3. Click Install.
4. Enter a Name and Password to authorize the installation and click OK.
   Wait while package installs.
5. A message shows that the package installed successfully or failed for a specified reason. Click Close.
   If the installation was successful, the Endpoint Security icon shows in the menu bar.
Notes on Installation

If you have included the VPN blade in the deployment package, make sure you meet these requirements:

Network requirements
- You have gateways that support remote VPN access and, if necessary, with the required Hotfix installed on them.
- If Visitor mode is configured on port 443 of a VPN gateway and the gateway’s WebUI is enabled, make sure that the WebUI listens for connections on a port other than 443. Otherwise, the client will not connect.

Keychain Requirements
- Only certificates issued by a public CA can be stored in the keychain password management system by double-clicking the PKCS#12 file.
- If you want users to enter a certificate issued by the ICA into the keychain, they must complete the enrollment process. During enrollment, the client automatically enters the certificate into the keychain.

Upgrading to OS X 10.11

OS X 10.11 can only work with E80.62 clients. Therefore you must upgrade the Endpoint Security client to this version before you can upgrade the operating system.

For Endpoint Security clients that include Full Disk Encryption, see sk108060 http://supportcontent.checkpoint.com/solutions?id=sk108060.

To upgrade an Endpoint Security client computer to OS X 10.11:
1. Upgrade the Endpoint Security client to E80.62.
2. Upgrade the operating system to OS X 10.11.

Uninstalling the Client on Mac

To uninstall the Endpoint Security client on Mac computers:
1. Open a terminal window.
2. Run:
   ```
   sudo "/Library/Application Support/Checkpoint/Endpoint Security/uninstall.sh"
   ```
   If the endpoint was encrypted, the uninstall script first prompts for a reboot so that HFS volumes can be decrypted. After decryption, the script continues to uninstall the client.

After you uninstall the Endpoint Security client, you must reset the computer through SmartEndpoint on the Security Management Server.

Note - We recommend that you run the database backup on a daily basis.
Uninstalling the Media Encryption Offline Tool

To uninstall the Media Encryption offline tool on Mac computers:

1. Open a Terminal window
2. Run
   
   `sudo /Library/Application\Support/Checkpoint/MediaEncryption/uninstall.sh`

Known Limitations

Known limitations for this release are in sk108376