Endpoint Security Client for Mac

E80.61

Release Notes

Classification: [Protected]
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 E80.61
For more about this release, see the E80.61 home page

Latest Version of this Document
Download the latest version of this document
To learn more, visit the Check Point Support Center

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 E80.61 Release Notes).

Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>19 July 2015</td>
<td>First release of this document</td>
</tr>
</tbody>
</table>
Introduction

Check Point Endpoint Security client secures endpoints running Mac 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 Mac OS X 10.10 Yosemite
- Support for the Media Encryption Offline Access utility on Mac OS X 10.10 Yosemite

From E80.60: New Capsule Docs Software Blade (alpha) for Mac

- Compatibility with both Check Point On-Premises deployment and Cloud Deployment
- Enhanced rendering capabilities
- Support unprotecting a document based on user permissions

From R77.20 (and higher): Full Disk Encryption Software Blade new features

- Dynamic Tokens
- Remote Help Response Length

Full Disk Encryption support for In-place major OS upgrade [until September, 2015, this is available only as EA]. See sk106668 http://supportcontent.checkpoint.com/solutions?id=sk106668.
System Requirements

This section describes client, management, and gateway requirements.

Management Requirements

E80.61 Endpoint Security clients for Mac work with R77.20 or higher Security Management Servers and Endpoint Security Management Servers.

To manage the Media Encryption blade, you must have R77.20 or higher Security Management Servers and Endpoint Security Management Servers.

To manage the Capsule Docs blade, you must have R77.20.01 Endpoint Security Management Servers. Contact your Check Point Sales Engineer to learn more about R77 support for Capsule Docs.

Upgrade your servers and SmartConsole to the required version before you deploy E80.61 clients.

Supported Upgrade Paths

This release is an upgrade for:

- Endpoint Security E80.41, E80.42, E80.50, E80.50.03 and E80.60 for Mac
- Endpoint Security VPN for Mac E75 and higher
- Full Disk Encryption R73 for Mac and higher

Client Requirements

E80.61 can be installed on these Mac platforms in 64-bit:

- Mac OS X 10.7 Lion
- Mac OS X 10.8 Mountain Lion
- Mac OS X 10.9 Mavericks
- Mac OS X 10.10 Yosemite

VPN Gateway Requirements

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 number for this release:

Endpoint Security Client: 860100122

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:

1. Download the E80.61 package from sk105123
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: EPS_E80.61_app.zip
   - For R77.20 and R77.30: EPS_E80.61_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.

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.

Known Limitations and Resolved Issues
