Mobile Access Portal Agent

The Check Point Mobile Access Portal offers a variety of on-demand client technologies, including SSL Network Extender, Compliance Scan and Secure Workspace.

The on-demand technologies are downloaded and invoked by the Mobile Access Portal Agent.

For Internet Explorer browsers, the Portal Agent is implemented as an ActiveX control. For all other Web browsers, it is implemented as a Java Plugin, leveraging the Java NPAPI technology.

Java Plugins have been deprecated by the various web browsers, including Chrome, Firefox and Edge.

This release introduces a new Mobile Access Portal Agent technology. It overcomes the limitations described above, and allows the on-demand clients to run on Chrome, Firefox, Edge, and Safari on the Windows, Linux, and macOS platforms.

What’s New

- Edge support on Windows platform.
- Chrome and Safari support on macOS.
- Windows 10 Spring Creators Update support by Secure Workspace.
- Support for Jumbo Hotfix Take 189 and higher.
- Support for Oracle OpenJDK 11.

Note - This Hotfix supports R80.10 Jumbo take 189 and higher. However, future Jumbo takes might include content that will conflict with this Hotfix. Installing such a Jumbo take on a system with this Hotfix will fail with an appropriate error message. If this occurs, please contact the Check Point Technical Support Center.

Installing the Hotfix

Install this release on Security Gateway and cluster members with R80.10 Jumbo Hotfix Take 189.

Make sure all members of a cluster are the same. If you install or uninstall from one cluster member, you must do the same on all the members.

We recommend you use Check Point Update Service Engine (CPUSE) to install this Hotfix. For detailed installation instructions, refer to sk92449 CPUSE - Gaia Software Updates (including Gaia Software Updates Agent) - section (4) “How to work with CPUSE.”

Online installation in Gaia Portal – using CPUSE

1. Take a snapshot of the Security Gateway, to save a backup.
2. Install the latest build of CPUSE Agent from sk92449.
3. Connect to the Gaia Portal on your Check Point machine and navigate to Upgrades (CPUSE).
4. Click Status and Actions.
5. In the upper right corner, click the Add Hotfixes From The Cloud button.
6. Paste the CPUSE Identifier Check_Point_R80.10_jhf_T189_MABDA_sk113410_FULL.tgz and start the search.
7. When the package is found, click the link to add the package to the list of available packages.
8. Select the Hotfix package:
   - On the toolbar, click **More** and then click **Verifier**.
   - Or
     - Right-click on the package name and then click **Verifier**.
9. Select the package: Click the **Install Update** button on the toolbar.
10. The machine reboots automatically.

**Offline installation in Gaia Portal – using CPUSE**

**Note** - Contact Check Point Support to get the offline package.
1. Take a snapshot of the Security Gateway, to save a backup.
2. Install the latest build of CPUSE Agent from **sk92449**.
3. Connect to the Gaia Portal on your Check Point machine and navigate to **Upgrades (CPUSE)**.
4. Click **Status and Actions**.
5. In the upper right corner, click the **Import Package** button.
6. In the **Import Package** window, click **Browse**... and select the CPUSE package (either offline TGZ file, or exported TAR file).
7. Click **Upload**.
8. Select the imported package:
   - On the toolbar, click **More** and then click **Verifier**.
   - Or
     - Right-click on the package name and then click **Verifier**.
9. Select the imported package: Click the **Install Update** button on the toolbar.
10. The machine reboots automatically.

**To install the Hotfix on a Security Gateway with VSX:**

On VSX Gateways, the Hotfix should be installed only using CPUSE in Clish (requires the latest build of CPUSE Agent). For detailed installation instructions, refer to **sk92449 CPUSE - Gaia Software Updates (including Gaia Software Updates Agent) - section (4) “How to work with CPUSE.”**

**Prerequisites for Windows platforms**

To use the on-demand clients of the Mobile Access Portal from a Windows computer, the user must have the Oracle Java Runtime Environment 8 (JRE 8u131 and higher) or the Oracle OpenJDK 11 installed.

If the configuration of the Mobile Access Portal has the ESOD Compliance Scanner enabled, users are required to use Java 32-bit version only. As there is no 32-bit version of OpenJDK, the ESOD Compliance Scanner will not work on Windows computers with OpenJDK 11. The relevant Scanner update will be provided later.

**Prerequisites for Linux platforms**

To browse the Mobile Access Portal from Linux computer the user should have prerequisites described in **sk119772**.

**Prerequisite for macOS platforms**

To use the on-demand clients of the Mobile Access Portal from a macOS computer, the user must have the Oracle Java Development Kit 8 (JDK 8u171 and higher) or the Oracle OpenJDK 11 installed.
Uninstalling the Hotfix

To uninstall the Hotfix from the Security Gateway:

1. Connect to the Gaia Portal on your Check Point machine and navigate to Upgrades (CPUSE).
2. Click Status and Actions.
3. Above the list of all software packages, click Showing Recommended packages and select All.
4. Right-click on the R80.10 Mobile Access Blade Deployment Agent (MABDA) for Chrome and Firefox package and click Uninstall.
5. A warning is displayed that the machine will automatically reboot after the uninstall.
6. Click OK to start the uninstall.

To uninstall the Hotfix from a Security Gateway with VSX:

On VSX Gateways, the Hotfix should be uninstalled only using CPUSE in Clish (requires the latest build of CPUSE Agent). For detailed installation instructions, refer to sk92449 CPUSE - Gaia Software Updates (including Gaia Software Updates Agent) - section (4) "How to work with CPUSE."

Configuration

No configuration is needed on the Security Gateway. The updated Mobile Access Portal Agent will be available immediately after the installation.
Known Limitations

- This Hotfix is only for Security Gateways R80.10 with Jumbo Hotfix Take 189.
- On Linux platforms, the Mobile Access Portal Agent supports only a single end user logged in when installing and using the new portal agent.
- On Linux platforms, the end user must be part of the sudo group and have sudo privileges.
- If the end user’s computer has a proxy server configured, there must be an exception for connections to localhost and 127.0.0.1 IP address. All such connections must bypass the proxy server.
- Users with older Windows 10 operating systems versions might have loopback isolation enabled. These users will experience repetitive installations of Mobile Access Portal Agent. To fix this behavior, the user should run the following command in Windows command line shell (cmd.exe):
  
  CheckNetIsolation LoopbackExempt -a -n="Microsoft.MicrosoftEdge_8wekyb3d8bbwe"

- After uninstalling the Hotfix from the Security Gateway with VSX, the Mobile Access portal may malfunction on virtual systems other than VS0. The administrator should contact Check Point support for the dedicated script to fix this issue.
- After uninstalling the Hotfix, Mobile Access portal and some components will not work. Affected systems:
  
  o All non-VSX after Legacy installation.
  o VS0 on VSX after Legacy installation.
  o VS1+ on VSX which were created AFTER Hotfix Legacy installation.

Fix or workaround:

  o Use CPUSE installation on non-VSX environment.
  o Run `$CVPNDIR/script/cvpn_post_utility.csh` after Legacy uninstall on non-VSX environment.
  o Contact R&D for the dedicated script for VSX environment.