27 September 2018

ENDPOINT SECURITY
CLIENTS FOR ATM
E80.86 AND HIGHER

Deployment Guide
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 https://www.checkpoint.com/products-solutions/certified-check-point-solutions/.

Check Point Endpoint Security
For more about this release, see the Endpoint Security home page http://supportcontent.checkpoint.com/solutions?id=sk117536.

Latest Version of this Document
Download the latest version of this document in PDF format http://supportcontent.checkpoint.com/documentation_download?ID=70165.
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 Clients for ATM E80.86 and Higher Deployment Guide.

Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>27 September 2018</td>
<td>Document now applies to E80.86 and higher</td>
</tr>
<tr>
<td>22 August 2018</td>
<td>First release of this document</td>
</tr>
</tbody>
</table>
### Contents

- **Important Information** ................................................................. 3
- **Introduction to Deploying Clients** .................................................. 5
- **Supported Client Versions** ............................................................. 5
- **Deployment, Installation and Upgrade** .............................................. 5
  - Requirements - Microsoft .NET .......................................................... 6
  - Installing an Endpoint Security Client Package that is Preconfigured for ATMs ... 6
  - Installing an Endpoint Security Client Package that is not Preconfigured for ATM .. 6
  - Upgrading Endpoint Security and Remote Access VPN Clients for ATM ........... 7
    - Supported Upgrade Paths .................................................................. 7
    - Upgrading Remote Access VPN Clients to Endpoint Security Clients .............. 8
    - Upgrading Endpoint Security for ATM Clients .................................... 8
- **Configuring Automatic Remediation** ............................................... 8
- **Troubleshooting** ............................................................................ 9
  - Turning on the Client GUI ............................................................... 9
- **Known Limitations** ....................................................................... 9
Introduction to Deploying Clients

This guide shows you how to deploy the Endpoint Security client for unattended clients, such as ATMs.

An ATM is an automated teller machine for bank customers.

The Endpoint Security client for ATMs does not include these blades and features, which are usually not needed on an ATM:

- Capsule Docs.
- SandBlast Agent for Browsers.

Full Disk Encryption is included. However:

- On BIOS (non-UEFI) systems, there is no pre-boot authentication, because it is an unattended client.
- The volume encryption algorithms 3DES and CAST are not supported.

The Endpoint Security client for ATMs does not have a GUI, and therefore has a smaller installed footprint than the regular client.

Supported Client Versions

The Endpoint Security client for ATM was introduced in E80.86. For the list of supported versions, see the Endpoint Security homepage http://supportcontent.checkpoint.com/solutions?id=sk117536.

Deployment, Installation and Upgrade

Two types of installation package are available for the Endpoint Security client for ATMs:

- **Endpoint Security Client package that is preconfigured for ATMs**
  
  This is the recommended package. It is a complete package for ATM that contains all Blades.

- **Endpoint Security Client package that is not preconfigured for ATMs**
  
  If you only need specific blades, you can deploy a package that is smaller than the complete client for ATM.
  
  There is a selection of client packages available, each with different permutation of blades.
  
  These packages are not preconfigured for ATMs, so you will need to do some manual configuration before installing them.
In this section you will learn how to
1. Download the package.
2. Deploy the package to the clients.
3. Install or upgrade the clients.

Requirements - Microsoft .NET

Before installing or upgrading a client, make sure that Microsoft .NET Framework 4.5 or higher is installed on the ATM machine.

The .NET Framework is needed for SandBlast Agent (Anti-Bot, Forensics, Anti-Ransomware, Threat Emulation, and Anti-Exploit), and to turn on the client GUI for troubleshooting ("Turning on the Client GUI" on page 9).

Installing an Endpoint Security Client Package that is Preconfigured for ATMs

To download the package
1. Go to the Endpoint Security home page
2. Go to Detailed Information per Release > Detailed Client Releases Information.
3. In the row for your client release, go to the Downloads column.
4. Click Show Downloads.

The name of the package is Complete Endpoint Security Client for ATM for 32/64 bit systems

To install the Complete Endpoint Security Client for ATM

Install the complete client using SmartEndpoint. See Deploying Endpoint Security Clients in:
- R77.30.03 Endpoint Security Administration Guide
- R80.20.M1 Endpoint Security Administration Guide

Installing an Endpoint Security Client Package that is not Preconfigured for ATM

There are two ways to configure the ATM machines before installing an Endpoint Security client package that is not preconfigured for ATMs:
- Setting a Registry key (for 64-bit Windows only)
- Running a command

Both ways give the same result. You can use software deployment tools, so there is no need to configure the ATM machine locally. Choose the most convenient way for your organization.
To Download the Package

1. Go to the Endpoint Security home page
   

2. Go to Detailed Information per Release > Detailed Client Releases Information.

3. In the row for your client release, go to the Downloads column.

4. Click Show Downloads.

The name of the package does not have “for ATM” in the name.

To install by setting a registry key on the ATM machines:

1. On ATM machines with 64-bit Windows, add this registry key before deploying the Endpoint Security Client:
   
   HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\CheckPoint\Endpoint Security\isATM=1 (REG_DWORD)

2. Install the complete Endpoint Security client using SmartEndpoint. See Deploying Endpoint Security Clients in:

   - R77.30.03 Endpoint Security Administration Guide

   - R80.20.M1 Endpoint Security Administration Guide

To install by running a command on the ATM machines:

1. Export the package from SmartEndpoint.

2. Use a software deployment tool such as Microsoft SCCM or GPO to distribute the package and install the client using the command line. Run this command with administrator privileges:

   EPS.msi /qb ISATM=1

Upgrading Endpoint Security and Remote Access VPN Clients for ATM

This section explains how to:

- Upgrade Remote Access VPN clients to Endpoint Security.
- Upgrade Endpoint Security clients.

To learn how to install or upgrade Remote Access VPN clients, refer to the Remote Access Clients for Windows 32/64-bit E80.72 and higher Administration Guide


Supported Upgrade Paths

For the supported upgrade paths for Endpoint Security clients and Remote Access VPN clients for ATM, see the:

- Release notes for your destination client version on the Endpoint Security Homepage
  http://supportcontent.checkpoint.com/solutions?id=sk117536, or the

- Home page for Endpoint Security Windows Clients for ATM for your destination client version
Upgrading Remote Access VPN Clients to Endpoint Security Clients

For ATM machines that already have Remote Access VPN client for ATM installed, upgrade to the Endpoint Security for ATM using an exported *preconfigured* package.

This is the only supported upgrade method.

See *Upgrading with an Exported Package* in:

- **R77.30.03 Endpoint Security Administration Guide**  

- **R80.20.M1 Endpoint Security Administration Guide**  

To change the VPN configuration settings in the package, use VPN configuration utility. To learn how to use the utility, search for *Creating Installation Package with VPN Configuration Utility* in the Remote Access Clients for Windows 32/64-bit E80.72 and higher Administration Guide  

To enforce the firewall policy in Endpoint Security client for ATM, use the Firewall Blade which is managed by the Endpoint Security Management Server. Migrate your Desktop Policy rules in SmartDashboard to Endpoint Security Firewall Policy rules in SmartEndpoint. To do that, you must manually define the rules in the Endpoint Security Firewall Policy.

Upgrading Endpoint Security for ATM Clients

The procedure for upgrading Endpoint Security for ATM clients from a lower version to the current version of Endpoint Security for ATM, is the same as the procedure for upgrading a regular Endpoint Security client.

To learn how to upgrade, see *Upgrading with Deployment Rules* in:

- **R77.30.03 Endpoint Security Administration Guide**  

- **R80.20.M1 Endpoint Security Administration Guide**  

You cannot change the VPN configuration settings in the package during software deployment.

**Configuring Automatic Remediation**

If there is a ransomware attack on ATMs, the administrator is unlikely to be able to manually restore files on the machines. This is because (by default) the Endpoint Security client for ATMs does not have a GUI for Anti-Ransomware Restoration. Also, it is not practical to give individual attention to a large number of ATMs.

We recommend that you configure SmartEndpoint so that the Endpoint Security clients for ATMs:

- Automatically restore files after a ransomware attack.
- Analyze incidents based on the Check Point recommended triggers, and apply remediation automatically.
To configure automatic file restoration and infection remediation:

1. In SmartEndpoint click the **Policy** tab.
2. From a SandBlast Agent Forensics and Anti-Ransomware rule, right-click the **Anti-Ransomware Backup Settings** action and select **Edit Shared Action**.
3. Select **Anti-Ransomware Automatic Restore and Remediate**.
4. Click **OK**.
5. In the SandBlast Agent Forensics and Anti-Ransomware rule, hover over the Action with the icon. It has the tooltip **Triggers and Automatic Response**.
6. Select **Automatically analyze and remediate infections**.
7. Install the Policy.

### Troubleshooting

#### Turning on the Client GUI

The GUI of the Endpoint Security client for ATMs (the yellow lock icon in the tray) does not show by default.

You can turn on the GUI if you need to do routine maintenance or to troubleshoot problems.

**Note** - Microsoft .NET Framework 4.5 or higher is needed to turn on the client GUI. Make sure it is installed on the ATM machine.

**To turn on the GUI of the Endpoint Security client:**

On a 32-bit systems run:

C:\Program Files\CheckPoint\Endpoint Security\UIFramework\Bin\cptrayUI.exe

On a 64-bit system, run

C:\Program Files (x86)\CheckPoint\Endpoint Security\UIFramework\Bin\cptrayUI.exe

**Note** - in the client GUI, the Remote Access VPN blade is grayed-out and shows as **Installed**. You cannot change the Remote Access VPN properties from the GUI.

**To shut down the GUI of the Endpoint Security client:**

Right click the lock icon in the tray and select **Shutdown**.

### Known Limitations

Limitations in previous releases apply unless explicitly shown as resolved. For the Known Limitations for your client release, see the *Endpoint Security homepage*