1.1. Giới thiệu tài liệu
Tài liệu nhằm mục đích hướng dẫn người dùng trong việc cài đặt, sử dụng phần mềm RAR-EP.
Phần mềm RAR-EP là phần mềm được cài đặt tại các máy trạm địa phương, có thể quản lý các thông tin:
Cấu hình máy và địa chỉ của máy trạm
Thiết bị ngoại vi đang cắm trên máy trạm
Phần mềm đang cài đặt trên máy trạm
Lịch sử website đã truy cập trên máy trạm
Phần mềm hỗ trợ trong việc xét duyệt máy trạm và các thiết bị ngoại vi cần truy cập hệ thống theo các cấp quản lý địa phương.
2.1.1. Cài đặt lần đầu tiên
Mục đích để người dùng nắm chi tiết các bước và các lưu ý trong việc cài đặt ứng dụng trên máy trạm lần đầu tiên
Bước 1: Mở Bkav → Tùy chọn (Nâng cao) → Phòng vệ chủ động → Bỏ tick Self Defense và chọn tắt → OK
Bước 2: Vào RUN → Gõ: regedit → Vào Computer\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Bkav → Xóa key: fNeedUninstallPass
Bước 3: Bật BMVPN, truy cập vào đường dẫn http://tailieu.dancuquocgia.bca/rarep → Tải Rar-Installer Setup phiên bản mới nhất
Kiểm tra trên máy tính nếu đã cài phần mềm Kaspersky Security Agent 3.12 thì tải và chạy file “netagent-change-server.bat”
Bước 4: Mở ứng dụng Rar-Installer Setup
Bước 5: Ứng dụng bắt đầu cài đặt bộ ứng dụng gồm:
.NET: ứng dụng hỗ trợ trong việc đọc thông tin thiết bị ngoại vi trên máy trạm
Antivirus: ứng dụng hỗ trợ trong việc quét Virus các tài liệu nhiễm mã độc
DLP: ứng dụng hỗ trợ trong việc theo dõi và quản lý thất thoát dữ liệu, tránh các thông tin nhạy cảm bị rò rỉ ngoài tổ chức
RAR-EP: ứng dụng quản lý các thông tin, địa chỉ máy trạm; danh sách thiết bị ngoại vi, website truy cập; phần mềm đang cài đặt trên máy trạm
Danh sách ứng dụng trong bộ cài đặt có thể thay đổi tùy theo cấu hình cài đặt của Quản trị viên trên hệ thống Quản trị tập trung Admin CMS.
Bước 6: Tại bước cài đặt Antivirus, nhấn Start installation trên popup xác nhận cài đặt Kaspersky
Bước 7: Hệ thống bắt đầu cài đặt phần mềm Antivirus. Quá trình cài đặt có thể mất vài phút
Bước 8: Đã cài đặt xong phần mềm Antivirus. Nhấn OK để tiếp tục cài đặt DLP và RAR-EP
Bước 9: Sau khi cài đặt xong bộ ứng dụng, hệ thống sẽ tự mở ứng dụng RAR-EP
2.1.2. Cập nhật phiên bản mới nhất của phần mềm
Khi có cập nhật phiên bản mới, người dùng mở ứng dụng Rar-Installer Setup sẽ được tự động cập nhật
Bước 1: Mở ứng dụng Rar-Installer Setup
Bước 2: Ứng dụng bắt đầu cài đặt bộ ứng dụng có cập nhật mới
Bước 3: Sau khi cài đặt xong bộ ứng dụng, hệ thống sẽ tự mở ứng dụng RAR-EP
2.1.3. Cấu hình máy trạm tương thích với ứng dụng RAREP
Bỏ Self Defense BKAV
Windows 64-bit
2.2. Cách gỡ ứng dụng
Có thể xóa ứng dụng thông qua Control Panel hoặc Installed App trên máy tính
Cách 1: Xóa ứng dụng tại Control Panel
Bước 1: Tại cửa sổ Control Panel, chọn mục Uninstall a program
Bước 2: Gỡ cài đặt lần lượt ứng dụng bằng cách nhấn chuột phải tại từng ứng dụng và chọn Uninstall
Kaspersky Security Center Network Agent
RAR-EP
RAR-Installer
Riêng ứng dụng RAR Endpoint Security cho Windows, chọn nút Change
Khi xóa các ứng dụng RAR-EP, RAR-Installer, RAR Endpoint Security cho Windows, hệ thống sẽ yêu cầu người dùng nhập mật khẩu (mật khẩu này được cung cấp bởi Quản trị viên)
Cách 2: Xóa ứng dụng tại Installed apps
Bước 1: Mở cửa sổ Settings, chọn mục Apps

Bước 2: Chọn mục Installed apps, sau đó nhấn action … và chọn Uninstall tại từng ứng dụng:
Kaspersky Security Center Network Agent
RAR-EP
Rar-Installer
Riêng ứng dụng RAR Endpoint Security cho Windows, chọn Modify. Sau đó xác nhận
Gỡ bỏ ứng dụng
Khi xóa các ứng dụng RAR-EP, RAR-Installer, RAR Endpoint Security cho Windows, hệ thống sẽ yêu cầu người dùng nhập mật khẩu (mật khẩu này được cung cấp bởi Quản trị viên)
2.3. Cách lấy log khi ứng dụng xảy ra lỗi
Mục đích để người dùng biết cách truy cập thư mục lấy file log và cung cấp cho đội kỹ thuật hỗ trợ khi có xảy ra bất kỳ lỗi nào không tự khắc phục được trên ứng dụng
Truy cập thư mục C:\Users\<tên user>\AppData\Local\RAR-EP\Logs để lấy log trên ứng dụng
Tên file log được hiển thị theo format <yyyymmdd>.txt - Năm tháng ngày lưu lịch sử log
Nếu tại thư mục C:\Users\<tên user> không thấy thư mục App Data thì nhấn chọn … trên thanh header > chọn Options > chọn Show hidden files, folders, and drives > nhấn OK để lưu cấu hình
2.4.1. Xem danh sách các máy trạm cùng địa phương quản lý
Người dùng chọn Thiết bị ngoại vi > Tất cả các máy > Màn hình hiển thị danh sách các máy trạm có địa chỉ cùng Phường/Xã của máy cá nhân
Thông tin máy tính hiển thị gồm:
Địa chỉ MAC
Trạng thái Kết nối của máy:
máy đã được kết nối (CONNECTED)
máy đã bị chặn (BLOCKED) do có phần mềm trên máy không thỏa điều kiện whitelist hoặc tên máy vi phạm whitelist đã cấu hình trên hệ thống quản trị tập trung CMS hoặc chưa có địa chỉ chính thức của máy được duyệt
Ngày tạo
Tỉnh/Thành
Quận/Huyện
Phường/Xã
Địa chỉ chính thức của máy trạm
Trạng thái duyệt địa chỉ
Thao tác:
Chi tiết: hiển thị danh sách các thiết bị của máy
2.4.2. Xem thông tin chi tiết của máy trạm cá nhân
Màn hình hiển thị thông tin chi tiết của máy trạm cá nhân bao gồm:
Thông tin cấu hình, địa chỉ máy trạm
Danh sách phần mềm đang cài trên máy trạm
Danh sách thiết bị đang kết nối với máy trạm
Danh sách lịch sử website truy cập trên máy trạm
Thông tin máy cá nhân gồm:
Địa chỉ MAC
Tỉnh/Thành
Quận/Huyện
Phường/Xã
Địa chỉ chính thức của máy trạm
Địa chỉ đang chờ cập nhật của máy trạm
Trạng thái duyệt địa chỉ
Trạng thái Kết nối của máy:
máy đã được kết nối (CONNECTED)
máy đã bị chặn (BLOCKED) do có phần mềm trên máy không thỏa điều kiện whitelist hoặc tên máy vi phạm whitelist đã cấu hình trên hệ thống quản trị tập trung CMS hoặc chưa có địa chỉ chính thức của máy được duyệt
Danh sách phần mềm đang chạy trên máy
Danh sách thiết bị đang kết nối với máy
Danh sách lịch sử các website đã truy cập trên máy
Thông tin danh sách phần mềm đang cài đặt trên máy gồm:
Tên phần mềm
Phiên bản

Phân loại: Phần mềm ứng dụng hay phần mềm hệ thống
Trạng thái:
Đã duyệt: tức là phần mềm thỏa điều kiện whitelist đã cấu hình trên CMS
Từ chối: tức là phần mềm không thỏa điều kiện whitelist đã cấu hình trên CMS
Quét phần mềm: ứng dụng sẽ quét lại để cập nhật danh sách phần mềm mới nhất đang cài đặt trên máy trạm
Nếu máy trạm hiện tại chưa cài đặt các phần mềm bắt buộc thì sẽ cảnh báo yêu cầu cài đặt thêm phần mềm
Nếu máy trạm hiện tại đang cài dư các phần mềm bị cấm thì sẽ cảnh báo yêu cầu gỡ bỏ phần mềm
Thông tin danh sách thiết bị đang kết nối với máy hiển thị theo cấu trúc dữ liệu dạng cây tương tự như Device Manager trên máy:
Tên thiết bị
Phân loại thiết bị
Trạng thái xét duyệt
Trạng thái kết nối mong muốn
Thao tác:
Xem chi tiết: lịch sử ghi nhận thời gian cập nhật trạng thái xét duyệt của thiết bị. Thông tin gồm:
Thời gian ghi nhận
Tài khoản cập nhật
Cấp bậc quản lý của tài khoản
Trạng thái xét duyệt
Trạng thái kết nối mong muốn
Trạng thái thực tế
Lý do từ chối thiết bị: trong trường hợp trường thái xét duyệt là Từ chối
Người dùng có thể lọc danh sách lịch sử theo thời gian
Để xem thông tin chi tiết thiết bị và lịch sử cập nhật trạng thái thsiết bị nhấn chọn … → Xem chi tiết
2.4.3. Xem lịch sử các sự kiện của thiết bị trên máy trạm
Người dùng có thể theo dõi các sự kiện cắm/rút thiết bị trên máy trạm và lịch sử xét duyệt trạng thái của từng thiết bị
Thông tin gồm:
Thời gian ghi nhận
Tài khoản người dùng đang đăng nhập lúc cắm/rút thiết bị trên máy cá nhân và xét duyệt trạng thái trên Admin
Cấp bậc quản lý: người dùng quản lý cấp Trung Ương, Tỉnh/Thành, Quận/Huyện, Phường/Xã
Mã thiết bị (GUID)
Tên thiết bị
Trạng thái cắm/rút và xét duyệt thiết bị
Trạng thái kết nối mong muốn
Trạng thái thực tế
Lý do khi từ chối thiết bị
2.4.4. Quét virus trên máy trạm
Người dùng có thể quét để phát hiện và ngăn chặn kịp tời các thư mục, tập tin bị nhiễm mã độc đang tồn tại trên máy trạm
Để quét virus, nhấn chọn Quét mã độc > Trạng thái quét tại thanh menu bên trái ứng dụng
Sau đó nhấn chọn để bắt đầu quét virus
Ứng dụng sẽ ghi nhận lại quá trình quét virus như trên màn hình
Nhấn để ngừng quét
2.4.5. Xem báo cáo nhiễm mã độc
Sau khi quét mã độc, thông tin các thư mục, tập tin đang cài đặt trên máy tính bị nhiễm mã độc sẽ được ghi nhận báo cáo
Thông tin báo cáo gồm:
Thư mục được quét virus
Thời gian bắt đầu và kết thúc của tiến trình quét virus
Số lượng tệp tin đã quét được
Số lượng mã độc phát hiện
Xem chi tiết: tải về file báo cáo chi tiết các file bị nhiễm mã độc của tiến trình quét virus
2.4.6. Cập nhật địa chỉ máy
Khi người dùng có nhu cầu thay đổi địa chỉ máy đến địa phương quản lý khác có

thể truy cập tính năng Cập nhật địa chỉ máy
Để thay đổi địa chỉ máy, nhấn chọn Cài đặt > Thay đổi tại tab Địa chỉ của máy → Khai báo thông tin địa chỉ mới → Nhấn Lưu thay đổi
Sau khi thay đổi địa chỉ chưa cập nhật ngay lập tức, mà sẽ cần xét duyệt từ cán bộ cấp cao thì địa chỉ mới sẽ được cập nhật
2.5.1. Danh sách trạng thái Phần mềm

No	Trạng thái	Note
1	Từ chối (DENIED)	Là phần mềm vi phạm danh sách blacklist và bị cắm cài đặt trên máy trạm (thuộc rule Không bao gồm - EXCLUDE)
2	Đã duyệt (APPROVED)	Là phần mềm không vi phạm danh sách blacklist và cho phép cài đặt trên máy trạm (không thuộc rule Không bao gồm - EXCLUDE)

2.5.2. Danh sách trạng thái Máy tính

No	Trạng thái	Note
1	Đã kết nối (CONNECTED)	Nếu máy trạm thỏa mãn 3 điều kiện sau: Tên máy trạm không vi phạm danh sách blacklist Tất cả phần mềm đang cài trên máy đều được chấp nhận cho phép cài đặt và đã cài đặt đủ phần mềm yêu cầu bắt buộc Đã được duyệt địa chỉ chính thức của máy
2	Đã chặn (BLOCKED)	Nếu máy trạm vi phạm 1 trong 3 điều kiện sau: Tên máy trạm không vi phạm danh sách blacklist Có ít nhất 1 phần mềm đang cài trên máy bịtừ chối cài đặt hoặc thiếu phần mềm yêu cầu bắt buộc cài đặt Chưa được duyệt địa chỉ chính thức của máy

2.5.3. Danh sách trạng thái Thiết bị
Chỉ hiển thị khi máy trạm được kích hoạt quy tắc whitelist.
Nếu máy trạm không được kích hoạt quy tắc whitelist thì thiết bị sẽ tự động cho phép kết nối (Quản trị viên có thể chặn kết nối thiết bị thủ công trên hệ thống quản trị tập trung CMS)

No	Trạng thái	Note
1	Từ chối (DENIED)	Thiết bị bị từ chốicó 2 trường hợp: Bị từ chối tự động là thiết bị vi phạm danh sách blacklist và bị cắm kết nối đến máy (Thuộc rule Không bao gồm - EXCLUDE) Bị từ chối thủ công theo xét duyệt của các cán bộ quản lý cấp cao
2	Đã duyệt (APPROVED)	Thiết bị được duyệt có 2 trường hợp: Được duyệt tự động là thiết bị thuộc whitelist và không vi phạm danh sách blacklist (thuộc rule Bao gồm - INCLUDE và không thuộc rule Không bao gồm - EXCLUDE) Được duyệt thủ công theo xét duyệt của các cán bộ quản lý cấp cao
3	Chờ duyệt cấp Phường/Xã (WAITING)	Là thiết bị không thuộc whitelist và cũng không vi phạm blacklist. Nên sẽ chờ xét duyệt thủ công theo các cán bộ quản lý cấp cao

4
Chờ duyệt cấp Quận/Huyện
(REQUEST TO DISTRICT)
Trạng thái xét duyệt thủ công khi cán bộ cấp Phường/Xã gửi xét duyệt thiết bị lên Quận/Huyện
5
Chờ duyệt cấp Tỉnh/Thành
(REQUEST TO PROVINCE)
Trạng thái xét duyệt thủ công khi cán bộ cấp Quận/Huyện gửi xét duyệt thiết bị lên Tỉnh/Thành
6
Chờ duyệt cấp Khu vực (REQUEST TO REGION)
Trạng thái xét duyệt thủ công khi cán bộ cấp Tỉnh/Thành gửi xét duyệt thiết bị lên Trung ương khu vực
2.5.4. Danh sách trạng thái Duyệt địa chỉ máy
No
Trạng thái
Note
1
Chờ duyệt
Khi máy vừa khởi tạo hoặc có thay đổi thông tin địa chỉ trên máy trạm thì sẽ cần cán bộ quản lý cấp cao xét duyệt địa chỉ
2
Đã duyệt
Khi cán bộ quản lý cấp cao đồng ý xét duyệt địa chỉ chính thức của máy trạm
3
Chưa duyệt
Khi cán bộ quản lý cấp cao cập nhật trạng thái xét duyệt địa chỉ chính thức của máy trạm do có nghi ngờ thông tin địa chỉ chính thức chưa hợp lệ