iSecurity Antivirus for AIX

User Guide
Version 1.0.1

www.razlee.com

Contents

Contents 2
About this AIX Manual 3
Starting to work with iSecurity Antivirus for AIX 8
Pre-Requisites 8
Installing 9
Uninstalling 9
Configuring 10
Refreshing Antivirus Signatures 10
Activating On-access 11
Testing On-Access 11
Deactivating On-access 12
Testing On-Demand 12
On-Demand Scanning 13
The Functionality of ”onlyNew” 13
Why You Need "onlyNew" 14
Deploying Web Interface 14

About this AIX Manual

This user guide is intended for system administrators and security administrators responsible for the implementation and management of security on AIX systems. However, any user with basic knowledge of AIX operations will be able to make full use of this product after reading this book.

Raz-Lee takes customer satisfaction seriously. Our products are designed for ease of use by personnel at all skill levels, especially those with minimal AIX experience. The documentation package includes a variety of materials to get you familiar with this software quickly and effectively.

This user guide is the only printed documentation necessary for understanding this product. It is available in HTML form as well as in user-friendly PDF format, which may be displayed or printed using Adobe Acrobat Reader version 6.0 or higher. If you do not have Acrobat Reader, you can download it from the Adobe website: http://www.adobe.com/. You can also read and print pages from the manual using any modern web browser.

This manual contains concise explanations of the various product features as well as step-by-step instructions for using and configuring the product.

Raz-Lee's iSecurity is an integrated, state-of-the-art security solution, providing cutting-edge tools for managing all aspects of network access, data, and audit security. Its individual components work together transparently, providing comprehensive "out-of-the- box" security. To learn more about the iSecurity Suite, visit our website at http://www.razlee.com/.

Intended Audience

The Antivirus for AIX User Guide document was developed for users, system administrators and security administrators responsible for the implementation and management of security on AIX systems. However, any user with a basic knowledge of AIX operations is able to make full use of this document following study of this User Guide.

NOTE: Deviations from IBM® standards are employed in certain circumstances in order to enhance clarity or when standard IBM® terminology conflicts with generally accepted industry conventions.

This document may also serve for new versions' upgrade approval by management.

Conventions Used in the Document

Menu options, field names, and function key names are written in **Courier New Bold**.

Links (internal or external) are emphasized with underline and blue color as follows: "About this AIX Manual" on page 3.

Commands and system messages are written in *Bold Italic*.

Key combinations are in Bold and separated by a dash, for example: **Enter**, **Shift-Tab**.

Emphasis is written in **Bold.**

Legal Notice

This document is provided by Raz-Lee Security for information purposes only and is not a legal binding document.

While Raz-Lee is doing its best to coordinate between this document and Raz-Lee's products, changes might occur. In case a change has been encountered, please inform Raz-Lee. Raz-Lee keeps its right to modify the software or the document as per its sole discretion Usage of this document, and all information (including product information) provided within, are subject to the following terms and conditions, and all applicable laws. If you do not agree with these terms, please do not access or use the remainder of this document.

This document contains highly confidential information, which is proprietary to Raz-Lee Security Ltd. and/or its affiliates (hereafter, "Raz-Lee"). No part of this document's contents may be used, copied, disclosed or conveyed to any third party in any manner whatsoever without prior written permission from Raz-Lee. The information included in this document is intended for your knowledge and for negotiation purposes only. Raz-Lee makes no implicit representations or warranties with respect to such information. The information included in this document is subject to change without notice. Any decision to rely on the information contained herein shall be at your sole responsibility, and Raz-Lee will not accept any liability for your decision to use any information or for any damages resulting therefrom. Certain laws do not allow limitations on implied warranties or the exclusion or limitation of certain damages. If these laws apply to you, some or all of the above disclaimers, exclusions, or limitations may not apply to you.

All registered or unregistered trademarks, product names, logos and other service marks mentioned within this document are the property of Raz-Lee or their respective owners. Nothing contained herein shall be construed as conferring by implication, estoppels, or otherwise any license or right, either express or implied, under any patent or trademark of Raz-Lee or any third party. No use of any trademark may be made without the prior written authorization of Raz-Lee. This document and all of its contents are protected intellectual property of Raz-Lee. Any copying, reprinting, reuse, reproduction, adaptation, distribution or translation without the prior written permission of Raz-Lee is prohibited.

Please check your End User License Agreement (EULA) for terms and Conditions.

Contacts

Raz-Lee Security Inc. www.razlee.com

Marketing: marketing@razlee.com 1-888-RAZLEE-4 (1-888-7295334)

Support: support@razlee.com 1-888-RAZLEE-2 (1-888-7295332)

Starting to work with iSecurity Antivirus for AIX

Pre-Requisites

- Supported AIX platforms: IBM AIX 7.2 TL5 SP7 or later, IBM AIX 7.3 or later.
  To ensure compatibility with the supported platforms, you can verify your AIX version using the following command:

  `oslevel -s`

  This command returns a four-part string, e.g. 7200-05-07-2346, where:

  7200 - AIX Version 7.2

  05 - Technology Level 5 (TL5)

  07 - Service Pack 7 (SP7)

  2346 - Built in week 46 of 2023.

  To format the output into a simpler form, use:

  oslevel -s | awk -F- '{printf "AIX %.1f TL%d SP%d\n",$1/1000,$2,$3}'

  Output: AIX 7.2 TL5 SP7
- Disk space: **`/home`** should have 2.5 GB free.
  - During installation: Additional 1.5 GB free is needed (in the download directory).
  - During upgrading: Additional 500 MB is needed.
- Minimum RAM: 1.7 GB.
- Signatures download:
  - From iSecurity server: Firewall should allow input from **`av.razlee.com`** (currently **`74.208.236.138`**).
    - The IP address might be changed in the future.
  - Via SSL, SSL Certificates for Antivirus signatures download:
    - For the first time: install the **`ca-certificates`** package by **`dnf`** or **`yum`**:
      - **`yum install ca-certificates`**
      - **`dnf install ca-certificates`**

- Web interface:
  - Java runtime version 8, or higher.
  - Web application server that supports Jakarta EE: Tomcat 10, WebSphere Application Server Liberty, etc.

Installing

On the AIX command line enter:

1. Log in as root.
2. **cd <download directory>**
3. To download the installer:
   via **wget**:
   wget --output-file=wget.log --timestamping --show-progress
   https://as400.razlee.com/products/AIX/AV/AV-V1.0.1-installer.bin.bz2
   via **PC web browser** download to the PC:
   https://as400.razlee.com/products/AIX/AV/AV-V1.0.1-installer.bin.bz2
   copy file **AV-V1.0.1-installer.bin.bz2** to the **<download directory>**
4. **cd <download directory>**
5. **/opt/freeware/bin/bzip2 -tdvv AV-V1.0.1-installer.bin.bz2**
6. **chmod 700 AV-V1.0.1-installer.bin**
7. **./AV-V1.0.1-installer.bin**

Running **installer.bin** installs Antivirus in the **/home/SMZVDTA** directory.

NOTE: Antivirus installation and configuration add special mounts (**namefs** mount) directories to the file system. The directories are under the **/SMZV** directory. These mount commands run online and also added to **/etc/inittab**, to keep the mounts during reboot. Uninstalling Antivirus removes the mounts from both online and the **/etc/inittab** file.

Uninstalling

On the AIX command line enter:

1. **/avmenu**
   The Antivirus main menu appears.

2. Select **6. Remove AV from computer (uninstall AV)** from the Configuration menu.

Uninstalling removes **namefs** directories and statements in **/etc/inittab** that were added during installation and configuration of Antivirus.

Configuring

On the AIX command line enter:

1. **/avmenu**
   The Antivirus main menu appears.
2. Select **1. Configuration**
   The Configuration menu appears.
3. To define how to send the email notifications:
   a. Select **1. AV Configuration**
      An editor opens **av.conf**
   b. Set values for the parameter **emailTo** (administrators that will receive the notifications) and the SMTP definitions: **emailSMTP**, **emailPort**, and **emailUser**
   c. Save and exit the editor.
   d. Select **2. Enter password of Antivirus email user**
      Enter the password of the Antivirus email user defined in SMTP definitions.
   e. Select **5. Test email setting**
      Check that the administrators, defined in the **emailTo** parameter, receive the test email.
4. To define the directories to be scanned On-Access, select **1. AV Configuration** from the Configuration menu. Set at least one **includePrefix** value.
   For example, if you set **includePrefix /home/e**, Antivirus On-Access will scan paths with the prefix **/home/e**

NOTE: Do not touch the **includePrefix /tmp/eicar.com** statement, it is used to test Antivirus.

Refreshing Antivirus Signatures

On the AIX command line enter:

1. **/avmenu**
   The Antivirus main menu appears.
2. Select **4. Refresh signatures**
   The Refresh signatures menu appears.
3. Select:
   - If the AIX has access to the Internet:
     - Use option **1. Refresh signatures from iSecurity site**
   - Else (if the AIX does not have access to the Internet):
     - Either
       - Use the option **3. Refresh signatures from Lan, AV config <lanUrl>**
     - or
       - Use the options **4. Refresh signatures from Dir, AV config <RefreshDir>**
     - For details please contact Razlee iSecurity Support at **support@razlee.com**
4. Select **5. Display current signatures** to check that the signature files **bytecode.cvd**, **daily.cvd** and **main.cvd** have been downloaded and updated.

Activating On-access

On the AIX command line enter:

1. **/avmenu**
   The Antivirus main menu appears.
2. Select **2. On-access activation**
3. Select **1. Start AV on-access**
   It may take a few minutes to load the signatures.
4. Select **3. AV on access Status**
   Repeat until it shows **Status Active**

Testing On-Access

NOTE: The EICAR Anti-Virus Test File or EICAR.com test file is a computer file that was developed by the European Institute for Computer Antivirus Research (EICAR) and Computer Antivirus Research Organization (CARO) to test the response of computer antivirus programs. Instead

of using real malware, which could cause real damage, this test file allows people to test anti-virus software without having to use a real computer virus.

For a general test, on the AIX command line enter:

1. **`/avmenu`**
   The Antivirus main menu appears.
2. Select **`4. Test AV on access`**
   You should receive an email about finding a test virus.

To test that On-Access works on another directory:

1. **`/avmenu`**
   The Antivirus main menu appears.
2. Select **`1. Configuration`**
   The Configuration menu appears.
3. Select **`4. Create virus file for test`**
   A demo virus is created as **`/SMZV/home/SMZVDTA/virus-for-test/eicar.com`**
4. Use a bash command line to copy it to a directory that was specified as **`includePrefix`** on the configuration file.
5. Touch the file by: **`cat target_directory/eicar.com`**.
6. The bash response should be **`: cat: 0652-050 Cannot open...`**
   You should receive an email about finding a test virus.

If the On-Access test fails, see "Configuring" on page 10 and repeat the steps specified there regarding the setup of **`includePrefix`** and email.

Deactivating On-access

On the AIX command line enter:

1. **`/avmenu`**
   The Antivirus main menu appears.
2. Select **`2. End AV on-access`**

Testing On-Demand

To test the On-Demand, on the AIX command line enter:

1. **`/avmenu`**
   The Antivirus main menu appears.

2. Select **2. End AV on-access**
3. Select **1. Configuration**
   The Configuration menu appears.
4. Select **4. Create virus file for test**
   A demo virus is created as **/home/SMZVDTA/virus-for-test/eicar.com**
5. Copy the **eicar.com** file from **/SMZVDTA** to the target directory that you want to scan.
6. **/scanav target_directory**
   The administrators should receive an email that summarizes the scanning.

On-Demand Scanning

Check the parameters of **scanav** with the **/scanav --help** command.
Use **/scanav target_directory** with your selected parameters
The administrators should receive an email that summarizes the scanning.

The Functionality of "onlyNew"

onlyNew is an important advantage of iSecurity Antivirus. When it is set, files that have been scanned will not be scanned again until they have changed.

NOTE: To use the **onlyNew** function, the file system **EAformat** has to be **v2**.

Changing the **EAformat** of the file system to **v2** is permanent. This change cannot be revoked.

The **onlyNew** attribute for a file or directory is kept:

- When you move a the file or directory.
- When you use "**tar -cU**" or "**tar -xU**"

For On-Access, set the **onlyNew** to be **Y** in the configuration file. On-Access will only scan files that have been modified since their last scan.

For On-Demand, when you run **/scanav**, add the **--only-new** flag.

Why You Need "onlyNew"

onlyNew is identical in On-Demand and On-Access detections and provides significant CPU savings. If one wishes to send the same file to 1,000 clients, iSecurity Antivirus for AIX will scan it just once, not 1,000 times.

The **onlyNew** parameter enables:

- **ReScanRlsUpg(N)** : if **onlyNew**=**Y**, Rescan file after AV Release Upgrade. A major product upgrade may bring new methods for virus detection. Setting to **Y** will force rescan.
- **ReScanImportFile (N)**: if **onlyNew**=**Y**, Rescan file that was imported from another AIX. The system hangs up during the installation of new products or releases as the AV has to check all the imported files. The **onlyNew** parameter enables not scanning files that were scanned on a different system in the organization. The transfer has to be done using "**tar -cU**" or "**tar -xU**".

A new feature was also implemented to bolster security and prevent hackers from bypassing the **onlyNew** feature by altering the file's last change date. Any such attempt triggers a rescan, ensuring the integrity of the system. Attaching the file stamp to a different file will also cause a rescan.

Deploying Web Interface

Download the web archive from:

https://as400.razlee.com/products/AIX/AV/WebApp/av.war

Edit the file: **tomcat_directory/conf/tomcat-users.xml**

Add these two lines:

```
<role rolename="razlee-admin"/>
<user username="av" password="razlee"
roles="razlee-admin"/>
```

NOTE: the user name **av** and password **razlee** are an example. Change them to appropriate values.

The **tomcat-users** section of the file should look like this:

```
<tomcat-users xmlns="http://tomcat.apache.org/xml"
              xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
              xsi:schemaLocation="http://tomcat.apache.org/xml tomcat-users.xsd"
              version="1.0">

  <role rolename="razlee-admin"/>
  <user username="av" password="razlee" roles="razlee-admin"/>

</tomcat-users>
```

Copy the **`av.war`** file to the **`tomcat_directory/webapps`** directory

Open **`http://AIX-IP-ADDRESS:8080/av/menu.html`** in your browser.

When prompted enter '**`av`**' as username and '**`razlee`**' as password or the values with which you have replaced them: