DISA Logo

ACAS HBSS Integration Guide

July 12, 2016

v5

Table of Contents

[Change Log 3](#_Toc456605851)

[Introduction 4](#_Toc456605852)

[Standards and Conventions 4](#_Toc456605853)

[Test Environment 4](#_Toc456605854)

[Red Hat Enterprise Linux 5 32-bit Library Dependencies 5](#_Toc456605855)

[Configuring ACAS Linux Server Settings (SecurityCenter, Nessus, PVS) 5](#_Toc456605856)

[Linux Server Settings for VirusScan Enterprise for Linux 1.9.x/2.0.x 5](#_Toc456605857)

[Linux Server Settings for Linux Firewall 6](#_Toc456605858)

[Linux Server Settings for HIPS General 6](#_Toc456605859)

[Configuring ACAS Windows Server Settings (Nessus, PVS) 7](#_Toc456605860)

[Windows Server Settings for VirusScan Enterprise 8.8.0 7](#_Toc456605861)

[Windows Server Settings for VSE Access Protection 8](#_Toc456605862)

[Windows Server Settings for HIPS General 8](#_Toc456605863)

[Windows Server Settings for HIPS Firewall 9](#_Toc456605864)

[Windows Server Settings for HIPS Firewall – Nessus Guidance 9](#_Toc456605865)

[Windows Server Settings for HIPS Firewall – PVS Guidance 10](#_Toc456605866)

[Target Settings for Malicious Process Detection and Security Content Automation Protocol (SCAP) Checks 10](#_Toc456605867)

[Dissolvable Agents Settings for Supported Linux Target 10](#_Toc456605868)

[Dissolvable Agents Settings for VirusScan Enterprise for Linux 1.9.x/2.0.x 10](#_Toc456605869)

[Dissolvable Agents Settings for HIPS General 11](#_Toc456605870)

[Dissolvable Agents Settings for Windows Target 12](#_Toc456605871)

[Dissolvable Agents Settings for VirusScan Enterprise 8.8.0 12](#_Toc456605872)

[Dissolvable Agents Settings for HIPS General 12](#_Toc456605873)

[References 14](#_Toc456605874)

[Useful Links 15](#_Toc456605875)

# Change Log

|  |  |  |
| --- | --- | --- |
| Date | Version | Changes |
| 12-July-2016 | 5 | * Formatting changes * Updated for latest HBSS Baseline * Added McAfee STIG references. * Added SC5 pathing to existing policy guidance * Updated wildcard format for exceptions * Added Test Environment section   + Added supported ACAS operating systems |
| 5-Aug-2014 | 4 | * Added guidance for Linux HIPS   + *HIPS General: Trusted Applications* for SecurityCenter, Nessus, and PVS * Added information for tested baseline(s) and versions * Added PVS 4.0.x port references * Added PVS “ProgramData” directory to Windows VSE exclusions |
| N/A | 3 | * Internal document update; not released to the field |
| 2-May-2014 | 2 | * Updated Windows SCAP & Malicious Process Detection executable paths |
| 19-Dec-2013 | 1 | * Initial document creation; incorporated existing content from *Settings\_for\_ACAS\_and\_HBSS* document |

Table 1

# Introduction

It is necessary to create exceptions in enterprise security software to ensure the Assured Compliance Assessment Solution (ACAS) components function properly and for vulnerabilities on target hosts to be properly enumerated. Without these exceptions the product may not work at all or the results may be incorrect. This document will illustrate these required exceptions for each supported ACAS component operating system.

## Standards and Conventions

Throughout the documentation, filenames, daemons, and executables are indicated with a **courier bold** font such as **gunzip**, **httpd**, and **/etc/passwd**.

Command line options and keywords are also indicated with the **courier bold** font. Command line examples may or may not include the command line prompt and output text from the results of the command. Command line examples will display the command being run in **courier bold** to indicate what the user typed while the sample output generated by the system will be indicated in courier (not bold). Following is an example running of the Unix **pwd** command:

# **pwd**/opt/sc/daemons  
#

|  |  |
| --- | --- |
|  | Important notes and considerations are highlighted with this symbol and grey text boxes. |

|  |  |
| --- | --- |
|  | Tips, examples, and best practices are highlighted with this symbol and white on blue text. |

# Test Environment

This document was tested using Host Based Security System (HBSS) and focuses on configuring VirusScan Enterprise for Linux 1.9.x/2.0.x, VirusScan Enterprise 8.8, and Host Intrusion Prevention System (HIPS) 8.0. Other HBSS components should work; however, they are out of scope for this document. VSEL 2.0.2 supports RHEL 7.x. VSEL 1.9.x supports RHEL 5.x and 6.x.

It may be necessary to work with the HBSS server administrator to make these changes. There are a number of settings and file paths referenced in this document that assume that the ACAS components were installed to their default locations. It may be necessary to tailor these settings to your environment, particularly if there were custom install locations used.

ACAS supports the following operating systems for use with ACAS components:

* Red Hat Enterprise Linux 6 64-bit
* Red Hat Enterprise Linux 5 64-bit
* Windows 7 64-bit
* Windows 8 64-bit
* Windows Server 2008 / 2008 R2 64-bit
* Windows Server 2012 / 2012 R2 64-bit

# Red Hat Enterprise Linux 5 32-bit Library Dependencies

The current accredited McAfee Agent (CMA) and VirusScan Enterprise (VSE) applications for Linux are 32-bit. The ACAS (RHEL) Kickstart is a 64-bit operating system, and therefore, requires several 32-bit library files to be installed before attempting a CMA or VSE installation. Note that each 32-bit library must match the version of its installed 64-bit counterpart. For example, the installed 64-bit library audit-libs-1.8-2.el5.x86\_64 requires audit-libs-1.8-2.el5.i386 for 32-bit compatibility; the versions must match. The table below lists the RPM file names required for HBSS components:

|  |  |
| --- | --- |
| 32-bit Versions of Required Libraries for Linux HBSS Components | |
| audit-libs | libselinux |
| audit-libs-python | libselinux-python |
| cracklib | libselinux-utils |
| cracklib-dicts | libsepol |
| glibc | PAM |

Table 2

The Red Hat Package Manager (RPM) can be used to query the installed 64-bit version of these libraries to determine its 32-bit counterpart. Login to the Linux host, for each RPM file use the following RPM command to view the version:

# **rpm –qa audit-libs**  
audit-libs-1.8-2.el5

In this example, the 64-bit version of audit-libs is 1.8-2, and therefore, the 32-bit version required is 1.8-2. Red Hat Package Manager can be used to install the 32-bit RPM with the following command as a privileged account:

# **rpm –ivh audit-libs-1.8-2-es5.x86.rpm**

Later versions of the RHEL 5 Kickstart and all versions of the RHEL 6 Kickstart do not require the addition of 32-bit libraries. These libraries are included with these distributions to accommodate HBSS component installation.

# Configuring ACAS Linux Server Settings (SecurityCenter, Nessus, PVS)

VirusScan Enterprise for Linux should be configured for any ACAS components using a Linux operating system. It is necessary to create a number of exceptions in various subdirectories on the system, depending on which products are installed. Ensure that policy changes are performed to both On-access scans, as well as, any Client Tasks performing full file system scans.

## Linux Server Settings for VirusScan Enterprise for Linux 1.9.x/2.0.x

Login to the HBSS ePolicy Orchestrator (ePO) server and select *Menu* | *Policy* | *Policy Catalog*. In the *Product* drop-down box, select *VirusScan Enterprise for Linux 1.9.x/2.0.x*. In the *Category* drop-down box, select *On-Access Scanning Policy*. Select the policy applied to the machine. Select the *Detection* tab, and in the *What not to scan* field, add the following directories:

Directories to be excluded (*also exclude all subdirectories*):

|  |  |  |
| --- | --- | --- |
| Product | Directory Path | Exclude all subdirectories |
| Nessus | /opt/nessus | Y |
| SecurityCenter 4.x | /opt/sc4 | Y |
| SecurityCenter 5.x | /opt/sc | Y |
| Passive Vulnerability Scanner | /opt/pvs | Y |

Table 3

Add these same excluded directories and subdirectories to any On-Demand scans configured to scan the Linux system. Client Task would need to be modified in order to exclude the directories. Once logged on to the ePO server, select *Menu* | *Policy* | *Client Task Catalog*. Under *Client Task Types*, select *VirusScan Enterprise for Linux 1.9.x/2.0.x,* then select *On Demand Scan*. Select the on demand scan applied to the machine. Select the *Detections* tab, and in the *What not to scan* field, add the same directories listed in Table 3.

|  |  |
| --- | --- |
|  | McAfee VSEL 1.9/2.0 Managed Client STIG (V-63049). Rule Title: The McAfee VirusScan Enterprise for Linux 1.9.x/2.0.x On-Demand scanner must only be configured with exclusions which are documented and approved by the ISSO/ISSM/AO. |

## Linux Server Settings for Linux Firewall

The ACAS Linux Kickstart image has iptables enabled by default with firewall rules configured according to the Red Hat Linux Security Technical Implementation Guide (STIG). The policies can be further restricted, but the existing settings should be sufficient for the majority of implementations. Ensure the local / host firewall does not block or modify traffic on the Passive Vulnerability Scanner (PVS) monitoring interface.

## Linux Server Settings for HIPS General

The following applications must be listed under trusted applications (Go to the “HIPs 8.0:General” policy and select “Trusted applications”category, modify the proper policies that are assigned to the applicable Linux-based ACAS host. Note that you may need to modify the paths of the programs if they were not installed in the default locations):

|  |  |
| --- | --- |
| Product | Product Executable |
| Nessus | /opt/nessus/sbin/nessusd |
| Nessus | /opt/nessus/sbin/nessus-service |
| SecurityCenter 4.x | /opt/sc4/support/bin/httpd |
| SecurityCenter 4.x | /opt/sc4/support/bin/php |
| SecurityCenter 5.x | /opt/sc/support/bin/httpd |
| SecurityCenter 5.x | /opt/sc/support/bin/php |
| PVS | /opt/pvs/bin/pvs |
| PVS | /opt/pvs/bin/pvs-proxy |

Table 4

**For each trusted binary, check the option “Mark trusted for IPS (All Platforms)” and “Mark trusted for Firewall (Windows)”.**

# Configuring ACAS Windows Server Settings (Nessus, PVS)

Windows systems will use both VSE and HIPS. Several exceptions must be made in order for these products to not affect vulnerability scans. Ensure that policy changes are performed on both On-Access scans, as well as, any Client Tasks performing on demand file system scans.

## Windows Server Settings for VirusScan Enterprise 8.8.0

Configure VirusScan Enterprise to exclude Nessus and PVS directories. While logged on to the ePO server, select *Menu* | *Policy* | *Policy Catalog*. In the *Product* drop-down box, select *VirusScan Enterprise 8.8.x*. In the *Category* drop-down box, select *On-Access Default Processes Policies*. Select the policy applied to the machine. Select the *Exclusions* tab, and in the *What not to scan* field, add the following directories:

Directories to be excluded on read/write access (*also exclude all subdirectories*):

|  |  |  |
| --- | --- | --- |
| Product | Directory Path | Exclude all subdirectories |
| Nessus | C:\Program Files\Tenable\Nessus\ C:\Program Files (x86)\Tenable\Nessus\ (*if using 32-bit version of Nessus*)  C:\ProgramData\Tenable\Nessus\ | Y |
| Passive Vulnerability Scanner | C:\Program Files\Tenable\PVS\  C:\Program Files (x86)\Tenable\PVS\ (*if using 32-bit version of PVS*) C:\ProgramData\Tenable\PVS\ | Y |

Table 5

**Do this for both the Workstation and the Server (under the “*Settings for:*” option at the top) if both Windows client and server (i.e. Windows 7 and Windows 2008 R2) will be used.**

Add these same excluded directories and subdirectories to any On-Demand scans configured to scan the Windows system. Client Task would need to be modified in order to exclude the directories. While logged on the ePO server, select *Menu | Policy | Client Task Catalog*. Under the *Client Task Types*, select *VirusScan Enterprise 8.8.x*, then select *On Demand Scan*. Select the on demand scan applied to the machine. Select the *Exclusions* tab, and in the *What not to scan* field, add the same directories listed in Table 5.

|  |  |
| --- | --- |
|  | McAfee VirusScan Enterprise STIG (V-6604). Rule Title: McAfee VirusScan On-Demand scan must be configured so there are no exclusions from the scan unless exclusions have been documented with, and approved by, the ISSO/ISSM. |

## 

## Windows Server Settings for VSE Access Protection

VSE Access Protection must be configured to allow Nessus to generate malicious outbound traffic for thorough scan results. There are two Access Protection Rules which require modification:

|  |  |
| --- | --- |
| Access Protection Rule | Trusted Process Name |
| Prevent mass mailing worms from sending mail | nessusd.exe |
| Prevent IRC communication | nessusd.exe |

Table 6

*Steps for creating exceptions in VSE Access Protection Policies:*

1. In the HBSS ePO server console, select *Menu* | *Policy* | *Policy Catalog*. In the *Product* drop-down box, select *VirusScan Enterprise 8.8.x*. In the *Category* drop-down box, select *Access Protection Policies*.
2. Select and edit the assigned access protection policy applied to the machine.
3. Select the appropriate target type of either “*Workstation*” or “*Server*”.
4. On the *Access Protection* tab, in the *Access protection rules* section, select the “Anti-virus Standard Protection” option under *Categories*. On the right, select “Prevent mass mailing worms from sending mail” under *Block/Report/Rules*, then click the “Edit” button.
5. Add or append “nessusd.exe” to the “Processes to exclude” input box. Select “*OK*”.
6. Select “Save”.
7. Repeat this process for the Access Protection Rule “Prevent IRC communication”.

**Do this for both the Workstation and the Server (under the “*Settings for:*” option at the top) if both Windows client and Server (i.e. Windows 7 and Windows 2008 R2) will be used.**

## Windows Server Settings for HIPS General

Add scanner IP address to Trusted Networks (Under Host Intrusion Prevention 8.0: General, Trusted Networks) – As with any network vulnerability scanner, the scanner IP address must be trusted by each of the systems it is scanning. **The scanner must trust its own IP address for IPS as well, otherwise results will be affected.**

The following applications must be listed under trusted applications (Go to the “HIPs 8.0: General” policy and select “Trusted applications”category, modify the proper policy that is assigned to only the scanners. Note that you may need to modify the paths of the programs if you didn’t install them to default locations):

|  |  |
| --- | --- |
| Product | Product Executable |
| Nessus | C:\Program Files\Tenable\Nessus\Nessusd.exe |
| Nessus | C:\Program Files\Tenable\Nessus\Nessus-service.exe |
| PVS | C:\Program Files\Tenable\pvs\pvs.exe |
| PVS | C:\Program Files\Tenable\pvs\pvs-proxy.exe |
| PVS | C:\Program Files\Tenable\pvs\pvs-proxy-service.exe |

Table 7

**For each trusted binary, check the option “Mark trusted for IPS (All Platforms)” and “Mark trusted for Firewall (Windows)”.**

## Windows Server Settings for HIPS Firewall

Nessus scanners must allow all inbound and outbound traffic for all protocols only for the Nessus executable files. Adjust the Firewall Policy by creating a rule that only applies to the following executable files:

|  |  |
| --- | --- |
| Product | Product Executable |
| Nessus | C:\Program Files\Tenable\Nessus\Nessusd.exe |
| Nessus | C:\Program Files\Tenable\Nessus\Nessus-service.exe |

Table 8

*Steps for creating exception rules in the Firewall Policy:*

1. In the HBSS ePO server console, select *Menu* | *Policy* | *Policy Catalog*. In the *Product* drop-down box, select *Host Intrusion Prevention 8.x:Firewall*. In the *Category* drop-down box, select *Firewall Rules (Windows, Mac, Linux)*.
2. Create or copy an existing policy and go to “*edit”*.
3. Select *“*New Rule”*.*
4. Give the rule a name, select “*Allow*” in the *Action* section, select “*Either*” in the *Direction* section, and select “*Enabled*” in the *Status* section. Select the “*Next*” button.
5. For Network Options, select “Any Protocol” in the Network protocol section. Select the “Next” button. For Transport Options, select “All Protocols” from the drop-down box in the Transport protocol section*.* Select the “*Next*” button.
6. For Applications, select “New”. Give it a name and select “*New*” in the *Executables* section.
7. Give the executable a name and add one of the full paths to the Nessus executable files above in the *File name* section. Select “Save”.
8. Repeat this process for the other Nessus executable.

**Ensure the new firewall rules are above the “DENY ALL (Keep At Bottom!)” Block-all rule.**

A sample ACAS Firewall Policy is provided for an example, if used it will be necessary to modify it for the specific environment. The Firewall Policy is purposely very restrictive. It was created to only allow Nessus scanning.

## Windows Server Settings for HIPS Firewall – Nessus Guidance

It may be desired to limit access to the Nessus web-based console to a specific set of IP addresses, such as a Security Analyst’s workstation. This restriction can be done by adding a HIPS Firewall rule with the following conditions:

* Allow inbound tcp/8834 from the IP address of the SecurityCenter server and the Security Analyst workstation(s)
* Deny all inbound for tcp/8834

## Windows Server Settings for HIPS Firewall – PVS Guidance

PVS scanners should have the HIPS Firewall completely disabled for the interface(s) used for monitoring the network. Monitoring interfaces are placed into promiscuous mode by the PVS application. These interfaces should be allowed to accept all traffic for proper evaluation. To further increase security, access to the PVS proxy can be restricted by adding a HIPS Firewall rule with the following conditions:

If using PVS 4.x:

* Allow inbound tcp/8835 from the IP address of the SecurityCenter server
* Deny all inbound for tcp/8835

Or, if using PVS 3.8.1:

* Allow inbound tcp/1234 from the IP address of the SecurityCenter server
* Deny all inbound for tcp/1234

# Target Settings for Malicious Process Detection and Security Content Automation Protocol (SCAP) Checks

Nessus Plugins 59275 “Malicious Process Detection”, 66756 “SCAP Windows Compliance Checks”, and 66757 “SCAP Linux Compliance Checks” use “Dissolvable” Agents deployed to the target for enhanced evaluation. These agents are deployed via a single executable file (.exe) or executable binary for Linux. When executed, several additional files are created and used during the evaluation process. Once the evaluation process is completed, all agent-related files are removed.

For Windows hosts, all Tenable Dissolvable Agent binaries (Malicious Process Detection and checks generated by SCAP) are deployed to, and executed from, “%SystemRoot%”. Other Malicious Process Detection and SCAP supporting files are deployed to “%SystemRoot%\temp”. For Linux hosts, all Tenable Dissolvable Agents (SCAP checks only) are deployed to, and executed from, a temporary directory within the home directory of the credential defined in the Scan. For example, if the "root" account was selected as the credential of the Scan the SCAP Dissolvable Agent files would be in "/root/.tmp-nessus/". This example assumes “/root” is the home directory of the target “root” account. SCAP Dissolvable Agent evaluation is currently supported on RHEL 5.x, CentOS 5.x, Scientific Linux 5.x, and Oracle Linux 5.x hosts.

# Dissolvable Agents Settings for Supported Linux Target

It is expected that target Linux systems will use both VirusScan Enterprise for Linux (VSEL) and HIPS. It is necessary to create several exceptions for SCAP evaluation functionality. **Add a Dissolvable Agent exception for each Linux credential used by Nessus to authenticate to a target.** Ensure that policy changes are performed on both On-access scans, as well as, any Client Tasks performing on demand file system scans.

## Dissolvable Agents Settings for VirusScan Enterprise for Linux 1.9.x/2.0.x

Login to the HBSS ePolicy Orchestrator (ePO) server and select *Menu* | *Policy* | *Policy Catalog*. In the *Product* drop-down box, select *VirusScan Enterprise for Linux 1.9.x/2.0.x*. In the *Category* drop-down box, select *On-Access Scanning Policy*. Select the policy applied to the machine. Select the *Detections* tab, and in the *What not to scan* field, add the following files listed in Table 9. Wildcard characters are required where GUID or random alpha-numeric strings are generated for dissolvable agent files.

Files to be excluded (*do not exclude all subdirectories*):

|  |  |
| --- | --- |
| File | Function |
| /home/acasuser/.tmp-nessus/tenable\_ovaldi\_.\* (extensions may vary) | SCAP / Ovaldi Dissolvable Agent executable file |
| /home/acasuser/.tmp-nessus/tenable\_oval\_def\_.\*.xml | Agent support file |
| /home/acasuser/.tmp-nessus/tenable\_.\*.tmp | Agent support file |
| /home/acasuser/.tmp-nessus/tenable\_.\*.xml | Agent support file |
| /home/acasuser/.tmp-nessus/tenable\_sys\_char\_.\*.xml | Agent support file |
| /home/acasuser/.tmp-nessus/ovaldi.log | Ovaldi Agent log file |

Table 9

**Add a Dissolvable Agent exception for each Linux credential used by Nessus to authenticate to a target. Replace “/home/acasuser” with the home directory path of each account used for credentialed scans.**

Add these same excluded files to any On-Demand scans configured to scan the Linux system. Client Task would need to be modified in order to exclude the files. Once logged on to the ePO server, select *Menu* | *Policy* | *Client Task Catalog*. Under *Client Task Types*, select *VirusScan Enterprise for Linux 1.9.x/2.0.x,* then select *On Demand Scan*. Select the on demand scan applied to the machine. Select the *Detection* tab, and in the *What not to scan* field, add the same files listed in Table 9.

|  |  |
| --- | --- |
|  | McAfee VSEL 1.9/2.0 Managed Client STIG (V-63049). Rule Title: The McAfee VirusScan Enterprise for Linux 1.9.x/2.0.x On-Demand scanner must only be configured with exclusions which are documented and approved by the ISSO/ISSM/AO. |

## Dissolvable Agents Settings for HIPS General

The following applications must be listed under trusted applications (Go to the HIPs 8.0: General” policy and select “Trusted applications”category, modify the proper policies that are assigned to the applicable Linux-based ACAS hosts. Note that you may need to modify the paths of the programs if they were not installed in the default locations):

|  |  |
| --- | --- |
| File | Function |
| /home/acasuser/.tmp-nessus/tenable\_ovaldi\_.\* | SCAP / Ovaldi Dissolvable Agent executable file |

Table 10

**Add a Dissolvable Agent exception for each Linux credential used by Nessus to authenticate to a target. Replace “/home/acasuser” with the home directory path of each account used for credentialed scans. For each trusted binary check the option “Mark trust for IPS (All Platforms)”.**

# Dissolvable Agents Settings for Windows Target

It is expected that target Windows systems will use both VSE and HIPS. It is necessary to create several exceptions for Malicious Process Detection and SCAP evaluation functionality

## Dissolvable Agents Settings for VirusScan Enterprise 8.8.0

Configure VirusScan Enterprise to exclude Malicious Process Detection and SCAP evaluation files. While logged on to the ePO server, select *Menu* | *Policy* | *Policy Catalog*. In the *Product* drop-down box, select *VirusScan Enterprise 8.8.x*. In the *Category* drop-down box, select *On-Access Default Processes Policies*. Select the policy applied to the machine. Select the *Exclusions* tab, and in the *What not to scan* field, add the following files listed in Table 11. Wildcard characters are required where GUID or random alpha-numeric strings are generated for dissolvable agent files.

Files to be excluded on read/write access (*do not exclude all subdirectories*):

|  |  |
| --- | --- |
| File | Function |
| %SystemRoot%\tenable\_mw\_scan\_\*.exe | Malicious Process Detection Dissolvable Agent executable file |
| %SystemRoot%\temp\nessus\_\*.txt | Agent support file |
| %SystemRoot%\temp\nessus\_\*.bat | Agent clean-up script |
| %SystemRoot%\temp\NES\*.TMP | Agent support file |
| %SystemRoot%\tenable\_ovaldi\_\*.exe | SCAP/Ovaldi Dissolvable Agent executable file |
| %SystemRoot%\temp\tenable\_oval\_def\_\*.xml | Agent support file |
| %SystemRoot%\temp\tenable\_\*.tmp | Agent support file |
| %SystemRoot%\temp\tenable\_\*.xml | Agent support file |
| %SystemRoot%\temp\tenable\_sys\_char\_\*.xml | Agent support file |
| %SystemRoot%\temp\ovaldi.log | Ovaldi Agent log file |

Table 11

**Do this for both the Workstation and the Server (under the “*Settings for:*” option at the top) if both Windows client and server (i.e. Windows 7 and Windows 2008 R2) will be used.**

Add these same excluded files to any On-Demand scans configured to scan the Windows system. Client Task would need to be modified in order to exclude the files. While logged on the ePO server, select *Menu | Policy | Client Task Catalog*. Under the *Client Task Types*, select *VirusScan Enterprise 8.8.x*, then select *On Demand Scan*. Select the on demand scan applied to the machine. Select the *Exclusions* tab, and in the *What not to scan* field, add the same files listed in Table 11.

|  |  |
| --- | --- |
|  | McAfee VirusScan Enterprise STIG (V-6604). Rule Title: McAfee VirusScan On-Demand scan must be configured so there are no exclusions from the scan unless exclusions have been documented with, and approved by, the ISSO/ISSM. |

## Dissolvable Agents Settings for HIPS General

The following applications must be listed under trusted applications (Go to the “*HIPs 8.0:General”* policy and select “Trusted Applications”category, modify the proper policy that is assigned to only the scanners. Note that you may need to modify the paths of the programs if they were not installed in the default locations):

|  |  |
| --- | --- |
| File | Function |
| %SystemRoot%\tenable\_mw\_scan\_.\*.exe | Malicious Process Detection Dissolvable Agent executable file |
| %SystemRoot%\temp\nessus\_.\*.bat | Agent clean-up script |
| %SystemRoot%\tenable\_ovaldi\_.\*.exe | SCAP/Ovaldi Dissolvable Agent executable file |

Table 12

# References

How to use wildcards when creating exclusions in VirusScan Enterprise 8.x:

<http://kc.mcafee.com/corporate/index?page=content&id=KB54812>

# Useful Links

***ACAS Homepage***

<https://disa.deps.mil/ext/cop/mae/netops/acas/SitePages/Home.aspx>

Contains access to the following: ACAS License Request Portal, ACAS Build 1 Request Portal, ACAS Working Group information, ACAS Training, and other important ACAS related information.

***Approved documentation/binaries are located on DoD Patch Repository***

Posted at: <https://patches.csd.disa.mil/CollectionInfo.aspx?id=442>   
(CAC is required for access). Click on ACAS > ACAS Software > then whichever application you need. All of our latest Plugins files and Red Hat patches can be found here also.

***ACAS Customer Support/OKC Helpdesk***

* Toll-free: 844-347-2457 (Select options 1,5, and 4)
* DSN: 850-0032 (Select options 1,5, and 4)
* Email: [disa.tinker.esd.mbx.okc-disa-peo-service-desk@mail.mil](mailto:disa.tinker.esd.mbx.okc-disa-peo-service-desk@mail.mil)

***SoftwareForge***

<https://software.forge.mil/sf/projects/acas>   
All of our test and development efforts are located here and do not represent the approved baselines.   
  
***Certification and Accreditation Artifacts***

Posted at ACAS SIPR Wiki: <https://www.intelink.sgov.gov/wiki/ACAS>

***ACAS Front Door***

<http://www.disa.mil/Cybersecurity/Network-Defense/ACAS>

***ACAS TTP***

Posted at: <https://powhatan.iiie.disa.mil/ttp/capability/capability.html>