AnyConnect HostScan Migration 4.3.x to 4.6.x and Later

Revised: August 29, 2019

Migrate AnyConnect HostScan 4.3.x to 4.6.x and Later

Migrate AnyConnect HostScan 4.3.x to 4.6.x and Later

This migration process is necessary when upgrading HostScan from version 4.3.x or earlier to version 4.6.x or later. It is a one-time procedure, necessary because of internal library changes that occurred with release 4.6.x and later. Migration is supported in ASDM 7.9.2 and later ASDM releases. You cannot migrate if you are running earlier versions of ASDM.

Note If you have a HostScan version earlier than 4.3.05050, you must upgrade to 4.3.05050, or a later 4.3.x version, prior to starting this migration process.

Beginning with macOS Catalina release (10.15.x), the operating system will no longer support executing 32-bit binaries, which are included in HostScan package 4.3.x and earlier. End users who attempt to connect from macOS Catalina to ASA headends running HostScan package 4.3.x and earlier will not be able to successfully establish VPN connections. If a device running macOS Catalina release attempts to connect with ASA headends running HostScan package 4.3 and earlier, a posture assessment failed popup appears. Due to the above-mentioned Apple enforcement, all HostScan versions prior to 4.7.x **must** be migrated to HostScan 4.8.00175 or later .

This migration guides you through the transition of antivirus (AV), antispyware (AS), and firewall (FW) policies in 4.3.x and earlier, to the new antimalware (AM) and firewall (PFW) policies. The new policy format is needed for HostScan 4.6.x and later.

Before you begin

In HostScan 4.6.x and later, the procedure to check for ANY antimalware (endpoint.am) and/or ANY personal firewall (endpoint.pfw) is now accomplished with LUA scripts. Refer to the supporting LUA Procedures for HostScan 4.6 and Later, on page 14 section.

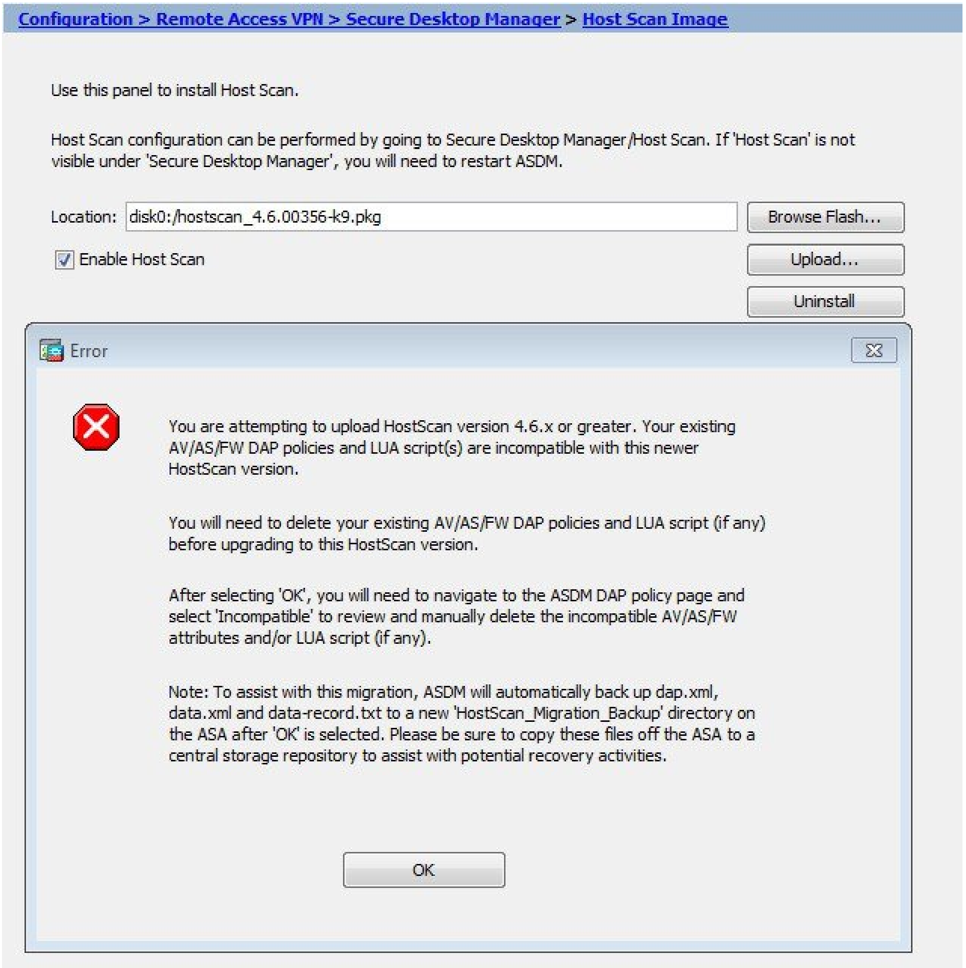
Procedure

Step 1 Initiate the HostScan Upgrade, making it part of the running configuration.

a) Choose **Configuration > Remote Access VPN > Secure Desktop Manager > Host Scan Image**.

b) Install and Enable HostScan on the ASA.

After choosing **Apply**, the error message below appears due to the fact that existing DAP entries or LUA scripts, created when using HostScan 4.3.x or earlier, are incompatible with HostScan 4.6.x or later.



Configuration > Remote Access VPN > Secure Desktop Manager > Host Scan Image

Use this panel to install Host Scan.

Host Scan configuration can be performed by going to Secure Desktop Manager/Host Scan. If 'Host Scan' is not visible under 'Secure Desktop Manager', you will need to restart ASDM.

Location: disk0:/hostscan_4.6.00356-k9.pkg

☑ Enable Host Scan

Browse Flash...
Upload...
Uninstall
Error

You are attempting to upload HostScan version 4.6.x or greater. Your existing AV/AS/FW DAP policies and LUA script(s) are incompatible with this newer HostScan version.

You will need to delete your existing AV/AS/FW DAP policies and LUA script (if any) before upgrading to this HostScan version.

After selecting 'OK', you will need to navigate to the ASDM DAP policy page and select 'Incompatible' to review and manually delete the incompatible AV/AS/FW attributes and/or LUA script (if any).

Note: To assist with this migration, ASDM will automatically back up dap.xml, data.xml and data-record.txt to a new 'HostScan_Migration_Backup' directory on the ASA after 'OK' is selected. Please be sure to copy these files off the ASA to a central storage repository to assist with potential recovery activities.

c) Select **OK**.

After acknowledging this message, the ASDM automatically backs up `dap.xml, data.xml`, and `data-record.txt` to a new `Hostscan_Migration_Backup` directory under `disk0` on the ASA.

Note The system will not allow migration if you rename or delete these backup files.

This backup is used later in this migration process to redefine these attributes in the proper format. We recommend copying these files to a safe repository for future reference if needed.

This backup action takes place the first time a HostScan 4.6.x or later installation is attempted. Once the backup is done and backup files are present, the system surmises that you do not need to do this again.

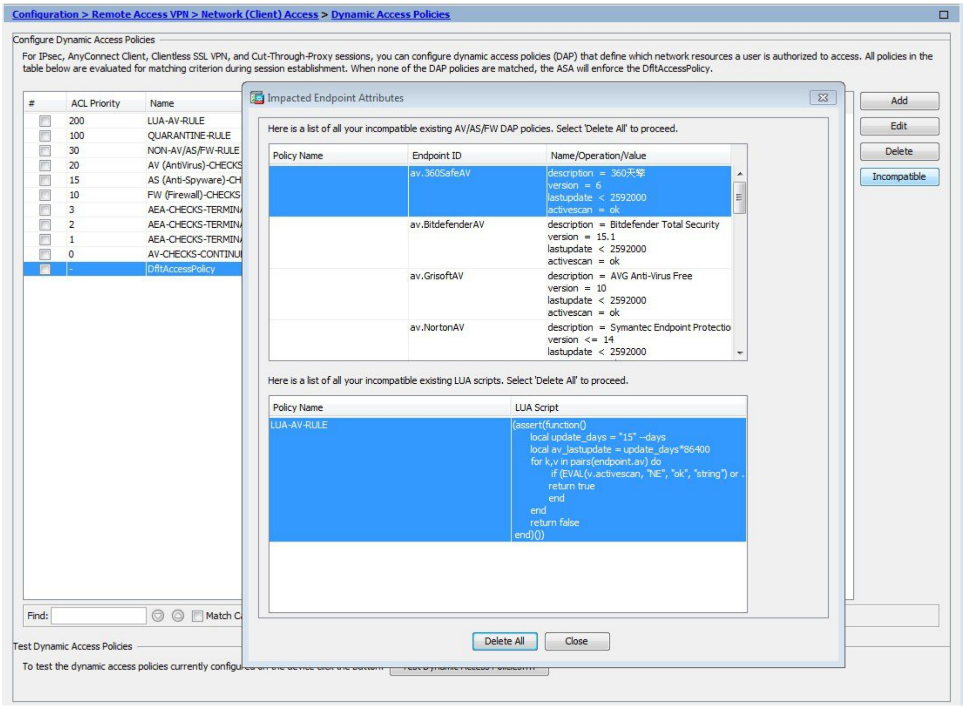
Step 2 Remove incompatible policies from the running configuration.

a) Go to **Configuration > Remote Access VPN > Network (Client) Access > Dynamic Access Policies**.

An **Incompatible** action appears after attempting the update of HostScan 4.6.x or later, and when the DAP records contain incompatible AV/AS/FW endpoint attributes and LUA scripts.

b) Click **Incompatible**.

The **Incompatible Endpoint Attributes** screen displays, populated with the incompatible AV/AS/FW Endpoint Attributes and LUA scripts from all DAP records.



Configuration > Remote Access VPN > Network (Client) Access > Dynamic Access Policies
Configure Dynamic Access Policies
Add
Edit
Delete
Incompatible
Find:
Match C
Impacted Endpoint Attributes
Delete All
Close
Test Dynamic Access Policies

For IPsec, AnyConnect Client, Clientless SSL VPN, and Cut-Through-Proxy sessions, you can configure dynamic access policies (DAP) that define which network resources a user is authorized to access. All policies in the table below are evaluated for matching criterion during session establishment. When none of the DAP policies are matched, the ASA will enforce the DfltAccessPolicy.

#	ACL Priority	Name
□	200	LUA-AV-RULE
□	100	QUARANTINE-RULE
□	30	NON-AV/AS/FW-RULE
□	20	AV (AntiVirus)-CHECKS
□	15	AS (Anti-Spyware)-CH
□	10	FW (Firewall)-CHECKS
□	3	AEA-CHECKS-TERMIN
□	2	AEA-CHECKS-TERMIN
□	1	AEA-CHECKS-TERMIN
□	0	AV-CHECKS-CONTINU
□	-	DfltAccessPolicy

Here is a list of all your incompatible existing AV/AS/FW DAP policies. Select 'Delete All' to proceed.

Policy Name	Endpoint ID	Name/Operation/Value

	av.360SafeAV	description = 360天擎
		version = 6
		lastupdate < 2592000
		activescan = ok

	av.BitdefenderAV	description = Bitdefender Total Security
		version = 15.1
		lastupdate < 2592000
		activescan = ok

	av.GrisoftAV	description = AVG Anti-Virus Free
		version = 10
		lastupdate < 2592000
		activescan = ok

	av.NortonAV	description = Symantec Endpoint Protectio version <= 14 lastupdate < 2592000

Here is a list of all your incompatible existing LUA scripts. Select 'Delete All' to proceed.

Policy Name: LUA-AV-RULE

LUA Script:

```
(assert(function()
    local update_days = "15" --days
    local av_lastupdate = update_days*86400
    for k,v in pairs(endpoint.av) do
        if (EVAL(v.activescan, "NE", "ok", "string") or .
        return true
        end
    end
    return false
end)())
```

To test the dynamic access policies currently configu

Note If the backup information is not available, you must repeat the upgrade initiation in the previous step.

c) Click **Delete All**.

Do not fret. Your polices have been saved in the backup. They are migrated using the backup information later in this process.

d) Click **OK** to confirm, then **Apply**, and then **Save.**

Step 3 Close and restart ASDM to reset the configuration.

You must restart ASDM at this point. Do not skip this step.

Step 4 Complete the HostScan upgrade (at Configuration > Remote Access VPN > Secure Desktop Manager > HostScan Image).

Install and Enable HostScan on the ASA again. This time, complete the procedure including saving the configuration.

Step 5 Close and restart ASDM to reset the configuration.

Again, you must restart ASDM at this point. Do not skip this step.

Step 6 Determine the DAP Polices that require migration.

Go to **Configuration > Remote Access VPN > Network (Client) Access > Dynamic Access Policies** to complete the migration.

A **Migrate Policies** action appears and is enabled only when the HostScan image version is greater than or equal to 4.6.x or later. If no attributes need migration, these buttons appear, but are disabled.

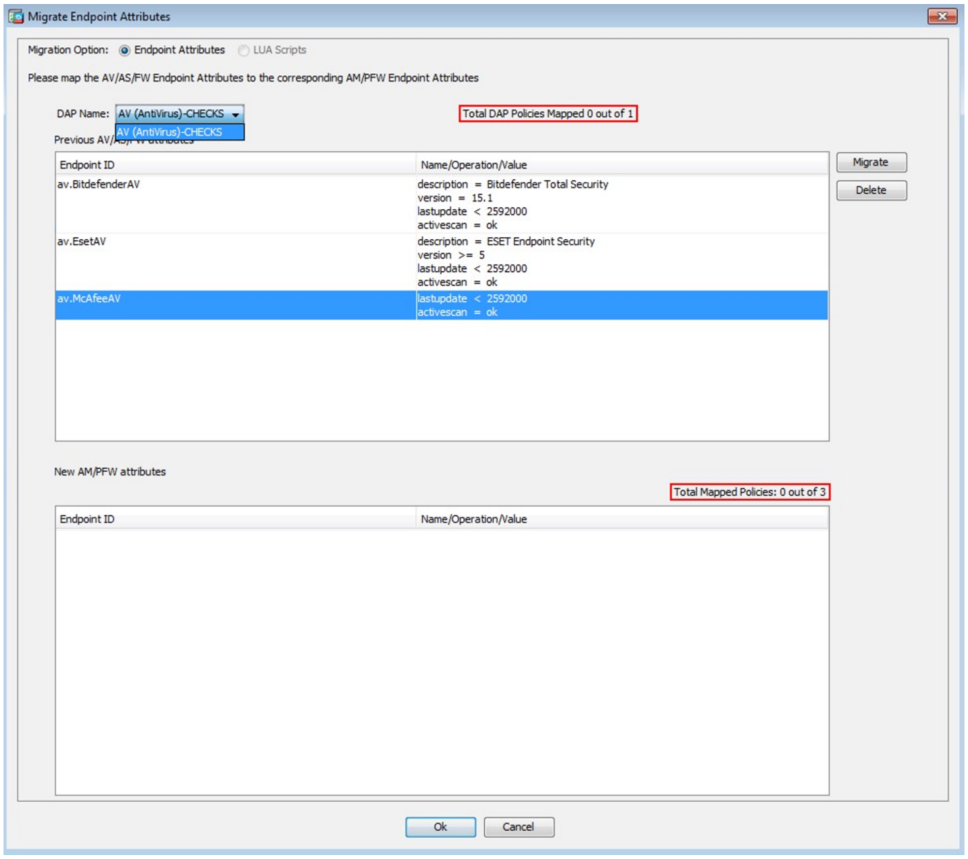
Step 7 Migrate the DAP Policies.

a) Click **Migrate Policies**.

The **Migrate Endpoint Attributes** screen displays. The incompatible AV/AS/FW endpoint attributes and LUA scripts are in the top table, and the current 4.6.x and later AM/PFW migrated endpoint attributes and LUA scripts are in the bottom table.

Take note of these guidelines when migrating policies:

- The UI screen has two radio buttons: one for **Endpoint Attributes** and one for **LUA Scripts**.
- More than one DAP Name may be available in the top left drop-down menu. Make sure to map each one.
- In HostScan 4.6 and later, antimalware attributes (which are antivirus and antispyware attributes combined) are referred to as AM, and firewall attributes are referred to as PFW. For example,
    - endpoint.*av* is now endpoint.*am*
    - endpoint.*as* is also now endpoint.*am*
    - endpoint.*fw* is now endpoint.*pfw*



Migrate Endpoint Attributes

Migration Option: ● Endpoint Attributes ○ LUA Scripts

Please map the AV/AS/FW Endpoint Attributes to the corresponding AM/PFW Endpoint Attributes

DAP Name: AV (AntiVirus)-CHECKS

Total DAP Policies Mapped 0 out of 1

Previous AV/AS/FW attributes

Endpoint ID	Name/Operation/Value

av.BitdefenderAV	description = Bitdefender Total Security
	version = 15.1
	lastupdate < 2592000
	activescan = ok

av.EsetAV	description = ESET Endpoint Security
	version >= 5
	lastupdate < 2592000
	activescan = ok

av.McAfeeAV	lastupdate < 2592000 activescan = ok

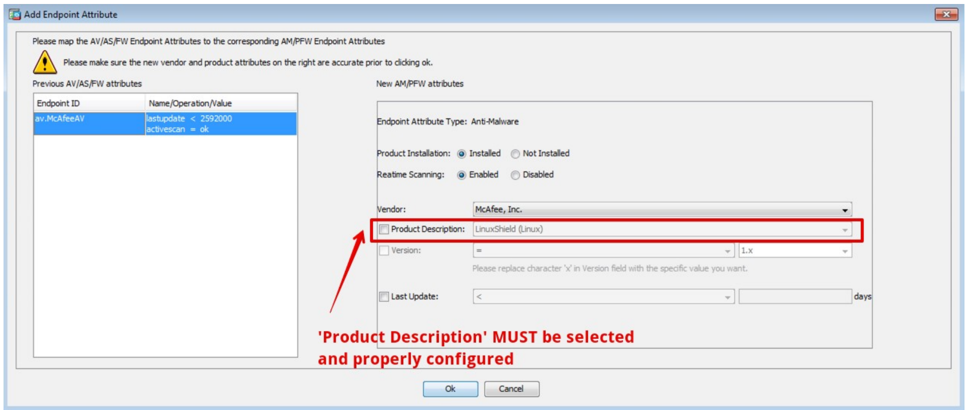
New AM/PFW attributes

Total Mapped Policies: 0 out of 3

Endpoint ID	Name/Operation/Value

b) Migrate each attribute or all at once.

Choose an attribute or script from the top table and click **Migrate.** The Add Endpoint Attribute screen displays. Incompatible endpoint attributes and LUA scripts appear on the left. The right side shows the mapping to the proper AM/PFW attribute and LUA script in the new format.



Please map the AV/AS/FW Endpoint Attributes to the corresponding AM/PFW Endpoint Attributes

Please make sure the new vendor and product attributes on the right are accurate prior to clicking ok.

Previous AV/AS/FW attributes

Endpoint ID	Name/Operation/Value
av.McAfeeAV	lastupdate < 2592000 activescan = ok

New AM/PFW attributes

Endpoint Attribute Type: Anti-Malware

Product Installation: ● Installed ○ Not Installed

Reatime Scanning: ● Enabled ○ Disabled

Vendor: McAfee, Inc.

□ Product Description: LinuxShield (Linux)

□ Version: = 1.x

Please replace character 'x' in Version field with the specific value you want.

□ Last Update: < days

'Product Description' MUST be selected and properly configured

Note You MUST choose **Product Description** and properly configure it to map with a specific product. If not, an incorrect Vendor/Product mapping results, causing the attribute check to not detect the antimalware.

Note When using ASDM version 7.12.1 and later, an error message notifies you of an incorrect Vendor/Product mapping *unless* you choose a Product Description.

c) Click **OK** (after choosing a Product Description).

The old attribute entry or LUA script is removed from the first table, and the new AM/PFW attribute entry or LUA script appears in the second table.

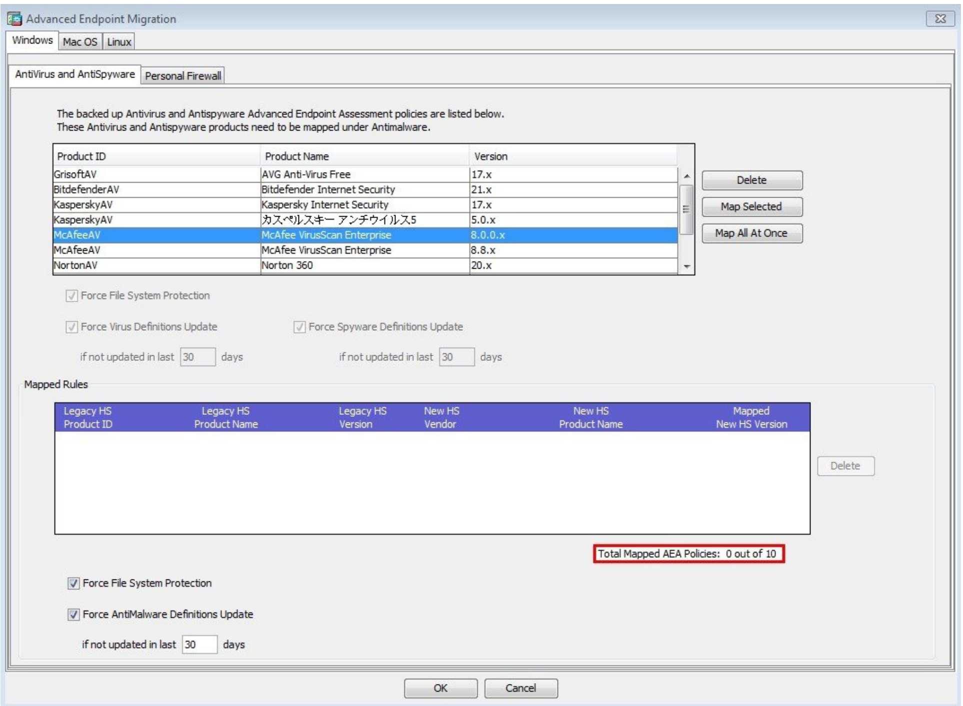
d) Click **Apply** and then **Save.**

Step 8 Determine which advanced endpoint assessment policies require migration.

a) Go to **Configuration** > **Remote Access VPN** > **Secure Desktop Manager** > **HostScan**.

b) Choose **Launch Migration**.

The Advanced Endpoint Migration dialog box displays, listing all antivirus and antispyware policies in the top list. Mapped Rules display in the bottom list as you carry out the migration.



The backed up Antivirus and Antispyware Advanced Endpoint Assessment policies are listed below.
These Antivirus and Antispyware products need to be mapped under Antimalware.

Product ID	Product Name	Version
GrisoftAV	AVG Anti-Virus Free	17.x
BitdefenderAV	Bitdefender Internet Security	21.x
KasperskyAV	Kaspersky Internet Security	17.x
KasperskyAV	カスペルスキー アンチウイルス5	5.0.x
McAfeeAV	McAfee VirusScan Enterprise	8.0.0.x
McAfeeAV	McAfee VirusScan Enterprise	8.8.x
NortonAV	Norton 360	20.x

☑ Force File System Protection

☑ Force Virus Definitions Update ☑ Force Spyware Definitions Update

if not updated in last 30 days if not updated in last 30 days

Mapped Rules

Legacy HS Product ID	Legacy HS Product Name	Legacy HS Version	New HS Vendor	New HS Product Name	Mapped New HS Version

Total Mapped AEA Policies: 0 out of 10

☑ Force File System Protection

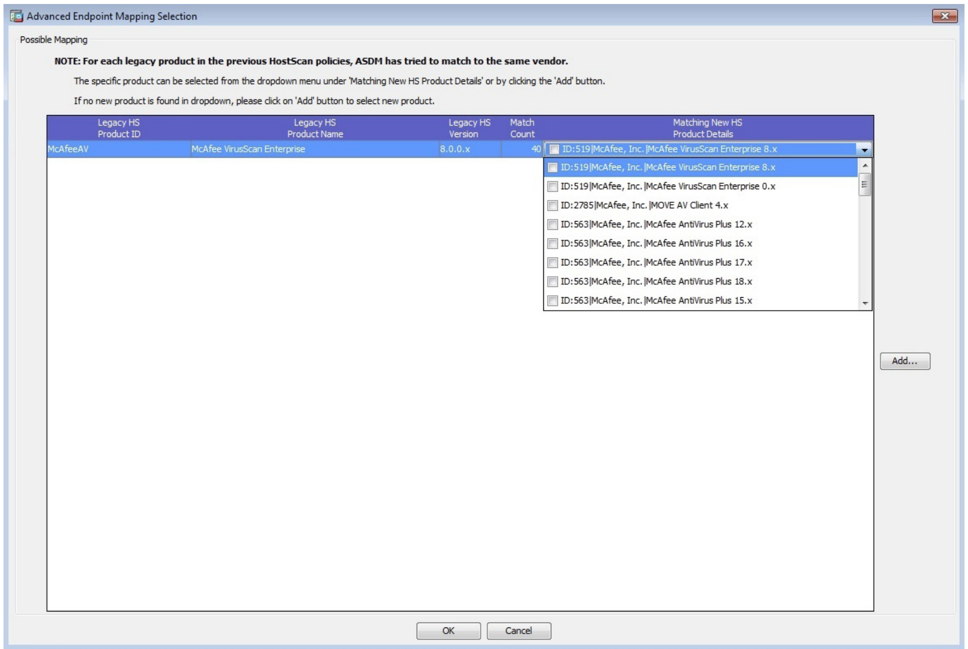
☑ Force AntiMalware Definitions Update

if not updated in last 30 days

Step 9 Migrate the Advanced Endpoint Assessment (AEA) Policies. Repeat this step until all policies are migrated.

a) Choose entries from the top table and click **Map Selected**, or click **Map All At Once**.

A **Possible Mapping** dialog box displays.



Possible Mapping

NOTE: For each legacy product in the previous HostScan policies, ASDM has tried to match to the same vendor.

The specific product can be selected from the dropdown menu under 'Matching New HS Product Details' or by clicking the 'Add' button.

If no new product is found in dropdown, please click on 'Add' button to select new product.

Legacy HS Product ID	Legacy HS Product Name	Legacy HS Version	Match Count	Matching New HS Product Details
McAfeeAV	McAfee VirusScan Enterprise	8.0.0.x	40	□ ID:519|McAfee, Inc. |McAfee VirusScan Enterprise 8.x

□ ID:519|McAfee, Inc. |McAfee VirusScan Enterprise 8.x
□ ID:519|McAfee, Inc. |McAfee VirusScan Enterprise 0.x
□ ID:2785|McAfee, Inc. |MOVE AV Client 4.x
□ ID:563|McAfee, Inc. |McAfee AntiVirus Plus 12.x
□ ID:563|McAfee, Inc. |McAfee AntiVirus Plus 16.x
□ ID:563|McAfee, Inc. |McAfee AntiVirus Plus 17.x
□ ID:563|McAfee, Inc. |McAfee AntiVirus Plus 18.x
□ ID:563|McAfee, Inc. |McAfee AntiVirus Plus 15.x

b) For each legacy product entry, choose from the drop-down list of possible **Matching New HS Product Details** to migrate the policy. Or, click **Add** to choose a policy when no possible matches are shown.

c) Click **OK** to return to the **Advanced Endpoint Migration** screen.

Step 10 Save the migrated AEA policies.

Click **OK** to return to the **HostScan** screen, and then **Apply All.**

Step 11 Remove and re-add any defined LUA scripts.

Existing LUA scripts will not work with HostScan 4.6.x or later. They must be manually removed from your configuration and re-added. Keep in mind the following new guidelines:

- Recreate all antivirus specifications to antimalware specifications by changing **endpoint.av** to **endpoint.am**.
- Recreate all antispyware specifications to antimalware specifications by changing **endpoint.as** to **endpoint.am**.
- Recreate all firewall specifications by changing **endpoint.fw** to **endpoint.pfw**.
- Use LUA Script for 'ANY' Antimalware (endpoint.am) with Last Update, on page 14 to check for ANY antimalware (endpoint.am) or LUA Script for 'ANY' Personal Firewall, on page 14 to check for ANY firewall (endpoint.pfw).

Refer to the supporting LUA procedures to update your scripts.

Step 12 Migration is complete. You must close and restart ASDM to reset the configuration.

Fallback AnyConnect HostScan 4.6.x or Later to 4.3.x

These files contain the configuration and policies that were in place when running the older HostScan release. They were created and saved in the `disk0/HostScan_Migration_Backup` directory when you installed the newer HostScan release.

This procedure guides you through a fallback to your previous HostScan release of 4.3.x or earlier. It restores the antivirus (AV), antispyware (AS), and firewall (FW) policies that were in place before attempting a migration to HostScan 4.6.x or later.

Before you begin

In order to be able to fallback to the earlier HostScan release, you must have the following backup files.

```
dap-bkp.xml
data-bkp.xml
data-record-bkp.txt
```

Procedure

Step 1 Save the configuration and policies that were associated with the older HostScan release from the backup directory.

These are the configuration and policies that were in place before you upgraded. They were created when you initially installed the newer HostScan release. They are necessary to restore your appliance to its previous state.

a) Go to **Tools** > **File Management**.
b) Copy the `dap-bkp.xml`, `data-bkp.xml` and `data-record-bkp.txt` from the `HostScan_Migration_Backup` folder under `disk0` on the ASA to your local system.
c) Delete the `HostScan_Migration_Backup` folder under `disk0` on the ASA.

Step 2 Uninstall the newer release of HostScan, 4.6.x or later.

a) In ASDM, navigate to **Configuration > Remote Access VPN > Secure Desktop Manager > Host Scan Image** to uninstall HostScan.

b) Click **Uninstall**, and then **Yes** to confirm.

Allow this to finish,and then restart ASDM before proceeding.

Step 3 Save any configuration and policies that are associated with this now uninstalled, newer version of HostScan.

a) Go to **Tools > File Management**.

b) Rename `disk0:/dap.xml` to `dap-new.xml`.

c) Rename `disk0:/sdesktop/data.xml` to `data-new.xml`.

These files, containing configuration and polices for the newer release, can be used to restore any new or migrated definitions you had put in place, and may want to go back to in the future.

Step 4 Install and Enable HostScan on the ASA to which you are falling back.

Allow this to finish and restart ASDM before proceeding.

Step 5 Restore the back-up configuration and policies.

a) Rename the saved `dap-bkp.xml` on your local system to `dap.xml`.

b) Rename the saved `data-bkp.xml` on your local system to `data.xml`.

c) Navigate to **Tools > File Management**.

d) Copy the `dap.xml` on your local system to `disk0` on the ASA.

e) Copy the `data.xml` on your local system to `disk0:/sdesktop/` on the ASA.

f) Copy the DAP CLI from the `data-record-bkp.txt` and execute it on the ASA.

Step 6 Close and restart ASDM.

You must do this to finish the process.

Supporting Procedures

Install and Enable HostScan on the ASA

Use this procedure to upload, or upgrade, and enable a new HostScan image on the ASA. This image can enable the HostScan functionality for AnyConnect.

You can specify a standalone HostScan package.

Note You do not need to restart the security appliance after you install or upgrade HostScan; however, you must exit and restart Adaptive Security Device Manager (ASDM) to access Secure Desktop Manager.

Before you begin

Note If you are attempting to upgrade to HostScan version 4.6.x or later from a 4.3.x version or earlier, you will receive an error message due to the fact that all existing AV/AS/FW DAP policies and LUA script(s) that you have previously established are incompatible with HostScan 4.6.x or later.

You must perform a one-time migration procedure to adapt your configuration. This procedure involves leaving this dialog box to migrate your configuration for compatibility with HostScan 4.6.x and later before saving this configuration. Abort this procedure and refer to the AnyConnect HostScan 4.3.x to 4.6.x or Later Migration Guide for detailed instructions. Briefly, migration involves navigating to the ASDM DAP policy page to review and manually delete the incompatible AV/AS/FW attributes, and then reviewing and rewriting LUA scripts.

Procedure

Step 1 Download the `hostscan_version-k9.pkg` file to your computer.

Step 2 Open ASDM and choose **Configuration** > **Remote Access VPN > Secure Desktop Manager** > **Host Scan Image**. ASDM opens the HostScan Image panel.

Step 3 Click **Upload** to prepare to transfer a copy of the HostScan package from your computer to a drive on the ASA.

Step 4 In the Upload Image dialog box, click **Browse Local Files** to search for the HostScan package on your local computer.

Step 5 Select the `hostscan_version-k9.pkg` file you downloaded above and click **Select**. The path to the file you selected is in the **Local File Path** field and the **Flash File System Path** field reflects the destination path of the HostScan package. If your ASA has more than one flash drive, you can edit the **Flash File System Path** to indicate another flash drive.

Step 6 Click **Upload File**. ASDM transfers a copy of the file to the flash card. An Information dialog box displays the following message:

```
File has been uploaded to flash successfully.
```

Step 7 Click **OK**.

Step 8 In the Use Uploaded Image dialog, click **OK** to use the HostScan package file you just uploaded as the current image.

Step 9 Check **Enable Host Scan** if it is not already checked.

Step 10 Click **Apply**.

Step 11 From the **File** menu, choose **Save Running Configuration To Flash**.

Endpoint Attribute Definitions

The following endpoint selection attributes are available for DAP use.The Attribute Name field shows you how to enter each attribute name in a LUA logical expression, used in the Advanced area in Dynamic Access Policy Selection Criteria pane. The *label* variable identifies the application, filename, process, or registry entry.

Attribute Type	**Attribute Name**	**Source**	**Value**	**Max String Length**	**Description**
Antimalware (Requires Cisco Secure Desktop)	endpoint.am["*label*"].exists	Host Scan	true	—	Antimalware program exists
	endpoint.am["*label*"].version		string	32	Version
	endpoint.am["*label*"].description		string	128	Antimalware description
	endpoint.am["*label*"].lastupdate		integer	—	Seconds since update of antimalware definitions
Personal firewall (Requires Secure Desktop)	endpoint.pfw["*label*"].exists	Host Scan	true	—	The personal firewall exists
	endpoint.pfw["*label*"].version		string	string	Version
	endpoint.pfw["*label*"].description		string	128	Personal firewall description
AnyConnect (Does not require Cisco Secure Desktop or Host Scan)	endpoint.anyconnect. clientversion	Endpoint	version	—	AnyConnect client version
	endpoint.anyconnect. platform		string	—	Operating system on which AnyConnect client is installed
	endpoint.anyconnect. platformversion		version	64	Version of operating system on which AnyConnect client is installed
	endpoint.anyconnect. devicetype		string	64	Mobile device type on which AnyConnect client is installed
	endpoint.anyconnect. deviceuniqueid			64	Unique ID of mobile device on which AnyConnect client is installed
	endpoint.anyconnect. macaddress		string	—	MAC Address of device on which AnyConnect client is installed Must be in the format xx-xx-xx-xx-xx-xx, where 'x' is a valid hexadecimal character
Application	endpoint.application. clienttype	Application	string	—	Client type: CLIENTLESS ANYCONNECT IPSEC L2TP

Attribute Type	**Attribute Name**	**Source**	**Value**	**Max String Length**	**Description**
Device	endpoint.device. hostname	Endpoint	string	64	Host Name only. Not FQDN
	endpoint.device.MAC		string	—	Mac Address for a network interface card. Only one Mac address per entry Must be in the format xxxx.xxxx.xxxx where x is a hexadecimal character.
	endpoint.device.id		string	64	BIOS Serial Number. The number format is manufacturer-specific. There is no format requirement
	endpoint.device.port		string	—	TCP port in listening state You can define a single port per line An integer between 1 and 65535
	endpoint.device. protection_version		string	64	Version of Host Scan image they are running
	endpoint.device. protection_extension		string	64	Version of Endpoint Assessment (OPSWAT)
File	endpoint.file["*label*"].exists	Secure Desktop	true	—	The files exists
	endpoint.file[“label”]. endpointid				
	endpoint.file["*label*"]. lastmodified		integer	—	Seconds since file was last modified
	endpoint.file["*label*"]. crc.32		integer	—	CRC32 hash of the file
NAC	endpoint.nac.status	NAC	string	—	User defined status string
Operating System	endpoint.os.version	Secure Desktop	string	32	Operating system
	endpoint.os.servicepack		integer	—	Service pack for Windows
Policy	endpoint.policy.location	Secure Desktop	string	64	Location value from Cisco Secure Desktop
Process	endpoint. process["*label*"].exists	Secure Desktop	true	—	The process exists
	endpoint. process["*label*"].path		string	255	Full path of the process

Attribute Type	Attribute Name	Source	Value	Max String Length	Description
Registry	endpoint. registry["*label*"].type	Secure Desktop	*dword string*	—	dword
	endpoint. registry["*label*"].value		string	255	Value of the registry entry
VLAN	endoint.vlan.type	CNA	string	—	VLAN type: ACCESS AUTH ERROR GUEST QUARANTINE ERROR STATIC TIMEOUT

Create Additional DAP Selection Criteria in DAP Using LUA

This section provides information about constructing logical expressions for AAA or endpoint attributes. Be aware that doing so requires sophisticated knowledge of LUA. You can find detailed LUA programming information at http://www.lua.org/manual/5.1/manual.html.

In the Advanced field you enter free-form LUA text that represents AAA and/or endpoint selection logical operations. ASDM does not validate text that you enter here; it just copies this text to the DAP policy file, and the ASA processes it, discarding any expressions it cannot parse.

This option is useful for adding selection criteria other than what is possible in the AAA and endpoint attribute areas above. For example, while you can configure the ASA to use AAA attributes that satisfy any, all, or none of the specified criteria, endpoint attributes are cumulative, and must all be satisfied. To let the security appliance employ one endpoint attribute or another, you need to create appropriate logical expressions in LUA and enter them here.

The following sections provide detailed explanations of creating LUA EVAL expressions, as well as examples.

- Syntax for Creating LUA EVAL Expressions, on page 13
- Examples of DAP EVAL Expressions, on page 17
- Additional LUA Functions, on page 15

Syntax for Creating LUA EVAL Expressions

Note If you must use Advanced mode, we recommend that you use EVAL expressions whenever possible for reasons of clarity, which makes verifying the program straightforward.

EVAL(<*attribute*> , <comparison>, {<*value*> | <*attribute*>}, [<type>])

<attribute>	AAA attribute or an attribute returned from Cisco Secure Desktop, see Endpoint Attribute Definitions, on page 10 for attribute definitions

<comparison>	One of the following strings (quotation marks required)	
	“EQ”	equal
	“NE”	not equal
	“LT”	less than
	“GT”	greater than
	“LE”	less than or equal
	“GE”	greater than or equal
<value>	A string in quotation marks that contains the value to compare the attribute against	
<type>	One of the following strings (quotation marks required)	
	“string”	case-sensitive string comparison
	“”	case-insensitive string comparison
	“integer”	number comparison, converts string values to numbers
	“hex”	number comparison using hexadecimal values, converts hex string to hex numbers
	“version”	compares versions of the form X.Y.Z. where X, Y, and Z are numbers

LUA Procedures for HostScan 4.6 and Later

LUA Script for 'ANY' Antimalware (endpoint.am) with Last Update

Use the following LUA script to check for 'ANY' antimalware product/vendor (endpoint.am). Modifications may apply to accommodate a different Last Update interval. The following example shows how a Last Update must have been performed in <30 days (noted as 2592000 seconds).

```
assert(function()
  for k,v in pairs(endpoint.am) do
    if(EVAL(v.activescan, "EQ", "ok", "string")and EVAL (v.lastupdate, "LT", "2592000", "integer"))
     then
             return true
         end
  end
  return false
end)()
```

LUA Script for 'ANY' Personal Firewall

Use the following LUA script to check for 'ANY' firewall product/vendor (endpoint.pfw):

```
assert(function()
    for k,v in pairs(endpoint.pfw) do
         if (EVAL(v.enabled, "EQ", "ok", "string")) then
```

```
                return true
            end
        end
        return false
end)()
```

Additional LUA Functions

When working with dynamic access policies, you might need additional flexibility of match criteria. For example, you might want to apply a different DAP based on the following:

- CheckAndMsg is a LUA function that you can configure DAP to call. It generates a user message based on a condition.
- Organizational Unit (OU) or other level of the hierarchy for the user object.
- Group names that follow a naming convention with many possible matches might require the ability to use a wildcard.

You can accomplish this flexibility by creating a LUA logical expression in the Advanced section of the DAP pane in ASDM.

The DAP CheckAndMsg Function

The ASA displays the message to the user only when the DAP record containing the LUA CheckAndMsg function is selected and results in a connection termination.

The syntax of the CheckAndMsg function follows:

```
CheckAndMsg(value, “<message string if value is true>”, “<message string if value if false>”)
```

Be aware of the following when creating CheckAndMsg functions:

- CheckAndMsg returns the value passed in as its first argument.
- Use the EVAL function as the first argument if you do not want to use string comparison. For example:

  ```
  (CheckAndMsg((EVAL(...)) , "true msg", "false msg"))
  ```

  CheckandMsg returns the result of the EVAL function, and the security appliance uses it to determine whether to choose the DAP record. If the record is selected and results in termination, the security appliance displays the appropriate message.

OU-Based Match Example

DAP can use many attributes returned from an LDAP server in a logical expression. See the DAP trace section for example output of this, or run a debug dap trace.

The LDAP server returns the user Distinguished Name (DN). This implicitly identifies where in the directory the user object is located. For example, if the user DN is CN=Example User, OU=Admins, dc=cisco, dc=com, this user is located in OU=Admins,dc=cisco,dc=com. If all administrators are in this OU, or any container below this level, you can use a logical expression to match this criteria as follows:

```
assert(function()
   if ( (type(aaa.ldap.distinguishedName) == "string") and
        (string.find(aaa.ldap.distinguishedName, "OU=Admins,dc=cisco,dc=com$") ~= nil) ) then
       return true
   end
   return false
end)()
```

In this example, the string.find function allows for a regular expression. Use the $ at the end of the string to anchor this string to the end of the distinguishedName field.

Group Membership Example

You can create a basic logical expression for pattern matching of AD group membership. Because users can be members of multiple groups, DAP parses the response from the LDAP server into separate entries in a table. You need an advanced function to accomplish the following:

- Compare the memberOf field as a string (in the event the user belongs to only one group).
- Iterate through each returned memberOf field if the returned data is of type "table."

The function we have written and tested for this purpose is shown below. In this example, if a user is a member of any group ending with "-stu," they match this DAP.

```
assert(function()
   local pattern = "-stu$"
   local attribute = aaa.ldap.memberOf
   if ((type(attribute) == "string") and
       (string.find(attribute, pattern) ~= nil)) then
       return true
   elseif (type(attribute) == "table") then
       local k, v
       for k, v in pairs(attribute) do
           if (string.find(v, pattern) ~= nil) then
               return true
           end
       end
   end
   return false
end)()
```

Deny Access Example

You can use the following function to deny access in the absence of an antimalware program. Use it with a DAP that has Action set to terminate.

```
assert(
    function()
for k,v in pairs(endpoint.am) do

        if (EVAL(v.exists, "EQ”, "true", "string")) then

            return false

        end
    end
    return CheckAndMsg(true, "Please install antimalware software before connecting.", nil)
end)()
```

If a user lacking an antimalware program attempts to log in, DAP displays the following message:

```
Please install antimalware software before connecting.
```

Examples of DAP EVAL Expressions

Study these examples for help in creating logical expressions in LUA:

Description	Example
Endpoint LUA checks for Windows 10	`(EVAL(endpoint.os.version,"EQ","Windows 10","string"))`
Endpoint LUA checks for a match on CLIENTLESS OR CVC client types.	`(EVAL(endpoint.application.clienttype,”EQ”,"CLIENTLESS") or EVAL(endpoint.application.clienttype, “EQ”,"CVC"))`
Endpoint LUA checks if a single Antimalware program Symantec Enterprise Protection is installed on the user PC, displays a message if it is not.	`(CheckAndMsg(EVAL(endpoint.am["538"].description,"NE","Symantec Endpoint Protection","string"),"Symantec Endpoint Protection was not found on your computer", nil))`
Endpoint LUA checks for McAfee Endpoint Protection versions 10 to 10.5.3 and versions above 10.6.	`(EVAL(endpoint.am["1637"].version,"GE","10","version") and EVAL(endpoint.am["1637"].version,"LT","10.5.4","version") or EVAL(endpoint.am["1637"].version,"GE","10.6","version"))`
Endpoint LUA checks if McAfee Antimalware definitions have been updated within the last 10 days(864000 sec) and displays a message if an update is needed.	`(CheckAndMsg(EVAL(endpoint.am["1637"].lastupdate,"GT","864000","integer"),"Update needed! Please wait for McAfee to load the latest dat file.", nil))`
Check for a specific hotfix after debug dap trace returns: `endpoint.os.windows.hotfix["KB923414"] = "true";`	`(CheckAndMsg(EVAL(endpoint.os.windows.hotfix["KB923414"],"NE","true"), "The required hotfix is not installed on your PC.",nil))`

Check for Antimalware Programs and Provide Messages

You can configure messages so that the end users are aware of and able to fix problems with their antimalware software. If access is allowed, the ASA displays all messages generated in the process of DAP evaluation on the portal page. If access is denied, the ASA collects all messages for the DAP that caused the "terminate" condition and displays them in the browser on the logon page.

The following example shows how to use this feature to check on the status of Symantec Endpoint Protection.

1. Copy and paste the following LUA expression into the Advanced field of the Add/Edit Dynamic Access Policy pane (click the double arrow on the far right to expand the field).

   ```
   (CheckAndMsg(EVAL(endpoint.am["538"].description,"EQ","Symantec Endpoint Protection","string") and
   EVAL(endpoint.am["538"].activescan,"NE","ok","string") "Symantec Endpoint Protection is disabled. You must
    enable before being granted access", nil))
   ```

2. In that same Advanced field, click the **OR** button.

3. In the Access Attributes section below, in the leftmost tab, Action, click **Terminate**.

4. Connect from a PC that has Symantec Endpoint Protection installed, but has Symantec Endpoint Protection disabled. The expected result is that the connection is not allowed and that the user will be presented the message "Symantec Endpoint Protection is disabled. You must enable before being granted access."

Check for Antimalware Programs and Definitions Older than 2 Days

This example checks for the presence of the Symantec and McAfee antimalware programs, and whether the virus definitions are older than 2 days (172,800 seconds). If the definitions are older than 2 days, the ASA terminates the session with a message and links for remediation. To accomplish this task, perform the following steps.

1. Copy and paste the following LUA expression into the Advanced field of the Add/Edit Dynamic Access Policy pane:

   ```
   (CheckAndMsg(EVAL(endpoint.am["538"].description,"EQ","Symantec Endpoint Protection","string") and
   EVAL(endpoint.am["538"].lastupdate,"GT","172800","integer"), "Symantec Endpoint Protection Virus Definitions
    are Out of Date. You must run LiveUpdate before being granted access", nil)) or
   (CheckAndMsg(EVAL(endpoint.am["1637"].description,"EQ","McAfee Endpoint Security","string") and
   EVAL(endpoint.am["1637"].lastupdate,"GT","172800","integer"), "McAfee Endpoint Security Virus Definitions
   are Out of Date. You must update your McAfee Virus Definitions before being granted access", nil))
   ```

2. In that same Advanced field, click **AND**.

3. In the Access Attributes section below, in leftmost tab Action, click **Terminate**.

4. Connect from a PC that has Symantec and McAfee antimalware programs with versions that are older than 2 days.

   The expected result is that the connection is not allowed and that the user is presented a message that the virus definitions are out of date.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA 95134-1706
USA

Asia Pacific Headquarters
CiscoSystems(USA)Pte.Ltd.
Singapore

Europe Headquarters
CiscoSystemsInternationalBV
Amsterdam,TheNetherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.