A WHITE PAPER

# **HBSS Install Notes**

Part 2 of 2: Configure ePO Server



- DoD Information Systems Agency (DISA) provides Host-Based Security System (HBSS)
- Deploying HBSS is time-consuming and error-prone, this Guide aims to alleviate this problem
- Enclave-specific decisions and strategy must be formulated for an effective HBSS deployment



## **Table of Contents**

1.0	HBSS Notes	2 of 2 – Configure ePO Server	2
1.	1 About th	ne Author	2
1.	2 Host-Ba	sed Security System (HBSS)	2
	1.2.1 D	ISA Documentation Sources	2
	1.2.2 el	PO Server Configuration: Module 2 and Beyond	3
	1.2.2.1	Step 2.1: Gather Information	3
	1.2.2.2	Step 2.2: Deploy McAfee Agent to ePO Server	8
	1.2.2.3	Step 2.3: Import Client Computers	8
	1.2.2.4	Step 2.3: Deploy McAfee Agent to Client Computers	10
	1.2.2.5	Step 2.5: Deploy SuperAgent Distributed Repository (SADR)	12
	1.2.2.6	Step 2.6: Deploy Rogue System Detection (RSD) Sensor	12
	1.2.2.7	Step 3.1: Global Updating	14
	1.2.2.8	Step 3.2: McAfee Agent Product Update	14
	1.2.2.9	Step 3.3:Daily Incremental Repository Replication Scheduled Task	15
	1.2.2.10	Step 3.4: Weekly Full Repository Replication Scheduled Task	15
	1.2.2.11	Step 3.5: Deploy Asset and HIPS Modules	15
	1.2.2.12	Step 3.6: Configure ePO Daily Inactive Agent Task	16
	1.2.2.13	Module 4: Import Queries/Create Custom Dashboard	17
	1.2.2.14	Module 5: Change User Credentials	17
	1.2.2.15	Module 6: PKI Installation and User Migration	20
	1.2.2.16	Module 7: Configure SSL Console Certificate (Section 7.1)	20
	1.2.2.17	Module 7: Configure SSL Console Certificate (Section 7.2)	21
	1.2.2.18	Module 8: Deploy HIPs to ePO	22
	1.2.3 el	PO Server Configuration: Final Steps	22



## **Version Control**

#### Change Activity Log

Date	Version	Comments	Owner
24 JUN 13	Draft A	Initial creation by extraction from "Tech Guide.docx"	Andrew Bruce
21 AUG 13	Draft A	Documentation on HBSS ePO Server, redacted from primary documents.	Andrew Bruce



## 1.0 HBSS Notes 2 of 2 – Configure ePO Server

This section is an excerpt from an actual Department of Defense (DoD) project that required the DoD Information Systems Agency (DISA) Host-Based Security System (HBSS) element. The HBSS element consists of the McAfee ePolicy Orchestrator (ePO) Server as well as other required software components. The section has been redacted to remove any identifying information, and is presented to the Information Assurance (IA) community in the hopes it will be useful to others tasked with implementing the HBSS component.

### 1.1 About the Author

Andrew Bruce is a Lead Scientist for Computer Sciences Corporation (CSC) in the Army Programs group of the North American Public Sector. CSC provides professional services to the Federal Government and the Department of Defense, specializing in customizing and developing architecture and governance models that enable tight integration to the Army's enterprise portfolio management initiatives. Mr. Bruce's job responsibilities include: working directly with customers and partners for new business development, supporting proposal efforts, overseeing Army customers' network infrastructure, working with project managers to ensure project completion, managing software development efforts throughout the entire system life-cycle, and leading new technology research and proofs-of-concept. After a career spanning three decades in shrink-wrap, commercial, and corporate software development, Mr. Bruce is focusing on Information Assurance to achieve his goal of building and managing large data centers providing cloud computing utility services for commercial and Government customers. Mr. Bruce holds the CISSP, PMP, and FITSP-D certifications as well as other vendor-specific Computing Environment (CE) certifications; he is proud to have received the Master's Degree in Information Assurance from Norwich University.

## 1.2 Host-Based Security System (HBSS)

The HBSS Notes 1 of 2 (see <u>https://www.softwareab.net/wordpress/?p=397</u>) covers the initial build from the pre-build HBSS package from DISA. Thus, we concentrate in this section on the ePO Server Configuration with the assumption that the admin has already completed the basic HBSS deployment.

#### 1.2.1 DISA Documentation Sources

The reader must have a valid Common Access Card (CAC) in order to view some of these resources:

- Main DISA HBSS Landing Page (<u>http://www.disa.mil/Services/Information-Assurance/HBS/HBSS</u>) Use this page to access HBSS news, documentation resources, the DISA Patch Repository, and more.
- **DISA HBSS Patch Repository** (<u>https://patches.csd.disa.mil/CollectionInfo.aspx?id=394</u>) Access the supported HBSS versions (4.5 and 4.6 as of 21 AUG 13).
- HBSS 4.6 Patch Repository (<u>https://patches.csd.disa.mil/Metadata.aspx?id=95505</u>) Access the Guides
  referenced in this document.

The specific DISA HBSS Guides from the 4.6 Patch Repository include: HBSS Notes 2 of 2 - Configure ePO Server.docx.doc



- CM-171644-HBSS\_4.6\_Build\_From\_Image\_Guide\_V1R4.pdf This is the Guide used for Part 1 of this article (available at <a href="https://www.softwareab.net/wordpress/?p=397">https://www.softwareab.net/wordpress/?p=397</a>). It leads the System Administrator (SA) through the basic steps required to deploy the HBSS image into a virtual machine (VM).
- CM-171645-HBSS\_4.6\_Configuration\_Guide\_V3R3.pdf This is the Guide primarily used for this article (Part 2 of the HBSS Notes. This article provides advice, strategy, and error identification / correction for the SA to use during an ePO Server configuration. It is referenced as the "DISA ePO Server Configuration Guide" in the text below.

Continue to the next section.

#### 1.2.2 ePO Server Configuration: Module 2 and Beyond

You should be at this section after you have either deployed from the DISA pre-built image or from the manual install. In either case, Module 2 from the DISA ePO Server Configuration Guide is all about deployment to the environment. This section documents how the HBSS packages were deployed within our target environment.

The complexity required to configure the ePO Server and to deploy agents requires individual sections for each major step.

#### 1.2.2.1 Step 2.1: Gather Information

Information gathering consists of two primary steps:

- 1. Understand the server landscape for ePO Agent deployment
- 2. Review and plan policies for deployment.

This section covers each of these steps.

#### 1.2.2.1.1 Understand the Server Landscape for ePO Agent Deployment

Begin by verifying the following table for the proposed clients and the ePO Server. The ePO Server is not in the domain so all settings are from local policy. Choose a standard system from the target environment for the "Client" settings to compare domain-level GPOs to local policy. Summarized in the table below:

Question	ePO Server	OUR TARGET ENVIRONMENT Client
How many computers are designated to receive the McAfee Agent?	[n/a]	TBD
What is the Network security: LAN Manager Authentication level local security policy setting found on the proposed clients? (ePO server default is 5)	5	5 (Domain)
What is the Microsoft Network client: Digitally sign communications (always) local security policy setting found on	Enabled	Enabled (Local)



the proposed clients?		
What is the Microsoft Network server: Digitally sign communications (always) local security policy setting found on the proposed clients?	Enabled	Enabled (Local)
What is the Network security: minimum session security for NTLM SSP base (including secure RPC) clients local security policy setting found on the proposed clients? (ePO server default is to have all 4 boxes checked)	Only two boxes; both checked	Only two boxes; both checked (Local)
What is the Network security: minimum session security for NTLM SSP base (including secure RPC) server local security policy setting found on the proposed clients? (ePO server default is to have all 4 boxes checked)	Only two boxes; both checked	Only two boxes; both checked (Local)
What is the System cryptography: Use FIPS compliant algorithms for encryption, hashing and signing local security policy setting found on the proposed clients?	Enabled	Enabled (Domain)
Do the proposed clients have file and print sharing enabled? (\My computer\Explore\Tools\Folder Options\View\Use Simple File Sharing)	Yes	Yes
Do the proposed clients have remote registry access enabled (\My Computer\Manage\Services and Applications\Services\Remote Registry)?	Yes	Yes
Do the proposed clients have the ADMIN\$ share enabled?	Yes	Yes

Once all information is gathered proceed to the next step.

#### 1.2.2.1.2 Review and Plan ePO Agent Deployment Policies

At first glance the process of review and planning the policies for the deployment ePO agents may appear unnecessary. After all, the DISA guide spends a significant amount of space to instruct the sysadmin on how to duplicate and modify the ePO policies. However, the policies applied to running VMs within an enclave like our target environment have the potential to break running applications. Thus, the agent-specific policies must be reviewed and a plan created for safe ePO agent deployment.

The analysis approach is to expand the System Tree to the Client Agents subgroup and to review the possible Assigned Policies as shown in the shot below. (Be aware that the server certificate is – at this point – invalid and will be updated later in the process.)



ePolicy Orchestrator 4.6.6 (Build: 1	76) - Windows Intern	et Explorer				
COO V W https://hbssep0002mv.		P 💌 😵 Certi	ficate error 😽 👳	ePolicy Orchestrator	4.6.6 ( 🗙	
Server: HBSSEPO002MV   Time: 8/	12/13 9:52:03 AM EC	)T   User: admi	n   <u>Log Off</u>			An
Menu System Tre	e of					
	Dashboa	ards System	Tree Queries & Re	ports Policy Catal	Check each pro	duct
▼ My Organization To review	Systems Ass	Inea Policies	Assigned Clienc Ta	sks Group Detail		
	Product: Asset	Baseline Monit	or 3.5.1.0		nforcement status: <u>En</u>	forcing
Client Agents	Category	Policy	Server	Inherit from	Broken Inheritance	Action
ePO Server	Trusted Activity	McAfee Defa	Local (HBSSEPO00;	Global Root	None	Edit A
RSD	File Permissions	My Default	Local (HBSSEPO00)	My Organization	None	Edit A
SADR	Registry Monitor	My Default	Local (HBSSEPO00)	My Organization	None	Edit A
► Lost&Found		-	Review eac	h policy		

**Note on "Enforcement Status" from above:** Next to each Product is a link labeled "Enforcement status" which can be clicked and set to "Enforcing" or "Not enforcing" as shown below:

Enforcement for: My Organization >	> Client Agents 1 Data Loss Prevention 9.2.0.0				
Inherit from: Must set this to "Brea inheritance" to change	Global Root     Specific product     Break inheritance and assign the policy and settings below e				
Enforcement status:	Enforcing     Not enforcing     Current setting				
Lock policy inheritance	<ul> <li>Unlocked (allow breaking inheritance below this point)</li> <li>Locked (prevent breaking inheritance below this point)</li> </ul>				
Broken inheritance below this point:	None				

However, this technique cannot be used to plan for system impact; for example, to set a policy to "Not enforcing" and then rely on logged events to determine whether the policy would break system functionality. Instead, the "Not enforcing" simply *ignores* the policy entirely from the agent.

Thus, it appears that all ePO policies must be "enforced" at the global product level. Within each ePO Policy, the administrator must examine the policy settings carefully prior to deployment. Where possible, policy-specific options may be used to control how violations are handled (that is, enforced or simply logged).

The following table identifies the policies as of 4.6.6, the possible system impact, and the planned approach. In the "System Impact" the possible values are:

- <n/a> Policy deployment will not break systems will not break even if the policy rules are enforced
- X Policy deployment may break systems



Not every Product is covered below; only those that apply to the D5-141 environment.

Product	Category	Policy	System Impact	Default Setting	Planned Setting
Asset Baseline Monitor 3.5.1.0	Trusted Activity	McAfee Default	<n a=""></n>	<empty></empty>	<default></default>
Asset Baseline Monitor 3.5.1.0	File Permissions	My Default	<n a=""></n>	<empty></empty>	<default></default>
Asset Baseline Monitor 3.5.1.0	Registry Monitor	My Default	<n a=""></n>	<empty></empty>	<default></default>
Data Loss Prevention 9.2.0.0: Policies	Agent Configuration	McAfee Default	Х	<not enforced&gt;</not 	<not enforced=""></not>
Data Loss Prevention 9.2.0.0: Policies	Computers Assignment Group	McAfee Default	<n a=""></n>	<empty></empty>	<default></default>
HIPS 8.0: Firewall	Firewall Options (Windows)	My Default	Х	<not enabled&gt;</not 	<default> (use existing client firewall rules)</default>
HIPS 8.0: Firewall	DNS Blocking (Windows)	My Default	Х	<empty></empty>	<default></default>
HIPS 8.0: Firewall	Firewall Rules (Windows)	My Default	X	PING, iSCSI, and other protocols blocked	<default> (because firewall options default to not enabled)</default>
HIPS 8.0: General	Client UI (Windows)	[ENCLAVE] – HIPS Client UI	<n a=""></n>	Standard logging rules	<default></default>
HIPS 8.0:	Trusted	[ENCLAVE]	<n a=""></n>	Retina	<default></default>



Product	Category	Policy	System Impact	Default Setting	Planned Setting
General	Networks (Windows)	– All Trusted Networks		server specified	
HIPS 8.0: General	Trusted Applications (All Platforms)	[ENCLAVE] – Client Trusted Applications	<n a=""></n>	<disa- specified&gt;</disa- 	<default></default>
HIPS 8.0: IPS	IPS Options (All Platforms)	[ENCLAVE] – HIPS IPS Options	Х	Enabled	<default> (leave as enabled as IPS protection can be modified to log-only)</default>
HIPS 8.0: IPS	IPS Protection (All Platforms)	[ENCLAVE] – HIPS IPS Protection	X	"High" severity can initiate actions	Modify so that all severity are asset to "Log":  Reaction based on signature severity levels  Reaction High High Log
HIPS 8.0: IPS	IPS Rules (All Platforms)	[ENCLAVE] – HIPS IPS Rules <disa base&gt; <mcafee></mcafee></disa 	<n a=""></n>	<default></default>	Accept the default signatures; the signatures by themselves can never break system functionality.
LinuxShield 1.5.1	On-Access Scanning	McAfee Default	Х	Signature- based	<default></default>
McAfee Agent	General	My Default	<n a=""></n>	Push to agent	<default> (does not look like the agent by itself can break any system functionality)</default>
McAfee Agent	Repository	My Default	<n a=""></n>	Push to agent	<default></default>
McAfee Agent	Troubleshooting	My Default	<n a=""></n>	Only logging	<default></default>
Policy Auditor	General	My Default	<n a=""></n>	Log-only	<default></default>



Product	Category	Policy	System Impact	Default Setting	Planned Setting
Agent 6.0.1					
Policy Auditor Agent 6.0.1	File Integrity Monitor	My Default	<n a=""></n>	Log-only	<default></default>
Rogue System Detection	General	My Default	<n a=""></n>	Exclude ePO server IP	<default></default>

Based on the analysis results, customize policy settings / actions prior to deploying policies to a client system.

#### 1.2.2.2 Step 2.2: Deploy McAfee Agent to ePO Server

For this exercise, deployed the agent to the ePO Server but did \*not\* apply policy. We need to verify correct operations without firewall policies to prove that the software is in place and that an agent can connect. For the ePO Server, installed the framepkg.exe application manually as detailed in Step 2.2.2.

#### **1.2.2.3** Step 2.3: Import Client Computers

The first step of the importation is to create an appropriate system tree organization within the ePO Server. To match the VM ware vSphere setup, the same tree organization was used:

- [ENCLAVE]
  - Client Agents
    - [Mgmt]
      - NonVMware
        - o DBMS
        - o Infrastructure
        - o Services
        - o Tools
        - UserBoxes
        - o Web Access
      - VMware

Consider the following screenshot comparing the vSphere and ePO setup:







This ensures that, at any level within the hierarchy, specialized policies can be applied. For example, the database servers may need different settings than other servers. Where necessary, additional subgroups can be created within the ePO server; for example, if the NTP server may require different HBSS policy settings than other Infrastructure servers.

After analyzing the impact of the possible agent policies, the first targeted client (the cloud.army.mil Web frontend 172.24.4.29), imported the VM into the ePO UI console manually. This completed successfully and other servers were imported where they could be left to run for 72 hours to ensure that no critical services broke due to HBSS: CALOCAL001CA (local Windows Certificate Authority); CLOUDAD002CD (secondary DNS and Active Directory domain controller); RETINAX001UT (Retina server); and, WSUSXXX001CW (Windows Server Update



Services).

#### 1.2.2.4 Step 2.3: Deploy McAfee Agent to Client Computers

Still on the targeted first client 172.24.4.29, used the auto-deploy feature from ePO Server UI console successfully. Verified that the McAfee Agent pushed successfully:

CAMWFEX001W1 on eschost011	hb.armycloud.cloud.army.mil			_ 🗆 🗙					
<u>F</u> ile Vie <u>w</u> <u>V</u> M									
II > 6 2 24	10 🐶 🐶								
👼 Control Panel\All Control Panel	Items\Programs and Features			- 🗆 🗵					
🌀 🕕 🕫 🔹 Control Panel 🔹 All Control Panel Items 🔹 Programs and Features 🔹 🚱 Search Programs and Features 👂									
Control Panel Home	Uninstall or change a program								
View installed updates	To uninstall a program, select it from the list and the	en click Uninstall, Change,	or Repair.						
😲 Turn Windows features on or off				-					
Install a program from the network	Organize 🔻 Uninstall		i=	= 🔻 🚷					
	Name 🔺 🚽	Publisher	▼ Install ▼	Size 🔹					
	7-Zip 9.20 (x64 edition)	Igor Pavlov	10/5/2012	4.53 MB					
	🖉 ActivClient CAC x64	ActivIdentity	10/4/2012	43.4 MB					
	WMcAfee Agent	McAfee, Inc.	7/11/2013	25.1 MB					
	Microsoft Visual C++ 2008 Redistributable - x64 9	Microsoft Corporation	10/5/2012	788 KB					
	Microsoft Visual C++ 2008 Redistributable - x64 9	Microsoft Corporation	10/5/2012	788 KB					
	Microsoft Visual C++ 2008 Redistributable - x86 9	Microsoft Corporation	10/5/2012	596 KB					
	Microsoft Visual C++ 2008 Redistributable - x86 9	Microsoft Corporation	10/5/2012	600 KB					
	E PHP 5.3.26	The PHP Group	6/20/2013	71.6 MB					
	🔘 Symantec Endpoint Protection	Symantec Corporation	7/5/2013	634 MB					
	🔂 Tumbleweed Desktop Validator	Tumbleweed	10/4/2012	20.9 MB					
	💷 Vim 7.3 (self-installing)		6/19/2013						
	VMware Tools	VMware, Inc.	6/4/2013	52.7 MB					
	McAfee, Inc. Product version: 4.6.0.31 Help link: https://m	22 1ysupport.mcafee.com		Þ					

Additional agents must be deployed very carefully based on the gathered information and the expected policy impact to the services provided by the target client. More information will be covered after the DISA Guide is complete; continue to the next section.

Notes on additional systems deployed:

- SEPMXXX001MV (Symantec Endpoint Protection Manager) The SEPM service stopped after the HBSS agent deployed. Restarting the service brought the system back up.
- CLOUDAD001CD (primary AD controller) Unable to connect to AD controller after McAfee agent installed; rebooting the system repaired.



• Non-domain computers: When deploying, put a "." as the domain name and a local administrator (such as local Retina scanner account). Shot below:

ePolicy Orchestrator 4.6.6 (Build: 176	) - Windows Internet Explorer					
🕞 🕘 🗢 👿 https://hbssepo002mv	🔎 😴 Certificate error 🤄 🔯 ePolicy Orchestrator 4.6.6 ( 🗙					
Server: HBSSEPO002MV   Time: 8/12,	/13 3:01:44 PM EDT   User: admin   <u>Log Off</u>					
Menu System Tree	Dashboards System Tree Queries & Reports Policy Catalog					
Deploy McAfee Agent						
Target systems:	camccxx010vm, camoutx020vd, camoutx040vq, camoutx050vp					
Agent version:	Windows McAfee Agent for Windows 4.6.0 (Current)     Non-Windows McAfee Agent for AIX 4.6.0 (Current)					
Installation options:	<ul> <li>Install only on systems that do not already have an agent managed by this ePC</li> <li>Force installation over existing version</li> </ul>					
Installation path:	<program_files_dir>\McAfee\Common Framework  Program Files  McAfee\Common Framework</program_files_dir>					
Credentials for agent installation:	Domain: User name: Password: Confirm password: Remember my credentials for future deployments!					

After installing to various test systems in "log-only" mode (no enforcement), deployed to \*all\* systems as shown below:



Server: HBSSEP0002MV   Time: 8/15/13 1:32:25 PM EDT   User: admin   Log Off							
Menu V System Tree			Dashboards System	Tree Queries & Rep	ports Policy Catalog		
System Tree	Sys	items	Assigned Policies	Assigned Client Tas	ks Group Details		
✓ My Organization		esetu his Gri	oup Only	Custom: None	•		
▼ Client Agents			System Name 🔺	Managed State	Tags		
<b>▼</b> Mgmt	11		CALOCAL001CA	Managed	Server		
▼ NonVMware	11		CLOUDAD001CD	Managed	Server		
DBMS	11		CLOUDAD002CD	Managed	Server		
Infrastructure	11		DATACOR002SC	Managed	Server		
Services			DNSDHCP002RT	Managed	Server		
Tools	11		KIOSKDS001UT	Managed	Workstation		
UserBoxes	H		NASSRVR001SX	Managed	Server		
Web Access	11		NASSRVR002SX	Managed	Server		
VMware	H		NFSSRVR001SN	Managed	Server		
Resource	8		NFSSRVR003SN	Managed	Server		
			NFSSRVR005SN	Managed	Server		
ePO Server	11		RETINAX001UT	Managed	Server		
RSD	11		routerx001rx	Unmanaged	manage		
SADR	8		routerx002rx	Unmanaged	0.00		
▶ Lost&Found			SEPMXXX001MV	Managed	Server		
	11		WSUSXXX001CW	Managed	Server		

Note that the "software routers" (ROUTERX001RX and ROUTERX002RX) are unmanaged; this is by design as those routers are scheduled for eventual disposal to be replaced with hardware routers.

## **1.2.2.5** Step 2.5: Deploy SuperAgent Distributed Repository (SADR)

The SADR is not used in our target environment environment. Continue to the next section.

### 1.2.2.6 Step 2.6: Deploy Rogue System Detection (RSD) Sensor

Each monitored subnet must have the Rogue System Detection (RSD) Sensor installed to at least system on that subnet (DISA Guide recommends installation to \*two\* systems per subnet). As part of the [ENCLAVE] deployment the following agents are created to cover each listed subnet:

Subnet	Agent 1	Agent 2	Notes
172.20.0.0/17	RDGTWYX001RG	<n a=""></n>	Remote Desktop Gateway is only system on this subnet



172.24.1.0/24	KIOSKDS001UT	NFSSRVR003SN	Kiosk and smaller NFS server physical boxes chosen
172.28.4.0/24	<n a=""></n>	<n a=""></n>	This is a storage-only network; instruct ePO to ignore
172.24.0.0/24	NASSRVR002SX	<n a=""></n>	This is only server on this subnet (legacy untagged)
172.24.12.0/22	CAMOUTX020VD	OUTSSVC001VX	cloud.army.mil environments (dev and OutSystems tools)
172.24.4.0/22	CALOCAL001CA	MGSRVR003UX	Two lesser-used systems at random on this subnet
172.26.4.0/22	<n a=""></n>	<n a=""></n>	This is a storage-only network; instruct ePO to ignore

Note that within your own environment, the key is to identify which systems will serve as RSD sensors and to \*document\* these systems. The RSD sensor agents will have customized HBSS policies assigned to them.

The install process is exactly as described in DISA guide. Recommended to login to each selected system and verify the install – issue a "Wake Up Agents" command from the ePolicy Orchestrator UI to force the systems. The result of a successful RSD install is below (log file on installed RSD agent):

im r	ssenso	r_RDGT	WYX001	IRG.log	= (C:\Pro	gram Files (x86)\M	IcAfee\RSD Se	nsor\logs) - GVIM
File	Edit	Tools S	yntax E	Buffers	Window H	Help		
9		18	96	1 1 %	ē (	🚯 🗞 🛃 👌	1 & t	`∰ ⊂=   ? ß
75	2013	3/08/1	5 13:4	44:28	: I	#03140	asdk	Getting message from message queue
76	2013	3/08/1	5 13:4	44:28:	: I	#03140	asdk	Received reverse connect notification
77	2013	3/08/1	5 13:4	44:28:	: I	#03140	asdk	Getting message from message queue
78	2013	3/08/1	5 13:4	44:28:	: I	#02784	elect	Adding the multicast certificate to the RSD
79	2013	3/08/1	5 13:4	44:49:	: I	#02752	listener	Received a packet from: 00:50:56:86:00:df.
80	2013	3/08/1	5 13:4	44:49:	: I	#02752	listener	Queueing Host: 172.20.4.64
81	2013	8/08/1	5 13:4	44:49:	: I	#02752	listener	Adding 00:50:56:86:00:df to resolver queue.
82	2013	8/08/1	5 13:4	44:49:	: I	#02752	listener	Received a packet from: 00:50:56:86:00:df.
83	2013	3/08/1	5 13:4	44:49:	: I	#02364	resolver	Starting to process a host
84	2013	3/08/1	5 13:4	44:50:	: I	#02752	listener	Received a packet from: 00:50:56:86:00:df.
85	2013	3/08/1	5 13:4	44:50:	: I	#02752	listener	Received a packet from: 00:50:56:86:00:df.
86	2013	8/08/1	5 13:4	44:52	: I	#02752	listener	Received a packet from: 00:50:56:86:00:df.

From the ePO UI, the results should be similar to the following:



Server: HBSSEP	0002MV   Time: 8/15/13	2:32:33 PM EDT   Us	er: admin   <u>Log Of</u>			
Menu	Detected Syste	ems Dashboard	s System Tree	Queries & Reports	Policy Catalog	
Subnet Status			Overall System	n Status		
Covered !	Subnets: 100%		Compliar	nt Systems: 1	100%	
	1		Managed			32
5	0	0	Rogue			0
Covered	Contain Roques	Uncovered	Exceptions			7
			Inactive			0
	<u>2 Iqn</u>	ored Add Subnet		I	mport/Export Excep	tions

Note that some systems such as Software Routers will be explicitly marked as "exceptions" and unmanaged. Otherwise these systems are detected as "rogues" with a correspondingly lower Compliant System count.

Finally, manually move the installed RSD systems to the "RSD" folder within the System Tree...this ensures that only the correct policies get applied to these systems (more relaxed than standard policies):

System Tree VMy Organization V		Sys	tems	Assigned Policies	Assigned Client	Tasks Group De
		Pr	eset:	and Oak	Cus	tom:
			nis Gr	oup Only	Nic	ne
Client Agents				System Name 🔺	Managed State	Tags
ePO Server		Ш		CALOCAL001CA	Managed	Server
RSD				CAMOUTX020VD	Managed	Server
SADR				KIOSKDS001UT	Managed	Workstation
► Lost&Found		1		MGTSRVR003UX	Managed	Server
		1		NASSRVR002SX	Managed	Server
		H		NFSSRVR003SN	Managed	Server
	1916			OUTSSVC001VX	Managed	Server
	10.00	H		RDGTWYX001RG	Managed	Server

Continue to the next section.

### 1.2.2.7 Step 3.1: Global Updating

Follow DISA Guide.

#### 1.2.2.8 Step 3.2: McAfee Agent Product Update

Remember to use prefix "[ENCLAVE] – " for the "Product Update Pulls" task. Selected these patches / service packs:

• MER for ePO 2.5.3.0



- Host Intrustion Prevention 8.8.0
- Host Intrusion Prevention 8.0.0
- Audit Engine Content 1111
- Findings Content 1086

Assigned to top-level [ENCLAVE] subgroup; created schedule to run at 8:30pm each day on all managed systems (local time):

My Organization>	When do you want this task to run?
Schedule status:	<ul> <li>Enabled</li> <li>Disabled</li> </ul>
Schedule type:	Daily V Every 1 Days
Effective period:	Start date: 08 / 15 / 2013
Start time:	8 💽 : 30 💽 PM 💟 Run once at that time Run at that time, and then repeat until:

Continue to next section.

#### **1.2.2.9** Step 3.3: Daily Incremental Repository Replication Scheduled Task

Selected each day (Sun-Fri only) at 9pm not to interfere with WSUS.

#### **1.2.2.10** Step 3.4: Weekly Full Repository Replication Scheduled Task

Selected 9pm on Saturday not to interfere with WSUS.

### 1.2.2.11 Step 3.5: Deploy Asset and HIPS Modules

For this step, deploy only Asset Baseline Monitor (ABM) 3.5.1.0 (as of 15 AUG 13). Apploy to the top [ENCLAVE] subgroup:



Server: HBSSEPO002MV   Time: 8/15/13 3:19:36 PM EDT   User: admin   Log Off							
Menu 7 System Tree	Dashboards System Tree Queries & Reports						
Client Task Assignment Builder	1 Select Task 2. Sche						
My Organization>	we" to add the client task.						
Name:	- ABM Deployment						
Description:	No description available						
Туре:	McAfee Agent > McAfee Agent: Product Deployment						
Schedule:	Status: Enabled Type: Run immediately						
Lock task inheritance:	No						
Tags:	Send this task to all computers						

After a successful deployment, you should see both McAfee Agent and McAfee Asset Baseline Monitor Agent as below:

Control Panel Home

#### Uninstall or change a program

To uninstall a program, select it from the list and then click Uninstall, Change, or Repair.

- View installed updates <sup>†</sup> Turn Windows features on or off
- Install a program from the netwo

rk	Organize + Uninstali								
	Name 🔺	-	Publisher	•	Install	-	Size	•	Version
	💷 7-Zip 9.20 (x64 edition)		Igor Pavlov		10/5/2012		4.53 M	В	9.20.00.0
	ActivClient CAC x64		ActivIdentity		10/4/2012		43.4 M	B	6.2
	4 Adobe AIR		Adobe Systems Incorporated		7/3/2013				3.7.0.2090
	Adobe Connect 9 Add-in		Adobe Systems Incorporated		3/8/2013				11,2,251,0
	Adobe Flash Player 11 ActiveX		Adobe Systems Incorporated		7/30/2013		6.00 M	В	11.8.800.94
	🖊 Adobe Flash Player 11 Plugin		Adobe Systems Incorporated		7/30/2013		6.00 M	B	11.8.800.94
	🝌 Adobe Reader XI (11.0.03)		Adobe Systems Incorporated		5/29/2013		127 M	B	11.0.03
	FrontMotion Firefox Community Edition (en-US)		FrontMotion		8/15/2013		74.2 M	B	23.0.0.0
	💿 Google Chrome		Google Inc.		10/5/2012				28.0.1500.95
	😽 GoToMeeting 5.4.0.1082		CitrixOnline		4/23/2013				5.4.0.1082
	🕌 Java 7 Update 25		Orade		6/26/2013		130 M	B	7.0.250
	WMcAfee Agent		McAfee, Inc.		8/12/2013		25.1 M	В	4.6.0.3122
	McAfee Asset Baseline Monitor Agent		McAfee, Inc.		8/15/2013		2.17 M	в	3.5.0.250
	The second secon							-	

Continue to the next section.

## 1.2.2.12 Step 3.6: Configure ePO Daily Inactive Agent Task

For this task, the only thing different is that a new subgroup named "Inactive Agents" was added to the System Tree and the action for a detected inactive agent is to move that system to the "Inactive Agents" subgroup as shown below:

```
HBSS Notes 2 of 2 - Configure ePO Server.docx.doc
```



Server: HBSSEPO	002MV   Time: 8/15/13 3	3:04:07 PM EDT   User:	admin   <u>Log Off</u>	
Menu v		Dashboards	System Tree	Quenes & Reports P
Server Task Bui	lder	1 Description	$\rightarrow$	2 Actions
What actions do y	you want the task to take	e?		
▼ 1. Actions:	Run Query		~	
Query: Language: Sub-Acti	Managed Inactive Ag English ons: Move Systems			
System 7	Tree group: My Organ	ization\	nactive Agents	Browse
When th	ese systems are move	d to the new location	:	
Disal	ble System Tree sorting (	on these systems		
O Enab	le System Tree sorting o	on these systems		
O Do n	ot change the System Tr	ree sorting status for an	y of these system	15

Other than that, follow the DISA Guide.

#### 1.2.2.13 Module 4: Import Queries/Create Custom Dashboard

Skipping this as of 15 AUG 13. Custom dashboards are beyond the scope of this article.

## 1.2.2.14 Module 5: Change User Credentials

Modified these instructions slightly to match our target environment's standards. Note that these instructions are specific to the DISA pre-built image...if using the manual HBSS build then the user names are already set as documented above.

1. Created a local user account for Retina scanner and added to DBA local group:



л ов	A		
<u></u>			
Description:			
Mambars .			
	4		
Adminis	trator		
Adminis	trator		
Adminis	trator		
xAdminis	trator		

- Renamed "napoleon" account (default Administrator account as shipped by DISA pre-built image) to "xAdministrator" and set password to strong [ENCLAVE] admin password. Then disabled account as per Windows STIG.
- 3. Instructions for the "eposql2" account are not correct. Here are the specific steps:
  - a. Step 5.1.35: Do \*not\* enforce password policy on the eposql2 account at this time.
  - Step 5.1.34 (typo): There is typo in DISA guide; this step number is repeated. For the instructions to restart "McAfee ePolicy Orchestrator 4.6.6 Server" service, be aware that this can take around 10 minutes \*and\* this service automatically starts the "McAfee ePolicy Orchestrator 4.6.6 Application Server" service.
  - c. Step 5.1.35 (*typo*): As with 5.1.34 above, this step number is a typo in DISA guide. The instruction to restart the "McAfee ePolicy Orchestrator 4.6.6 Event Parser" will *fail*. The service will fail to start...if you look in Application event log you will see "Login failed for user 'eposql2'" which makes perfect sense because you just changed this SQL account's password above.
  - d. Step 5.1.43: This step has you test the "eposql2" account settings. Be aware that the SQL account will probably be locked out at this point (due to the failure of the McAfee Event Parser service to start). Go into SQL Server Management Studio and unlock eposql2 account if necessary. Then verify that the "Test Connection" function from "https://localhost:8005/core/config" screen works. (After you verify correct operations, go back to SQL Server Management Studio and set the Enforce



Password Policy and Enforce Password Expiration.) Please note that to view the "Apply" button in Internet Explorer for the "Test Connection" function, you must maximize the IE browser window:

Configure Database Settings - Windo	ws internet support	alEI.
Contraction (10) (attack acceleration)	Anny D 1 Certificate 21 77 S Configure Database Settings X	0.0.2
Configure Detabase Settings		
Host same or IP address:	HBSSEP0002MV	
Database server instancer	C1	
Betabase server port:	[2453	
Database name:	#PO4_HB552K8-FOC	
SSL communication with database server	Tity to one 55.	
User name:	sposg2	
User domain:		
Uver paseword:	Charge pasavord: Uner pathword: Cardier pasavord:	
Test Convertion   The database convertion	an sean bedand, successfully.	Maximize window to view this batton
		Renty

- 4. Created a local ePO User account and added to "ePO User Group" local group. Set never to expire (this account is mapped to the "epoadmin" ePO account created below).
- Changed Web browser login account from "admin" to "epoadmin". Within the ePO user properties, assigned this account to use your standard administrator notification password as the email address. Mapped the account to the Windows ePO User account created above.
- 6. Be sure to update \*all\* HIPS 8.0:General (Client UI) policies with the new "Administrator password to unlock the UI" specified in step 5.1.63 (not just the specific policy created for our target environment).



Host Intrusion Pr	revention 8.0:General	> Client UI (Wind	ows) > My Default	
General Settings	Advanced Options	Troubleshooting		
Advanced option	5:	Product integr	ity check enabled on of client rules (for all featur	es) enabled
Administrator pa the UI:	ssword to unlock	Password: Confirm password		<u></u>
Client UI langua	ge se <mark>tting:</mark>	Automatic		Update with modified epoadmin password
Disabling feature	25:	Allow disabling	of features from the tray ico Override IPS at policy enfor Override Firewall at policy e	n (remember mapped to Windows account enforcement
- 1 1		-		

After issuing the Agent Wakeup, **strongly recommend to reboot HBSS server** and verify that all services restart \*and\* that deployed agents are still valid.

#### 1.2.2.15 Module 6: PKI Installation and User Migration

Skipping this module for our target environment.

### **1.2.2.16** Module 7: Configure SSL Console Certificate (Section 7.1)

This section is incomplete in DISA Guide. For Section 7.1 ("Generate and Submit Server Certificate Request") there are no instructions from DISA Patch Repository. Please be aware that normally one would issue a request to and receive a signed server certificate from your DoD certificate authority. For the example below we are using a local certificate authority. However, most steps remain the same.

Follow these steps:

- 1. Add entry in local DNS for the validated enclave-specific fully-qualified domain name (FQDN); such as "foo.army.mil".
- 2. Create local certificate for the validated enclave-specific FQDN (note that for our target environment this certificate was already created during the HBSS Manual install in July 2013 same cert was used for the HBSS DISA Install in August 2013).
- 3. Open ePO Console.
- 4. Menu -> Configuration -> Server Settings -> Server Certificate. Then click "Edit" button as prompted.
- 5. Enter the location for the enclave-specific FQDN certificate and private key as created:



Edit Server Certificate					
Notes:	After applying the new certificate, ePolicy Orchestrator will need to be restarted in order for it to take effect.				
New certificate:	<ul> <li>Regenerate a self-signed certificate a</li> <li>Use the provided certificate and privat Certificate (PKCS7, PEM encoded, DER encoded, or PKCS52 file with</li> </ul>	nd private losy, te losy. Sc\OodSvatems\LocalCA	Browse		
	extension like .cercrt .pem, .der, .p12, .p7b):	Sector and a sector sector sector	biorradini		
	Certificate file passwords		This is for PKCS12 certificate file. This is for PKCS12 certificate file.		
	Certificate alles name:		If not specified, the first certificate will be used.		
	Private key (PEH):	S:\OutSystems\LocalCA	Browse		
	Drivate key password)	•••••			

- 6. Reboot HBSS server (just as fast as waiting for ePO Services to restart).
- 7. Update ePO UI console shortcut to reference the enclave-specific FQDN instead of the ePO server hostname.



Server certificate is now updated.

### **1.2.2.17** Module 7: Configure SSL Console Certificate (Section 7.2)

The SQL Server certificate section is not necessary for our target environment as the DISA pre-built image ships with SQL Server 2008 already.



#### 1.2.2.18 Module 8: Deploy HIPs to ePO

Follow steps in DISA Guide.

The ePO Server is now fully configured. Continue to the next section.

#### 1.2.3 ePO Server Configuration: Final Steps

This section lists the steps performed after the DISA guides were used.

1. Enable Microsoft Updates. Turn off IE ESC from Server Manager, then from Windows Updates select the "Get updates for other Microsoft products. *Find out more*".

oneror runer par contror runer reems p	muowstopuute		
🔾 🗢 🚰 🔸 Control Panel 🔸 All Control	Panel Items 👻 Windows Update	¥ 😽	Search Control Panel
Control Panel Home	Windows Update		
Check for updates			
Change settings	Checking for up	dates	
View update history			
Restore hidden updates			
Updates: frequently asked questions	1.4		
	Most recent check for updates:	Today at 9:09 AM	
	Updates were installed:	Today at 8:56 AM (Failed).	View update history
	You receive updates:	Managed by your system a	dministrator
	(	You checked online fo	r updates from Microsoft Update.
Microsoft Update is now enabled.		Check for updates manage	d by your system administrator

 Setup SMTP. Set SMTP server name to the enclave-specific mail server and the from address to a valid identifier (such as "foo@army.mil").

SMTP server name:	
SMTP server port:	25
Authentication:	Do not authenticate     Authenticate User name: Password: Confirm password:
From address:	x

3. Enable email notification for Automatic Responses. The ePO Server ships with a number of "Automatic Responses" (Menu -> Automation -> Automatic Responses). Duplicate each automatic response (with



prefix "[ENCLAVE] – " for the name). For each *email notification response* enable the response and set the email destination to the "ePO Administrator" account as shown below:

Contacts	
ePO Administrator <apg@belva0314sdsmtp1.escc.army.mil></apg@belva0314sdsmtp1.escc.army.mil>	

#### The final result should resemble:

Auto	Automatic Responses						
Pres	set: All Quick find:		Apply <u>Clear</u>	Show selected rows			
	Name 🔺	Status	Event Category	Event Type	Actions		
	- Distributed Repository Replication failed	Enabled	ePO Notification Events	Server	View   Edit   Duplicate		
	Malware detected and not handled	Enabled	ePO Notification Events	Threat	View   Edit   Duplicate		
	Master Repository Update failed	Enabled	ePO Notification Events	Server	View   Edit   Duplicate		
	Master Repository Update succeeded	Enabled	ePO Notification Events	Server	View   Edit   Duplicate		
	Non-compliant computer detected	Enabled	ePO Notification Events	Server	View   Edit   Duplicate		
	RSD: Query New Rogue Detection	Disabled	Detected System Evenu	System Detection	View   Edit   Duplicate		
	Software Manager new product update available	Enabled	ePO Notification Events	Server Enable the automa	View   Edit   Duplicate		
	Distributed Repository Replication failed	Disabled	ePO Notification Events	Server notifications that s	uppert Edit Duplicate		
	Malware detected and not handled	Disabled	ePO Notification Events	Threat email response	View   Edit   Duplicate		
	Master Repository Update failed	Disabled	ePO Notification Events	Server	View   Edit   Duplicate		
	Master Repository Update succeeded	Disabled	ePO Notification Events	Server	View   Edit   Duplicate		

Now you will receive at least one notification from your ePO Server each day, as well as upon any errors.

Other post-install configuration instructions provided as necessary in the future.