A WHITE PAPER

HBSS Install Notes
Part 2 of 2: Configure ePO Server

Topic Summary:

- 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 the Author ........................................................................................................... 2

1.2  Host-Based Security System (HBSS) ............................................................................ 2

1.2.1  DISA Documentation Sources .................................................................................. 2

1.2.2  ePO 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  ePO Server Configuration: Final Steps .................................................................... 22
## Version Control

### Change Activity Log

<table>
<thead>
<tr>
<th>Date</th>
<th>Version</th>
<th>Comments</th>
<th>Owner</th>
</tr>
</thead>
<tbody>
<tr>
<td>24 JUN 13</td>
<td>Draft A</td>
<td>Initial creation by extraction from “Tech Guide.docx”</td>
<td>Andrew Bruce</td>
</tr>
<tr>
<td>21 AUG 13</td>
<td>Draft A</td>
<td>Documentation on HBSS ePO Server, redacted from primary documents.</td>
<td>Andrew Bruce</td>
</tr>
</tbody>
</table>
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 https://www.softwareab.net/wordpress/?p=397) 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** ([http://www.disa.mil/Services/Information-Assurance/HBS/HBSS](http://www.disa.mil/Services/Information-Assurance/HBS/HBSS)) – Use this page to access HBSS news, documentation resources, the DISA Patch Repository, and more.

The specific DISA HBSS Guides from the 4.6 Patch Repository include:
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:

<table>
<thead>
<tr>
<th>Question</th>
<th>ePO Server</th>
<th>OUR TARGET ENVIRONMENT Client</th>
</tr>
</thead>
<tbody>
<tr>
<td>How many computers are designated to receive the McAfee Agent?</td>
<td>[n/a]</td>
<td>TBD</td>
</tr>
<tr>
<td>What is the Network security: LAN Manager Authentication level local security policy setting found on the proposed clients? (ePO server default is 5)</td>
<td>5</td>
<td>5 (Domain)</td>
</tr>
<tr>
<td>What is the Microsoft Network client: Digitally sign communications (always) local security policy setting found on</td>
<td>Enabled</td>
<td>Enabled (Local)</td>
</tr>
<tr>
<td>Question</td>
<td>Proposed Clients</td>
<td>ePO Server Default</td>
</tr>
<tr>
<td>------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>------------------</td>
<td>-------------------</td>
</tr>
<tr>
<td>What is the Microsoft Network server: Digitally sign communications (always) local security policy setting found on the proposed clients?</td>
<td>Enabled</td>
<td>Enabled (Local)</td>
</tr>
<tr>
<td>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)</td>
<td>Only two boxes; both checked</td>
<td>Only two boxes; both checked (Local)</td>
</tr>
<tr>
<td>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)</td>
<td>Only two boxes; both checked</td>
<td>Only two boxes; both checked (Local)</td>
</tr>
<tr>
<td>What is the System cryptography: Use FIPS compliant algorithms for encryption, hashing and signing local security policy setting found on the proposed clients?</td>
<td>Enabled</td>
<td>Enabled (Domain)</td>
</tr>
<tr>
<td>Do the proposed clients have file and print sharing enabled? (\My computer\Explore\Tools\Folder Options\View\Use Simple File Sharing)</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Do the proposed clients have remote registry access enabled (\My Computer\Manage\Services and Applications\Services\Remote Registry)?</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Do the proposed clients have the ADMIN$ share enabled?</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

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.)
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:

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

HBSS Notes 2 of 2 - Configure ePO Server.docx.doc
Not every Product is covered below; only those that apply to the D5-141 environment.

<table>
<thead>
<tr>
<th>Product</th>
<th>Category</th>
<th>Policy</th>
<th>System Impact</th>
<th>Default Setting</th>
<th>Planned Setting</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asset Baseline Monitor 3.5.1.0</td>
<td>Trusted Activity</td>
<td>McAfee Default</td>
<td>&lt;n/a&gt;</td>
<td>&lt;empty&gt;</td>
<td>&lt;default&gt;</td>
<td></td>
</tr>
<tr>
<td></td>
<td>File Permissions</td>
<td>My Default</td>
<td>&lt;n/a&gt;</td>
<td>&lt;empty&gt;</td>
<td>&lt;default&gt;</td>
<td></td>
</tr>
<tr>
<td>Asset Baseline Monitor 3.5.1.0</td>
<td>Registry Monitor</td>
<td>My Default</td>
<td>&lt;n/a&gt;</td>
<td>&lt;empty&gt;</td>
<td>&lt;default&gt;</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Agent Configuration</td>
<td>McAfee Default</td>
<td>X</td>
<td>&lt;not enforced&gt;</td>
<td>&lt;not enforced&gt;</td>
<td></td>
</tr>
<tr>
<td>Data Loss Prevention 9.2.0.0: Policies</td>
<td>Computers Assignment Group</td>
<td>My Default</td>
<td>&lt;n/a&gt;</td>
<td>&lt;empty&gt;</td>
<td>&lt;default&gt;</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Firewall Options (Windows)</td>
<td>McAfee Default</td>
<td>X</td>
<td>&lt;not enabled&gt;</td>
<td>&lt;not enforced&gt;</td>
<td></td>
</tr>
<tr>
<td>HIPS 8.0: Firewall</td>
<td>DNS Blocking (Windows)</td>
<td>My Default</td>
<td>X</td>
<td>&lt;empty&gt;</td>
<td>&lt;default&gt;</td>
<td></td>
</tr>
<tr>
<td>HIPS 8.0: Firewall</td>
<td>Firewall Rules (Windows)</td>
<td>My Default</td>
<td>X</td>
<td>PING, iSCSI, and other protocols blocked</td>
<td>&lt;default&gt; (because firewall options default to not enabled)</td>
<td></td>
</tr>
<tr>
<td>HIPS 8.0: General</td>
<td>Client UI (Windows)</td>
<td>[ENCLAVE] – HIPS Client UI</td>
<td>&lt;n/a&gt;</td>
<td>Standard logging rules</td>
<td>&lt;default&gt;</td>
<td></td>
</tr>
<tr>
<td>HIPS 8.0:</td>
<td>Trusted</td>
<td>[ENCLAVE]</td>
<td>&lt;n/a&gt;</td>
<td>Retina</td>
<td>&lt;default&gt;</td>
<td></td>
</tr>
<tr>
<td>Product</td>
<td>Category</td>
<td>Policy</td>
<td>System Impact</td>
<td>Default Setting</td>
<td>Planned Setting</td>
<td></td>
</tr>
<tr>
<td>---------------</td>
<td>----------------------</td>
<td>---------------------------------------------</td>
<td>---------------</td>
<td>---------------------</td>
<td>----------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>General</td>
<td>Networks (Windows)</td>
<td>– All Trusted Networks</td>
<td></td>
<td>server specified</td>
<td></td>
<td></td>
</tr>
<tr>
<td>HIPS 8.0:</td>
<td>Trusted Applications (All Platforms)</td>
<td>[ENCLAVE] – Client Trusted Applications</td>
<td>&lt;n/a&gt;</td>
<td>DISA-specified</td>
<td>&lt;default&gt;</td>
<td></td>
</tr>
<tr>
<td>General</td>
<td>IPS Options (All Platforms)</td>
<td>[ENCLAVE] – HIPS IPS Options</td>
<td>X</td>
<td>Enabled</td>
<td>&lt;default&gt; (leave as enabled as IPS protection can be modified to log-only)</td>
<td></td>
</tr>
<tr>
<td>HIPS 8.0:</td>
<td>IPS Protection (All Platforms)</td>
<td>[ENCLAVE] – HIPS IPS Protection</td>
<td></td>
<td></td>
<td>“High” severity can initiate actions Modify so that all severity are asset to “Log”:</td>
<td></td>
</tr>
<tr>
<td>LinuxShield</td>
<td>On-Access Scanning</td>
<td>McAfee Default</td>
<td>X</td>
<td>Signature-based</td>
<td>&lt;default&gt;</td>
<td></td>
</tr>
<tr>
<td>McAfee Agent</td>
<td>General</td>
<td>My Default</td>
<td>&lt;n/a&gt;</td>
<td>Push to agent</td>
<td>&lt;default&gt; (does not look like the agent by itself can break any system functionality)</td>
<td></td>
</tr>
<tr>
<td>McAfee Agent</td>
<td>Repository</td>
<td>My Default</td>
<td>&lt;n/a&gt;</td>
<td>Only logging</td>
<td>&lt;default&gt;</td>
<td></td>
</tr>
<tr>
<td>McAfee Agent</td>
<td>Troubleshooting</td>
<td>My Default</td>
<td>&lt;n/a&gt;</td>
<td></td>
<td>&lt;default&gt;</td>
<td></td>
</tr>
<tr>
<td>Policy Auditor</td>
<td>General</td>
<td>My Default</td>
<td>&lt;n/a&gt;</td>
<td>Log-only</td>
<td>&lt;default&gt;</td>
<td></td>
</tr>
<tr>
<td>Product</td>
<td>Category</td>
<td>Policy</td>
<td>System Impact</td>
<td>Default Setting</td>
<td>Planned Setting</td>
<td></td>
</tr>
<tr>
<td>--------------------------</td>
<td>----------------</td>
<td>--------------</td>
<td>---------------</td>
<td>----------------</td>
<td>-----------------</td>
<td></td>
</tr>
<tr>
<td>Agent 6.0.1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Policy Auditor Agent 6.0.1</td>
<td></td>
<td>My Default</td>
<td>&lt;n/a&gt;</td>
<td>Log-only</td>
<td>&lt;default&gt;</td>
<td></td>
</tr>
<tr>
<td>Rogue System Detection</td>
<td>General</td>
<td>My Default</td>
<td>&lt;n/a&gt;</td>
<td>Exclude ePO server IP</td>
<td>&lt;default&gt;</td>
<td></td>
</tr>
</tbody>
</table>

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 VMware vSphere setup, the same tree organization was used:

- [ENCLAVE]
  - Client Agents
    - [Mgmt]
    - NonVMware
      - DBMS
      - Infrastructure
      - Services
      - Tools
      - UserBoxes
      - 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: CALLOCAL001CA (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:

![Image of Control Panel](image.png)

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:

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

<table>
<thead>
<tr>
<th>Subnet</th>
<th>Agent 1</th>
<th>Agent 2</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>172.20.0.0/17</td>
<td>RDGTWYX001RG</td>
<td>&lt;n/a&gt;</td>
<td>Remote Desktop Gateway is only system on this subnet</td>
</tr>
</tbody>
</table>
### HBSS Notes Part 2 of 2 – ePO Server Configuration

<table>
<thead>
<tr>
<th>Address Range</th>
<th>System 1</th>
<th>System 2</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>172.24.1.0/24</td>
<td>KIOSKDS001UT</td>
<td>NFSSRVR002SN</td>
<td>Kiosk and smaller NFS server physical boxes chosen</td>
</tr>
<tr>
<td>172.28.4.0/24</td>
<td>&lt;n/a&gt;</td>
<td>&lt;n/a&gt;</td>
<td>This is a storage-only network; instruct ePO to ignore</td>
</tr>
<tr>
<td>172.24.0.0/24</td>
<td>NASSRVR002SX</td>
<td>&lt;n/a&gt;</td>
<td>This is only server on this subnet (legacy untagged)</td>
</tr>
<tr>
<td>172.24.12.0/22</td>
<td>CAMOUTX020VD</td>
<td>OUTSSVC001VX</td>
<td>Cloud.army.mil environments (dev and OutSystems tools)</td>
</tr>
<tr>
<td>172.24.4.0/22</td>
<td>CALOCAL001CA</td>
<td>MGSRVRO03UX</td>
<td>Two lesser-used systems at random on this subnet</td>
</tr>
<tr>
<td>172.26.4.0/22</td>
<td>&lt;n/a&gt;</td>
<td>&lt;n/a&gt;</td>
<td>This is a storage-only network; instruct ePO to ignore</td>
</tr>
</tbody>
</table>

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):

```
75 2013/08/15 13:44:20: 1 000140 asdk  Getting message from message queue
76 2013/08/15 13:44:20: 1 000140 asdk  Received reverse connect notification
77 2013/08/15 13:44:20: 1 000140 asdk  Received message from message queue
78 2013/08/15 13:44:20: 1 002704 agent  Adding the multicast certificate to the RSD
79 2013/08/15 13:44:20: 1 002752 listener  Received a packet from 00:50:56:06:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:}
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):

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 Intrusion 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):

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). Deploy to the top [ENCLAVE] subgroup:
After a successful deployment, you should see both McAfee Agent and McAfee Asset Baseline Monitor Agent as below:

![Client Task Assignment Builder](image)

*Control Panel Home*

*View installed updates*

1. Turn Windows features on or off
2. Install a program from the network

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:
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:
2. 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.
   b. 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” service 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 Enf
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).

5. 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).
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.
5. Enter the location for the enclave-specific FQDN certificate and private key as created:
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”.

2. **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”).

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:

The final result should resemble:

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.