

## Pre-install checklist for TrendMicro DeepSecurity 8.0 POC

- Use this checklist to ensure the environment is ready for a Proof of Concept.
- Double click each checkbox indicating the item is ready.
- Return this document to your Trend Micro sales representative

### VMware Requirements

Minimum two ESXi 5.0 or 4.1 hosts	<input type="checkbox"/>
ESXi 5.0 patch 1 <a href="http://kb.vmware.com/kb/1027808">http://kb.vmware.com/kb/1027808</a> <sup>1 (see page 2)</sup>	<input type="checkbox"/>
ESXi 4.1 patch 3 <a href="http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&amp;cmd=displayKC&amp;externalId=2019860">http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&amp;cmd=displayKC&amp;externalId=2019860</a>	<input type="checkbox"/>
VMware vCenter 5.0	<input type="checkbox"/>
VMware VShield Manager 5.0 or 5.0.1	<input type="checkbox"/>
One ESX host must be put into maintenance mode during the vShield kernel module installation. (VMs on this host will either have to be suspended or vMotioned to another ESXi host)	<input type="checkbox"/>

### Guest Virtual Machines Requirements

VMware Tools 5.0 with vShield driver installed <sup>2 (see page 2)</sup>	<input type="checkbox"/>
Virtual disks: LSI Logic parallel, LSI SAS or VMware paravirtual SCSI driver (Buslogic <i>not</i> supported)	<input type="checkbox"/>
Windows2003 or 2008 server; Windows XP or Windows7	<input type="checkbox"/>

### DeepSecurity Manager Requirements- Physical Server or Virtual Machine

Windows2003 SP2 or Windows2008 server	<input type="checkbox"/>
DeepSecurity software - <a href="http://downloadcenter.trendmicro.com/">http://downloadcenter.trendmicro.com/</a>	<input type="checkbox"/>
TrendMicro Deep Security license key	<input type="checkbox"/>
Database- Microsoft SQL Server, SQL Server Express or Oracle 10g, 11i	<input type="checkbox"/>

### Firewall requirements (TCP protocol)

Source	Destination	Destination port	
Deep Security Manager	vCenter	443	<input type="checkbox"/>
Deep Security Manager	vShield Manager	443	<input type="checkbox"/>
Deep Security Manager	ESX host	4118, 4119	<input type="checkbox"/>
ESX host	Deep Security Manager	4120, 4119	<input type="checkbox"/>
Deep Security Virtual Appliance	vShield Manager	443	<input type="checkbox"/>
ESX host	vShield Manager	443	<input type="checkbox"/>
vShield Manager	vCenter	443	<input type="checkbox"/>
Deep Security Manager	Oracle Database Listener	1526	<input type="checkbox"/>
Deep Security Manager	Deep Security Agent	4118	<input type="checkbox"/>
Deep Security Agent	Deep Security Manager	4120	<input type="checkbox"/>
Deep Security Agent/Appliance	Deep Security Relay	4122	<input type="checkbox"/>
Desktop browser (console)	Deep Security Manager	4119	<input type="checkbox"/>

### Time synchronization requirements

System time in synchronized between all VMs, DeepSecurity Manager, VCenter and ESXi	<input type="checkbox"/>
---	--------------------------

### Optional - SMTP server, Windows Active Directory Server

SMTP server available for email notification	<input type="checkbox"/>
ActiveDirectory available for synchronizing users and target systems.	<input type="checkbox"/>

### Optional - firewall ports

Source	Destination	port	
Deep Security Manager	SMTP server	25	<input type="checkbox"/>
Deep Security Manager	Active Directory	389/636	<input type="checkbox"/>

### Login credentials requirements

VMware vCenter Administrator username/password <sup>3</sup>	<input type="checkbox"/>
VMware vShield Administrator username and password	
Windows Administrator username/password to enable installation of DeepSecurity Manager software.	<input type="checkbox"/>
Database: Microsoft SQLServer/Oracle user username/password (the DB user should have sufficient privileges to create a new tables and schema)	<input type="checkbox"/>
ActiveDirectory user with read-only privileges if synchronization is required with Active Directory.	<input type="checkbox"/>

3 - If administrator access is not possible, a special list of vCenter privileges can be provided by Trend Micro sales support

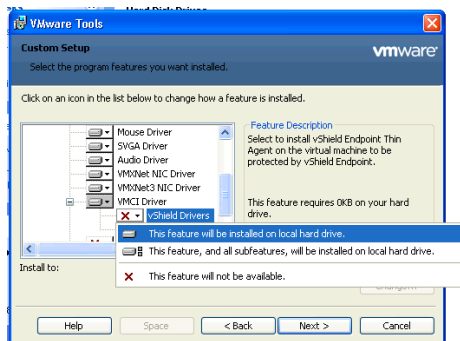
### Installing VMware vShield Endpoint Driver, included in VMTools 5.0, on Guest Virtual Machines

VMware vShield Endpoint Driver is included in the VMware Tools installation on a guest VM per this table:

VMTools Install option	vShield Endpoint	Action to take to install vShield Endpoint
Typical	vShield Endpoint is <b>not</b> installed	<b>Do not</b> select this option <sup>4</sup>
Complete	vShield Endpoint <b>is</b> installed	This option can be used
Custom	vShield Endpoint <b>must be explicitly</b> selected	<i>See details below</i>

4 - if VMTools was installed using the "Typical" option, re-run the installer and select custom to install vShield Endpoint.

When doing a custom install of VMware Tools 5, vShield Endpoint is **not** included by default. Therefore select "custom install" for a new install of VMTools or "interactive upgrade" for a reconfiguration of a prior "Typical" install and click on the red X and select "install to local drive".



### Applying vSphere 5.0 patch 1 (build 474610) to a single ESXi 5.0 host.

ESXi hosts can be updated using VMware Update Manager. To update a single host, download patch 1 by searching for build 474610 here: <http://www.vmware.com/patchmgr/download.portal>. Upload the ZIP file to the ESXi local datastore and install the patch using vCLI:

```
esxcli --server=<IP ADDRESS OF ESXi> --username=root software vib update --
depot=/vmfs/volumes/datastore1/ESXi500-201109001.zip
```