Installation Guide
Revision B

McAfee Advanced Threat Defense 4.2.0
COPYRIGHT
Copyright © 2017 McAfee, LLC

TRADEMARK ATTRIBUTIONS
McAfee and the McAfee logo, McAfee Active Protection, ePolicy Orchestrator, McAfee ePO, McAfee EMM, Foundstone, McAfee LiveSafe, McAfee QuickClean, Safe Eyes, McAfee SECURE, SecureOS, McAfee Shredder, SiteAdvisor, McAfee Stinger, True Key, TrustedSource, VirusScan are trademarks or registered trademarks of McAfee, LLC or its subsidiaries in the US and other countries. Other marks and brands may be claimed as the property of others.

LICENSE INFORMATION
License Agreement
NOTICE TO ALL USERS: CAREFULLY READ THE APPROPRIATE LEGAL AGREEMENT CORRESPONDING TO THE LICENSE YOU PURCHASED, WHICH SETS FORTH THE GENERAL TERMS AND CONDITIONS FOR THE USE OF THE LICENSED SOFTWARE. IF YOU DO NOT KNOW WHICH TYPE OF LICENSE YOU HAVE ACQUIRED, PLEASE CONSULT THE SALES AND OTHER RELATED LICENSE GRANT OR PURCHASE ORDER DOCUMENTS THAT ACCOMPANY YOUR SOFTWARE PACKAGING OR THAT YOU HAVE RECEIVED SEPARATELY AS PART OF THE PURCHASE (AS A BOOKLET, A FILE ON THE PRODUCT CD, OR A FILE AVAILABLE ON THE WEBSITE FROM WHICH YOU DOWNLOADED THE SOFTWARE PACKAGE). IF YOU DO NOT AGREE TO ALL OF THE TERMS SET FORTH IN THE AGREEMENT, DO NOT INSTALL THE SOFTWARE. IF APPLICABLE, YOU MAY RETURN THE PRODUCT TO MCAFEE OR THE PLACE OF PURCHASE FOR A FULL REFUND.
Contents

1 McAfee Advanced Threat Defense deployment options .......................... 7

2 Plan your deployment ........................................................................ 9
   Requirements ............................................................................ 9
   Web interface client requirements ............................................ 9
   Cluster requirements ............................................................... 10
   Analyzer VM requirements ....................................................... 11
   Hardware specifications ............................................................ 11
   System environmental limits ...................................................... 16
   Default ports used in Advanced Threat Defense communication ....... 18
   Warnings and cautions ............................................................... 20
   Deployment checklist ................................................................. 20

3 Installing the OS, software, and Email Connector ............................... 23
   Installer package details ............................................................. 24
   Install the OS to your appliance ................................................ 25
   Install the OS to your appliance remotely using RMM .................. 27
   Install the Advanced Threat Defense software ............................ 28
   Installing Virtual Advanced Threat Defense ................................. 28
   Install Virtual Advanced Threat Defense on ESXi server ............... 30
   Install Virtual Advanced Threat Defense on Hyper-V using the automated script ........ 31
   Install Virtual Advanced Threat Defense on Hyper-V manually ...... 32
   Deploy Virtual Advanced Threat Defense from Azure Marketplace .... 33
   Create an analyzer VM on Azure ................................................. 34
   Prepare your sandbox virtual machine ....................................... 35
   Activate the product .................................................................. 36
   Install Email Connector ............................................................. 38

4 Accessing the Advanced Threat Defense web interface ........................ 41
   McAfee Advanced Threat Defense client requirements .................. 41
   Log on to the Advanced Threat Defense web interface .................. 42

5 Manage users and performance ......................................................... 43
   Manage users ........................................................................... 43
   Add users ................................................................................. 43
   Types of users .......................................................................... 43
   Command-line Interface user .................................................... 44
   Super Administrator .................................................................. 44
   Network Security Platform user ................................................. 44
   Upload Administrator .................................................................. 44
   Web Gateway user .................................................................... 44
   Email Gateway user ................................................................... 44
   TIE user .................................................................................. 45
   Virtual Network Security Platform user ...................................... 45
6 Creating analyzer VMs

Create a VM using the VM Builder ........................................ 54
Create a virtual machine on VMWare ESXi ................................. 55
Create a virtual machine on Hyper-V Manager ............................. 56
Create a virtual disk file .......................................................... 58
  Create a virtual disk file for Windows 7 ................................ 58
  Create a virtual disk file for Windows 8 ................................ 59
  Create a virtual disk file for Windows XP ................................ 60
  Create a virtual disk file for Windows Server 2003 ...................... 60
  Create a virtual disk file for Windows Server 2008 ...................... 61
  Create a virtual disk file for Windows 8.1 ................................. 62
  Create a virtual disk file for Windows 10 ................................. 63
  Create a virtual disk file for Windows 10 version 1703 (Redstone 2) 63
  Create a virtual disk file for Windows 2012 ............................... 64
  Create a virtual disk file for Windows 2012 R2 ........................... 65
  Create a virtual disk file for Windows Server 2016 Standard ........ 65
Install Microsoft Office on the virtual machine ............................ 66
Enable PDF file analysis .......................................................... 66
Enable JAR file analysis .......................................................... 66
Enable Flash file analysis ........................................................ 67
Complete the VMDK and VHDX file creation process ....................... 67
Prepare the virtual disk image for analysis .................................. 67
  Run the VM Provisioner Tool ................................................. 67
  Prepare your VMDK or VHDX image for analysis manually .......... 68
Import the virtual disk file ...................................................... 96
Convert the VMDK and VHDX file to an image file ......................... 96
Managing VM profiles ............................................................. 97
  Create VM profiles ............................................................. 98

7 Configuring ATD for malware analysis .................................. 101
Configuring Advanced Threat Defense for malware analysis ............ 101
High-level steps to configure malware analysis ............................ 102
Configure the McAfee Virtual Advanced Threat Defense network information .......................................................... 102
Configure the security and performance options ............................ 103
Configure proxy servers for Internet connectivity .......................... 104
  Configure Advanced Threat Defense to communicate with McAfee GTI 104
Enable the malware site proxy .................................................. 104
Configure DNS setting ........................................................... 105
Configure the syslog settings .................................................... 105
Configuring the TAXII settings ................................................ 107
Enable and configure TAXII settings ........................................ 107
Configure the date and time ................................................... 109
Add the Advanced Threat Defense logon banner ................... 110
Configure telemetry ................................................................ 110
Enable telemetry .................................................................... 112
Configure Common Settings .................................................... 112
  Configure maximum threshold wait time .............................. 112
  Enable Common Criteria (CC) mode ...................................... 113
  Enable account lock out ...................................................... 114
Configuring Email Connector .................................................. 114
  Enable and configure Email Connector ................................. 114
  Configuring your Secure Email Gateway for Email Connector .... 116
  Configure Email Connector filtering rules ............................. 116
  Understanding Email Headers with analysis status ................. 117
Uploading certificates .............................................................. 118
  Upload trusted CA certificates ............................................. 119
  Upload web certificates ...................................................... 119

Index .................................................................................. 121
You can deploy McAfee Advanced Threat Defense in the following ways:

- **Standalone deployment** — This is a simple way of deploying McAfee Advanced Threat Defense. In this case, it is not integrated with other externally installed McAfee products. When deployed as a standalone Appliance, you can manually submit the suspicious files using the McAfee Advanced Threat Defense web application. Alternatively, you can submit the samples using an FTP client. This deployment option is used, for example, during the testing and evaluation phase, to fine-tune configuration, and to analyze suspicious files in an isolated network segment. Also, research engineers might use the standalone deployment option for detailed analysis of malware.

- **Integration with Network Security Platform** — This deployment involves integrating McAfee Advanced Threat Defense with Network Security Platform Sensor and Manager. Based on how you have configured the corresponding Advanced Malware policy, an inline Sensor detects a file download and sends a copy of the file to McAfee Advanced Threat Defense for analysis. If McAfee Advanced Threat Defense detects a malware within a few seconds, the Sensor can block the download. The Manager displays the results of the analysis from McAfee Advanced Threat Defense.

  If McAfee Advanced Threat Defense requires more time for analysis, the Sensor allows the file to be downloaded. If McAfee Advanced Threat Defense detects a malware after the file has been downloaded, it informs Network Security Platform, and you can use the Sensor to quarantine the host until it is cleaned and remediated. You can configure the Manager to update all the Sensors about this malicious file. Therefore, if that file is downloaded again anywhere in your network, your Sensors might be able to block it.

  For information on how to integrate Network Security Platform and McAfee Advanced Threat Defense, refer to the latest Network Security Platform Integration Guide.

- **Integration with McAfee® Web Gateway** — You can configure McAfee Advanced Threat Defense as an additional engine for anti-malware protection. When your network user downloads a file, the native McAfee Gateway Anti-malware Engine on McAfee® Web Gateway scans the file and determines a malware score. Based on this score and the file type, McAfee® Web Gateway sends a copy of the file to McAfee Advanced Threat Defense for deeper inspection and dynamic analysis. A progress page informs your users that the requested file is being analyzed for malware. Based on the malware severity level reported by McAfee Advanced Threat Defense, McAfee® Web Gateway determines if the file is allowed or blocked. If it is blocked, the reasons are displayed for your users. You can view the details of the malware that was detected in the log file.

  This design ensures that only those files that require an in-depth analysis are sent to McAfee Advanced Threat Defense. This balances your users’ experience in terms of download speed and security. For information on how to integrate McAfee Advanced Threat Defense and McAfee® Web Gateway, see the McAfee® Web Gateway Product Guide, version 7.4.
• Integration with McAfee® ePolicy Orchestrator (McAfee ePO) — This integration enables McAfee Advanced Threat Defense to retrieve information regarding the target host. Knowing the operating system on the target host, enables it to select a similar virtual environment for dynamic analysis.
  • Dynamic analysis requires the suspicious file to be executed for a specific time period. During this time, the malware is likely to have reached the intended target. You can then take the required remedial steps to clean the affected host.
  • This integration also enables you to identify the other hosts infected by the same malware and take the appropriate remedial steps.

How the deployment options address the four major aspects of anti-malware process cycle:

• Detection of file download: As soon as a user accesses a file, the inline Network Security Platform Sensor or McAfee® Web Gateway detects this and sends a copy of the file to McAfee Advanced Threat Defense for analysis.

• Analysis of the file for malware: Even before the user fully downloads the file, McAfee Advanced Threat Defense can detect a known malware using sources that are local to it or on the cloud.

• Block future downloads of the same file: Every time McAfee Advanced Threat Defense detects a medium, high, or very high severity malware, it updates its local black list.

• Identify and remediate affected hosts: Integration with Network Security Platform enables you to quarantine the host until it is cleaned up and remediated.
Plan your deployment

Before you install Advanced Threat Defense, verify that you have everything you need, and that your environment meets the minimum system requirements.

Contents
- Requirements
- Hardware specifications
- System environmental limits
- Default ports used in Advanced Threat Defense communication
- Warnings and cautions
- Deployment checklist

Requirements

To ensure that your deployment is successful, your environment must meet the minimum requirements.

Web interface client requirements

To log on to the Advanced Threat Defense web interface, make sure that your client meets the requirements.

Table 2-1  Supported operating systems

<table>
<thead>
<tr>
<th>Operating system</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft Windows</td>
<td>• 7 32-bit Service Pack 1</td>
</tr>
<tr>
<td></td>
<td>• 7 64-bit Service Pack 1</td>
</tr>
<tr>
<td></td>
<td>• 8 0 Professional 32-bit</td>
</tr>
<tr>
<td></td>
<td>• 8 0 Professional 64-bit</td>
</tr>
<tr>
<td></td>
<td>• 8 1</td>
</tr>
<tr>
<td></td>
<td>• 10</td>
</tr>
<tr>
<td>Microsoft Windows Server</td>
<td>• 2003 32-bit Service Pack 1</td>
</tr>
<tr>
<td></td>
<td>• 2008 R2 Service Pack 1</td>
</tr>
</tbody>
</table>

Table 2-2  Supported browsers

<table>
<thead>
<tr>
<th>Browser</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internet Explorer</td>
<td>version 6 to 11.</td>
</tr>
<tr>
<td>Google Chrome</td>
<td>version 59 to 62.</td>
</tr>
<tr>
<td>Mozilla Firefox</td>
<td>version 54.0 to 56.0.</td>
</tr>
</tbody>
</table>
Cluster requirements

To create clusters of one or more Advanced Threat Defense Appliances, make sure your environment meets the requirements.

- Use the Advanced Threat Defense Appliance eth-0 interfaces, or management ports.
- For optimal performance, all of the node eth-0 interfaces must be in the same layer-2 network of the OSI reference model.

When you setup a Virtual Advanced Threat Defense cluster, the Primary and Backup nodes must reside on the same ESXi server. The Secondary nodes can be on the same or a different ESXi server.

- All nodes must have the same:
  - Advanced Threat Defense software version
  - Analyzer VMs
  - McAfee Anti-Malware Engine DAT and engine versions
  - McAfee Gateway Anti-Malware Engine DAT and engine versions

Advanced Threat Defense cluster network connections

Eth-0 interface of the primary acts as the management interface of the cluster whereas the eth-0 of the secondary and backup node are used to exchange information with the primary.

The Backup node acts as a secondary node till the time the Primary node goes down for some reason and the Backup node takes the role of the primary node. The primary node load balances the files received on the eth-0 interface among the secondary nodes based on the number of files submitted to a node. A highly burdened node receives lesser number of samples for processing as opposed to a less burdened node. The primary node transfers files to be analyzed by the secondary node through the eth-0 interface and uses the same to retrieve results. When cluster configuration changes are made using the primary node, they are synchronized across the secondary nodes and the backup node through the eth-0 interface.

Figure 2-1 An example Advanced Threat Defense cluster deployment
In this example, eth-1 is used to provide network access to malware running on the analyzer VMs. This isolates the network traffic generated by malware from the production network to which eth-0 interfaces are connected.

A local database is maintained at the Primary node which lists the MD5 hash value along with corresponding node-id of the samples blacklisted by Advanced Threat Defense cluster node. Node-id is the primary identifier of a node that processes a particular sample. Whenever a sample is submitted to Advanced Threat Defense, the Primary node looks for an existing entry of this sample in its newly created database. If the MD5 hash value of a sample matches with an existing one in the database, this previously blacklisted sample is sent to the node based on the corresponding node-id of the sample. This approach ensures that every previously submitted, blacklisted sample reaches the node that analyzed it earlier, hence avoiding re-analysis of the blacklisted samples by any other node in the cluster.

Advanced Threat Defense determines the wait time for a submitted sample before it gets picked for analysis. The wait time is calculated based on the current sample analysis rate of the nodes. For samples submitted through MEG, a default threshold wait time of 780 seconds is allotted. Advanced Threat Defense rejects all the incoming samples from MEG until the wait time drops below this threshold value.

**Analyzer VM requirements**

To create the analyzer VM and VM profile, review the recommended requirements.

- If you already have a VMDK or VHDX file, it must be a single file that contains all the files required to create the VM.
- The platforms and other specifications listed here are based on McAfee test results.
### Recommended RAM size

<table>
<thead>
<tr>
<th>Operating system</th>
<th>RAM size (MB)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft Windows XP 32-bit (Service Pack 2 and 3)</td>
<td>512</td>
</tr>
<tr>
<td>Microsoft Windows 7 32-bit (Service Pack 1)</td>
<td>1024</td>
</tr>
<tr>
<td>Microsoft Windows 7 64-bit (Service Pack 1)</td>
<td>2048</td>
</tr>
<tr>
<td>Microsoft Windows 8 Professional 32-bit</td>
<td>2048</td>
</tr>
<tr>
<td>Microsoft Windows 8 Professional 64-bit</td>
<td>2048</td>
</tr>
<tr>
<td>Microsoft Windows 8.1 64-bit Enterprise (Update 1 version 6.3 build 9600)</td>
<td>2048</td>
</tr>
<tr>
<td>Microsoft Windows 8.1 64-bit Professional (Update 1 version 6.3 build 9600)</td>
<td>2048</td>
</tr>
<tr>
<td>Microsoft Windows 10 Enterprise 64-bit version 1607, 1703, and 1511</td>
<td>3072</td>
</tr>
<tr>
<td>Microsoft Windows 10 Professional version 1607</td>
<td>2048</td>
</tr>
<tr>
<td>Microsoft Windows Server 2003 32-bit (Service Pack 1 and 2)</td>
<td>2048</td>
</tr>
<tr>
<td>Microsoft Windows Server 2008 R2 (Service Pack 1)</td>
<td>2048</td>
</tr>
<tr>
<td>Microsoft Windows Server 2012 Datacenter</td>
<td>2048</td>
</tr>
<tr>
<td>Microsoft Windows Server 2012 R2 Standard</td>
<td>2048</td>
</tr>
<tr>
<td>Microsoft Windows Server 2012 R2 Datacenter</td>
<td>2048</td>
</tr>
<tr>
<td>Microsoft Windows Server 2016 Standard</td>
<td>2048</td>
</tr>
</tbody>
</table>

### Supported operating systems

To create an ISO image, Advanced Threat Defense supports the following operating systems.

<table>
<thead>
<tr>
<th>Operating system</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft Windows</td>
<td>• XP 32-bit Service Pack 2 and 3&lt;br&gt;• 7 32-bit Service Pack 1&lt;br&gt;• 7 64-bit Service Pack 1&lt;br&gt;• 8 Professional 32-bit&lt;br&gt;• 8 Professional 64-bit&lt;br&gt;• 8.1 Enterprise (Update 1 version 6.3 build 9600)&lt;br&gt;• 8.1 Professional (Update 1 version 6.3 build 9600)&lt;br&gt;• 10 Enterprise 64-bit version 1607, 1703, and 1511&lt;br&gt;• 10 Professional version 1607</td>
</tr>
<tr>
<td>Microsoft Windows Server</td>
<td>• 2003 32-bit Service Pack 1 and 2&lt;br&gt;• 2008 R2 Service Pack 1&lt;br&gt;• 2012 Datacenter</td>
</tr>
<tr>
<td>Android</td>
<td>• 2.3&lt;br&gt;• 4.3&lt;br&gt;• 5.2</td>
</tr>
</tbody>
</table>
If you are using a Microsoft Windows operating system, you must have the license key, and it must come in one of these languages:

- English
- Chinese Simplified
- Japanese
- German
- Italian
- Spanish
- French

### Supported applications

#### Table 2-3 Required applications

<table>
<thead>
<tr>
<th>Application</th>
<th>Supported version</th>
<th>Supported languages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internet Explorer</td>
<td>6,7,8,9,10, and 11</td>
<td>English, Chinese-Simplified, Japanese, German, and Italian.</td>
</tr>
<tr>
<td>Mozilla Firefox</td>
<td>all versions until 56.0</td>
<td>English, Chinese-Simplified, Japanese, German, and Italian.</td>
</tr>
<tr>
<td>Google Chrome</td>
<td>all versions until 62</td>
<td>All languages</td>
</tr>
<tr>
<td>JustSystems Ichitaro word processor</td>
<td>Government 8 and Pro 3 Recommended OS: Microsoft Windows 7</td>
<td>Japanese</td>
</tr>
<tr>
<td>Adobe Flash Player software and plugin</td>
<td>13</td>
<td>English</td>
</tr>
<tr>
<td>Adobe Flash Player plugin only</td>
<td>22.0.0.210</td>
<td>English</td>
</tr>
<tr>
<td>Adobe Reader</td>
<td>• 9, • 10, • 11</td>
<td>English</td>
</tr>
<tr>
<td>jdk-7u25</td>
<td>• 32-bit on all 32-bit operating systems, • 64-bit on all 64-bit operating systems</td>
<td>English</td>
</tr>
<tr>
<td>jre-7u25</td>
<td>• 32-bit on all 32-bit operating systems, • 64-bit on all 64-bit operating systems</td>
<td>English</td>
</tr>
<tr>
<td>jdk-8u101</td>
<td>• 32-bit on all 32-bit operating systems, • 64-bit on all 64-bit operating systems</td>
<td>English</td>
</tr>
<tr>
<td>jre-8u101</td>
<td>• 32-bit on all 32-bit operating systems, • 64-bit on all 64-bit operating systems</td>
<td>English</td>
</tr>
</tbody>
</table>

### Disk space

The minimum available disk space must be 200 MB. The maximum used total disk space must not exceed 30 GB.

The disk space affects the maximum number of VMs you can create.
Maximum VMs

The following table specifies the maximum number of VMs that you can create for each Microsoft Windows operating system. The number of VMs listed in the table is based on the assumption that the disk space occupied by Windows is not more than 22 GB.

- The disk space occupied by Windows could affect the maximum number of VMs you can create. For example, if the OS occupies 30 GB, then you can only create 21 VMs on ATD-3000/3100 and 42 VMs in ATD-6000/6100.

<table>
<thead>
<tr>
<th>Operating system</th>
<th>Minimum disk space occupied</th>
<th>ATD-3000 (Number of VMs)</th>
<th>ATD-6000 (Number of VMs)</th>
<th>ATD-3100 (Number of VMs)</th>
<th>ATD-6100 (Number of VMs)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft Windows XP Service Pack 2 and 3</td>
<td>5 GB</td>
<td>29</td>
<td>59</td>
<td>29</td>
<td>59</td>
</tr>
<tr>
<td>Microsoft Windows 7 32-bit</td>
<td>12 GB</td>
<td>29</td>
<td>59</td>
<td>29</td>
<td>59</td>
</tr>
<tr>
<td>Microsoft Windows 7 64-bit</td>
<td>14 GB</td>
<td>29</td>
<td>59</td>
<td>29</td>
<td>59</td>
</tr>
<tr>
<td>Microsoft Windows 8 Professional 32-bit</td>
<td>25–30 GB</td>
<td>29</td>
<td>59</td>
<td>29</td>
<td>59</td>
</tr>
<tr>
<td>Microsoft Windows 8 Professional 64-bit</td>
<td>25–30 GB</td>
<td>29</td>
<td>59</td>
<td>29</td>
<td>59</td>
</tr>
<tr>
<td>Microsoft Windows 8.1 Enterprise and Professional (Update 1 version 6.3 build 9600)</td>
<td>25–30 GB</td>
<td>29</td>
<td>59</td>
<td>29</td>
<td>59</td>
</tr>
<tr>
<td>Microsoft Windows 10 Enterprise 64-bit (version 1507, 1511, 1607, 1703) and Professional 1607</td>
<td>25–30 GB</td>
<td>29</td>
<td>59</td>
<td>29</td>
<td>59</td>
</tr>
<tr>
<td>Microsoft Windows Server 2003 Service Pack 1 and 2</td>
<td>5 GB</td>
<td>29</td>
<td>59</td>
<td>29</td>
<td>59</td>
</tr>
<tr>
<td>Microsoft Windows Server 2008 64bit Service Pack 1</td>
<td>14 GB</td>
<td>29</td>
<td>59</td>
<td>29</td>
<td>59</td>
</tr>
<tr>
<td>Microsoft Windows 2012 R2 Datacenter and Standard 64-bit</td>
<td>25–30 GB</td>
<td>29</td>
<td>59</td>
<td>29</td>
<td>59</td>
</tr>
</tbody>
</table>

Supported VM Provisioner Tool operating systems

To use the VM Provisioner Tool, you must use a supported operating system.

- Microsoft Windows XP 32-bit (Service Pack 2 and 3)
- Microsoft Windows 7 32-bit and 64-bit (Service Pack 1)
- Microsoft Windows 8 Professional 32-bit and 64-bit
- Microsoft Windows 8.1 64-bit Enterprise (Update 1 version 6.3 build 9600)
- Microsoft Windows 8.1 64-bit Professional (Update 1 version 6.3 build 9600)
- Microsoft Windows 10 Enterprise 64-bit version 1607, 1703, and 1511
- Microsoft Windows 10 Professional 64-bit version 1607
- Microsoft Windows Server 2003 Service Pack 1
• Microsoft Windows Server 2008 R2 (Service Pack 1)
• Microsoft Windows Server 2012 Datacenter
• Microsoft Windows Server 2012 R2 Datacenter
• Microsoft Windows Server 2012 R2 Standard
• Microsoft Windows Server 2016 Standard

Hardware specifications

Before you set up the Advanced Threat Defense Appliance, review the hardware specifications.

<table>
<thead>
<tr>
<th>Specification</th>
<th>ATD-3100</th>
<th>ATD-6100</th>
<th>ATD-3000</th>
<th>ATD-6000</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Packaging</strong></td>
<td>Length = 38&quot;, Width = 24&quot;, Height = 7&quot;</td>
<td>Length = 38&quot;, Width = 24&quot;, Height = 7&quot;</td>
<td>Length = 38&quot;, Width = 24&quot;, Height = 7&quot;</td>
<td>Length = 36&quot;, Width = 24&quot;, Height = 7&quot;</td>
</tr>
<tr>
<td><strong>Chassis</strong></td>
<td>R1208WTTGSR (Wildcat Pass)</td>
<td>R1208WTTGSR (Wildcat Pass)</td>
<td>R1304GZ4GC</td>
<td>R2304LH2HKC</td>
</tr>
<tr>
<td><strong>Chassis Dimension</strong></td>
<td>Length = 28&quot;, Width = 17.3&quot;, Height = 1.7&quot;</td>
<td>Length = 28&quot;, Width = 17.3&quot;, Height = 1.7&quot;</td>
<td>Length = 29&quot;, Width = 17.25&quot;, Height = 1.7&quot;</td>
<td>Length = 29&quot;, Width = 17.25&quot;, Height = 3.43&quot;</td>
</tr>
<tr>
<td><strong>Weight</strong></td>
<td>22.7 Kg (50 lbs)</td>
<td>22.7 Kg (50 lbs)</td>
<td>15 Kg (33 lbs)</td>
<td>22.7 Kg (50 lbs.)</td>
</tr>
<tr>
<td><strong>Form Factor</strong></td>
<td>1U rack mountable; fits 19-inch rack</td>
<td>1U rack mountable; fits 19-inch rack</td>
<td>1U rack mountable; fits 19-inch rack</td>
<td>2U rack mountable; fits 19-inch rack</td>
</tr>
<tr>
<td><strong>Motherboard</strong></td>
<td>S2600WTT</td>
<td>S2600WTT</td>
<td>S2600GZ4</td>
<td>S4600LH2</td>
</tr>
<tr>
<td><strong>CPU</strong></td>
<td>2 x E5-2609v4, 1.7GHz, 20M cache, 8 Cores</td>
<td>2 x E5-2695v4, 2.1GHz, 45M cache, 18 Cores</td>
<td>2 x E5-2658, 2.10GHz, 20M Cache, 8 Cores</td>
<td>4 x E5-4640, 2.40GHz, 20M Cache, 8 Cores</td>
</tr>
</tbody>
</table>
| **Storage**         | • Disk space HDD: 4 x 1.2TB, SAS, 12GB/s, 10K RPM, 2.5", Raid-5  
                      • SSD: 2 x Intel Enterprise grade 400GB, 2.5", Raid-0 | • Disk space HDD: 6 x 1.2TB, SAS, 12GB/s, 10K RPM, 2.5", Raid-5  
                      • SSD: 2 x Intel Enterprise grade 800 GB, 2.5", Raid-0 | • Disk space HDD: 2 x 4TB  
                      • SSD: 2 x 400 GB | • Disk space HDD: 4 x 4TB  
                      • SSD: 2 x 800 GB |
| **Memory**          | 16 x 16 GB DDR4 2400MHz ECC       | 16 x 32 GB DDR4 2400MHz ECC       | 192 GB                            | 256 GB                            |
| **Remote Management** | RMM4LITE2                        | RMM4LITE2                        | RMM4R                             | RMM4                             |
| **Power Supply**    | 750 W redundant                   | 750 W redundant                   | 2x 750W, AC redundant, hot swappable | 2x 1600W, AC redundant, hot swappable |
| **Network Interfaces** | Dual Integrated 10 GB and Dual 10 GB Module  | Dual Integrated 10 GB and Dual 10 GB Module  | Dual Integrated 10 GB and Dual 10 GB Module  | Dual Integrated 10 GB and Dual 10 GB Module  |
## System environmental limits

These are the system environmental limits for the Advanced Threat Defense Appliance.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>State or category</th>
<th>ATD-3100 and ATD 6100</th>
<th>ATD-3000</th>
<th>ATD-6000</th>
</tr>
</thead>
</table>
| Temperature | Operating | • **ASHRAE Class A2**  
— Continuous Operation, 10° C to 35° C (50° F to 95° F) with the maximum rate of change not to exceed 10°C per hour  
• **ASHRAE Class A3**  
— Includes operation up to 40° C for up to 900 hours per year  
• **ASHRAE Class A4**  
— Includes operation up to 45° C for up to 90 hours per year | +10°C to +35°C (+50°F to +95°F) with the maximum rate of change not to exceed 10°C per hour | +10°C to +35°C (+50°F to +95°F) with the maximum rate of change not to exceed 10°C per hour |
| Shipping | -40°C to 70°C (-40°F to 158°F) | -40°C to +70°C (-40°F to +158°F) | -40°C to +70°C (-40°F to +158°F) |
| Altitude | Operating | Support operation up to 3050 meters (10,000 feet) with ASHRAE class deratings | Support operation up to 3050 meters (10,000 feet) | Support operation up to 3050 meters (10,000 feet) |
| Humidity | Shipping | 50% to 90%, non-condensing with a maximum wet bulb of 28°C (at temperatures from 25°C to 35°C) | • **Operational** — 10% to 90%  
• **Non-operational** — 90% at 35°C | • **Operational** — 10% to 90%  
• **Non-operational** — 50% to 90% with a maximum wet bulb of 28°C (at temperatures from 25°C to 35°C) |
| Shock | Operating | Half sine, 2 g peak, 11 milliseconds | Half sine, 2 g peak, 11 milliseconds | Half sine, 2 g peak, 11 milliseconds |
| Unpackaged | Trapezoidal, 25 g, velocity change is based on packaged weight | Trapezoidal, 25 g, velocity change 136 inches/second (≥40 lbs to < 80 lbs) | Trapezoidal, 25 g, velocity change is based on packaged weight |
| Packaged | International Safe Transit Association (ISTA) Test Procedure 3A 2008 | Non-palletized free fall in height 24 inches (≥40 lbs to < 80 lbs) | • Product Weight: ≥ 40 to < 80  
• Non-palletized Free Fall Height = 18 inches  
• Palletized (single product) Free Fall Height = NA |
<table>
<thead>
<tr>
<th>Parameter</th>
<th>State or Category</th>
<th>ATD-3100 and ATD 6100</th>
<th>ATD-3000</th>
<th>ATD-6000</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vibration</td>
<td>Unpackaged</td>
<td>5 Hz to 500 Hz, 2.20 g RMS random</td>
<td>5 Hz to 500 Hz, 2.20 g RMS random</td>
<td>5 Hz to 500 Hz, 2.20 g RMS random</td>
</tr>
<tr>
<td></td>
<td>Packaged</td>
<td>International Safe Transit Association (ISTA) Test Procedure 3A 2008</td>
<td>5 Hz to 500 Hz, 1.09 g RMS random</td>
<td>5 Hz to 500 Hz, 1.09 g RMS random</td>
</tr>
<tr>
<td>AC-DC</td>
<td>Voltage</td>
<td>ATD-3100</td>
<td>100 - 240 V at 5.8 Amps</td>
<td>100 - 240 V. 8.5 Amps</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 115V - 5.4 Amps</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 220V - 2.7 Amps</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>ATD-6100</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 115V - 6.7 Amps</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 220V - 3.4 Amps</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Frequency</td>
<td>47 Hz to 63 Hz</td>
<td>50 - 60 Hz</td>
<td>50 - 60 Hz</td>
</tr>
<tr>
<td></td>
<td>Source Interrupt</td>
<td>No Loss of data for power line drop-out of 12 milliseconds</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Surge (Operating and non-operating)</td>
<td>Unidirectional</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Line to earth Only</td>
<td>• AC Leads — 2.0 kV</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• I/O Leads — 1.0 kV</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• DC Leads — 0.5 kV</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ESD</td>
<td>Air Discharged</td>
<td>12.0 kV</td>
<td>+/-12 kV except I/O port +/- 8 kV per Intel® Environmental test specification</td>
<td>12.0 kV</td>
</tr>
<tr>
<td></td>
<td>Contact Discharge</td>
<td>8.0 kV</td>
<td></td>
<td>8.0 kV</td>
</tr>
<tr>
<td>Acoustic noise</td>
<td>Power level &lt;300 W</td>
<td>7.0 BA</td>
<td>Sound power: 7.0 BA in operating conditions at typical office ambient temperature (23 +/- 2 degrees C)</td>
<td>Sound power: 7.0 BA in operating conditions at typical office ambient temperature (23 +/- 2 degrees °C)</td>
</tr>
<tr>
<td></td>
<td>Power level &gt;300 W</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Power level &gt;600 W</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Power level &gt;1000 W</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Certifications</td>
<td>Safety certification</td>
<td>UL 1950, CSA-C22.2 No. 950, EN-60950, IEC 950, EN 60825, 21CFR1040 CB license and report covering all national country deviations</td>
<td>FCC Part 15, Class A (CFR 47) (USA) ICES-003 Class A (Canada), EN55022 Class A (Europe), CISPR22 Class A (Int’l)</td>
<td>FCC Part 15, Class A (CFR 47) (USA) ICES-003 Class A (Canada), EN55022 Class A (Europe), CISPR22 Class A (Int’l)</td>
</tr>
<tr>
<td></td>
<td>EMI certification</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Default ports used in Advanced Threat Defense communication

The Advanced Threat Defense Appliance uses many ports for network communications.

<table>
<thead>
<tr>
<th>Client</th>
<th>Server</th>
<th>Default port</th>
<th>Configurable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any (desktop)</td>
<td>Advanced Threat Defense</td>
<td>TCP 443 (HTTPS)</td>
<td>No</td>
<td>Access the Advanced Threat Defense web interface.</td>
</tr>
<tr>
<td>Any (desktop)</td>
<td>Advanced Threat Defense</td>
<td>TCP 6080 (HTTPS)</td>
<td>No</td>
<td>For VM activation process and X-mode.</td>
</tr>
<tr>
<td>Sensor</td>
<td>Advanced Threat Defense</td>
<td>TCP 8505</td>
<td>No</td>
<td>Communication channel between a Sensor and Advanced Threat Defense.</td>
</tr>
<tr>
<td>Manager</td>
<td>Advanced Threat Defense</td>
<td>TCP 443 (HTTPS)</td>
<td>No</td>
<td>Communication between the Manager and Advanced Threat Defense through the RESTful APIs.</td>
</tr>
<tr>
<td>Advanced Threat Defense</td>
<td>McAfee ePO</td>
<td>TCP 8443</td>
<td>Yes</td>
<td>Host information queries.</td>
</tr>
<tr>
<td>Advanced Threat Defense</td>
<td>tunnel.web.trustedsource.org</td>
<td>TCP 443 (HTTPS)</td>
<td>No</td>
<td>File Reputation queries.</td>
</tr>
<tr>
<td>Advanced Threat Defense</td>
<td>List.smartfilter.com</td>
<td>TCP 80 (HTTP)</td>
<td>No</td>
<td>URL updates.</td>
</tr>
<tr>
<td>Any (SSH client)</td>
<td>Advanced Threat Defense</td>
<td>TCP 2222 (SSH)</td>
<td>No</td>
<td>CLI access.</td>
</tr>
</tbody>
</table>
### Plan your deployment

**Default ports used in Advanced Threat Defense communication**

<table>
<thead>
<tr>
<th>Client</th>
<th>Server</th>
<th>Default port</th>
<th>Configurable</th>
<th>Description</th>
</tr>
</thead>
</table>
| Advanced Threat Defense (DAT updates) | wpm.webwasher.com  
wpm-2.webwasher.com  
wpm-3.webwasher.com  
wpm-4.webwasher.com  
wpm-usa.webwasher.com  
wpm-usa1.webwasher.com  
wpm-usa2.webwasher.com  
wpm-asia.webwasher.com  
tau.mcafee.com  
tau-2.mcafee.com  
tau-3.mcafee.com  
tau-4.mcafee.com  
tau-usa.mcafee.com  
tau-usa1.mcafee.com  
tau-usa2.mcafee.com  
tau-manual.mcafee.com  
tau-ldv1.securelabs.webwasher.com  
tau-ldv2.securelabs.webwasher.com  
tau-ldv3.securelabs.webwasher.com  
tau-europe.mcafee.com  
tau-dnv1.securelabs.webwasher.com  
tau-dnv2.securelabs.webwasher.com  
tau-dnv3.securelabs.webwasher.com  
tau-asia.mcafee.com  
rpns.mcafee.com  
mwg-update.mcafee.com | TCP 443 (HTTPS) | No | Updates for McAfee Gateway Anti-Malware Engine and McAfee Anti-Malware Engine. |
| Advanced Threat Defense (Software updates) | atdupdate.mcafee.com | TCP 443 (HTTPS) | No | Updates for the Advanced Threat Defense software |
Warnings and cautions

Read and follow these safety warnings when you install the Advanced Threat Defense Appliance. Failure to observe these safety warnings could result in serious physical injury.

- **Advanced Threat Defense Appliance power on/off** — the push-button on/off power switch on the front panel of the Advanced Threat Defense Appliance does not turn off the AC power. To remove AC power from the Advanced Threat Defense Appliance, you must unplug the AC power cord from either the power supply or wall outlet for both the power supplies. If you press the push-button on/off power switch on the front panel of the Advanced Threat Defense Appliance while the appliance is running, it reboots. If you want to power off the appliance, use CLI command — shutdown, after the system halts press the power button until the appliance powers off.

- **The power supplies in your system might produce high voltages and energy hazards, which can cause bodily harm. Only trained service technicians are authorized to remove the covers and access any of the components inside the system.**

- **Hazardous conditions — devices and cables:** Hazardous electrical conditions might be present on power, telephone, and communication cables. Turn off the Advanced Threat Defense Appliance and disconnect telecommunications systems, networks, modems, and both the power cords attached to the Advanced Threat Defense Appliance before opening it. Otherwise, personal injury or equipment damage can result.

- **Avoid injury — lifting the Advanced Threat Defense Appliance and attaching it to the rack is a two-person job.**

- **This equipment is intended to be grounded. Ensure that the host is connected to earth ground during normal use.**

- **Do not remove the outer shell of the Advanced Threat Defense Appliance. Doing so invalidates your warranty.**

- **Do not operate the system unless all cards, faceplates, front covers, and rear covers are in place. Blank faceplates and cover panels prevent exposure to hazardous voltages and currents inside the chassis, contain electromagnetic interference (EMI) that might disrupt other equipment and direct the flow of cooling air through the chassis.**

- **To avoid electric shock, do not connect safety extra-low voltage (SELV) circuits to telephone-network voltage (TNV) circuits. LAN ports contain SELV circuits, and WAN ports contain TNV circuits. Some LAN and WAN ports both use RJ-45 connectors. Use caution when connecting cables.**

### Deployment checklist

To make sure that your network is ready to set up Advanced Threat Defense, review the deployment checklist.

<table>
<thead>
<tr>
<th>Determine...</th>
<th>Verified</th>
</tr>
</thead>
<tbody>
<tr>
<td>If you environment meets all of the minimum requirements</td>
<td></td>
</tr>
<tr>
<td>The location that you want to install the Advanced Threat Defense Appliance and familiarized yourself with the network access card ports and connectors</td>
<td></td>
</tr>
<tr>
<td>That you have the following information to configure the Advanced Threat Defense Appliance:</td>
<td></td>
</tr>
<tr>
<td>• IPv4 address that you want to assign to the Advanced Threat Defense Appliance</td>
<td></td>
</tr>
<tr>
<td>• Network mask</td>
<td></td>
</tr>
<tr>
<td>• Default gateway address</td>
<td></td>
</tr>
<tr>
<td>Determine...</td>
<td>Verified</td>
</tr>
<tr>
<td>---------------------------------------------------------------------------</td>
<td>----------</td>
</tr>
<tr>
<td>The type of installation that is best for your network:</td>
<td></td>
</tr>
<tr>
<td>• Standalone</td>
<td></td>
</tr>
<tr>
<td>• Virtual</td>
<td></td>
</tr>
<tr>
<td>• Cluster</td>
<td></td>
</tr>
<tr>
<td>Which users you want to assign administrator permissions</td>
<td></td>
</tr>
<tr>
<td>If you plan to use Advanced Threat Defense with any compatible McAfee product</td>
<td></td>
</tr>
</tbody>
</table>
Installing the OS, software, and Email Connector

Your Advanced Threat Defense Appliance comes pre-installed with an operating system (OS) and Advanced Threat Defense software. Email Connector is not pre-installed and you need to install it separately.

**OS and Advanced Threat Defense software for your appliance**

You can do a clean install of the OS and Advanced Threat Defense software for both physical and virtual appliances. One of the scenarios for you to perform a clean install is during a software migration.

During a software migration, such as migrating to Advanced Threat Defense 4.2, your existing version of Advanced Threat Defense should meet the migration path criteria.

**For example**, if your current Advanced Threat Defense version is 3.8.0 or above, you can directly migrate to Advanced Threat Defense 4.2 using the migration package. But, if your current Advanced Threat Defense version is 3.6.0 or below, you have two choices:

- **upgrade your Advanced Threat Defense software to 3.8.0 and then use the migration package to migrate to 4.2.**
  
  All your data, configurations, and certificates on your Advanced Threat Defense appliance are backed up and restored.

- **perform a clean install of your OS and Advanced Threat Defense software.**
  
  You lose all your data, configurations, and certificates from your Advanced Threat Defense appliance.

If your current Advanced Threat Defense version is 3.8.0 or above, McAfee recommends that you use the migration package to upgrade to Advanced Threat Defense 4.2. For more information, see *McAfee Advanced Threat Defense Migration Guide*.

**Virtual Advanced Threat Defense**

Similarly you can do a clean install of the Virtual Advanced Threat Defense appliance. You can download the appliance installation files for your respective hypervisor from the download site.

McAfee recommends that you use the migration package to upgrade to Advanced Threat Defense 4.2. For more information, see *McAfee Advanced Threat Defense Migration Guide*.

**Email Connector**

Email Connector protects you from email borne threats by analyzing email attachments through Advanced Threat Defense.

Email Connector is not installed by-default when you install Advanced Threat Defense.

To install Email connector:
• Download the Email connector installer from the download site.
• SFTP the installer to your appliance.
• Install Email connector.

Contents
- Installer package details
- Install the OS to your appliance
- Install the OS to your appliance remotely using RMM
- Install the Advanced Threat Defense software
- Installing Virtual Advanced Threat Defense
- Install Email Connector

Installer package details
Review and identify the packages you would use while installing the Operating system, Advanced Threat Defense software, and Email Connector.

<table>
<thead>
<tr>
<th>Installer package name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>migration-4.2.x.x.xxxxx.msu</td>
<td>Migration package.</td>
</tr>
<tr>
<td></td>
<td>This package migrates your Advanced Threat Defense Appliance to 4.2.</td>
</tr>
<tr>
<td></td>
<td>Use this package only if:</td>
</tr>
<tr>
<td></td>
<td>• Advanced Threat Defense version is 3.8.0 or later.</td>
</tr>
<tr>
<td></td>
<td>• Virtual Advanced Threat Defense version is 3.10.0 or above.</td>
</tr>
<tr>
<td></td>
<td>For more information, see McAfee Advanced Threat Defense Migration Guide.</td>
</tr>
<tr>
<td>ATD_installer.xxxxx.x86_64.iso</td>
<td>Operating System installation package.</td>
</tr>
<tr>
<td></td>
<td>This package does a clean install of the Operating System for your appliance.</td>
</tr>
<tr>
<td></td>
<td>For more information, see:</td>
</tr>
<tr>
<td></td>
<td>• For on-premises or direct install – Install the OS to your appliance</td>
</tr>
<tr>
<td></td>
<td>• For install using RMM – Install the OS to your appliance remotely using RMM</td>
</tr>
<tr>
<td>Installer package name</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| system-4.2.x.xx.xxxxx.msu            | Advanced Threat Defense installation package  
Virtual Advanced Threat Defense upgrade package  
This package does the follow:  
• Installs the Advanced Threat Defense software on your appliance.  
• Upgrade your Virtual Advanced Threat Defense appliance.  
  
  [This package does not install Email Connector by-default.]
For more information, see:  
• Install the Advanced Threat Defense software in this guide.  
• Virtual Advanced Threat Defense Addendum |
| vATD-MIO-4_2_x_xx-xxxxx-xxxxx.ova     | Virtual Advanced Threat Defense installation package for VMWare ESXi.  
Use this package to deploy a new Virtual Advanced Threat Defense 4.2 appliance on your ESXi server.  
  
  [This package does not install Email Connector by-default.]
| hvATD_MIH_4_x_x_xx-xxxxx-xxxxx.zip   | Virtual Advanced Threat Defense installation package for Microsoft Hyper-V  
Use this package to deploy a new Virtual Advanced Threat Defense 4.2 appliance on your Hyper-V server.  
  
  [This package does not install Email Connector by-default.]
| systemex-4.2.x.xx.xxxxx.msu          | Email Connector installation package.  
This package installs email connector on Advanced Threat Defense 4.2 appliance and Virtual Advanced Threat Defense appliance.  
For more information, see Install Email Connector. |

Install the OS to your appliance

You can do a clean install of Advanced Threat Defense on your appliance. The clean install begins with installing the OS.

**Task**

1. Download the OS installer and transfer it to a USB storage device. To download the installer, follow these steps:
   b. Enter your grant number and the captcha, then click Submit.
   c. Download the OS and Advanced Threat Defense installers.

OS Installer: `ATD_installer.xxxxx.x86_64.iso`
Advanced Threat Defense installer: `system-4.2.x.xx.xxxxx.msu`
2. Make the USB storage device bootable and connect it to the Advanced Threat Defense Appliance. To make your
USB storage device bootable, follow these steps:
   a. Connect your USB storage device to your Linux system.
      • Minimum required capacity of the USB Storage Device is 4 GB.
      • Recommended Linux distributions are CentOS Linux 6.5 or Red Hat Enterprise Linux 7.
   b. Identify your USB storage device. Use the `dmesg` command to identify your USB storage device.
      ```
      dmesg | grep sd
      ```
      The command returns a list of all connected devices on your system.
   c. Format your USB storage device. Use the `dd` command to format your USB storage device.
      ```
      dd if=/dev/zero of=/dev/sdX count=1234
      ```
      Replace `/dev/sdX` with the device name as reported by the `dmesg` command earlier.
   d. Copy the OS ISO image to your Linux system.
   e. Write the OS ISO image to your USB storage device. Use the `dd` command to write the image to your USB
      storage device.
      ```
      dd if=<OS Installer Location> of=/dev/sdX bs=4M && sync
      ```
      Replace `<OS Installer Location>` with the full path to the ISO image file you downloaded, `sdX` with
      the device name as reported by the `dmesg` command earlier.

3. Connect the USB Storage Device to your Advanced Threat Defense appliance. Connect your RMM terminal
or Advanced Threat Defense Monitor Console and keyboard to your Advanced Threat Defense appliance,
then reboot your appliance using the `reboot` command.

4. At the time of reboot, press F6 on the keyboard to enter the boot menu.

5. From the boot device selection prompt, use the up or down arrow keys on the keyboard to select your USB
storage device, then press Enter.

   The OS installation begins from the USB storage device.

   Installer prompts you to take backup of your data or to proceed with a clean install. Since this is a clean
install, any inputs to back up your data will fail. If you want to back up your data, we recommend you upgrade
to Advanced Threat Defense 3.8.0 and then migrate to Advanced Threat Defense 4.0. For more information,
see McAfee Advanced Threat Defense Migration Guide.

6. Click Cancel to cancel the backup prompt, then click Yes to confirm to proceed with a clean install.

   The backup prompt screen times out in 120 seconds. If you do not provide any inputs with in the given time,
the backup is initiated by default.

The OS installation now begins. Your appliance will reboot during the course of installation.
Once the OS installation is complete, you'll see the Log on screen to your appliance.
Install the OS to your appliance remotely using RMM

You can choose to install the OS remotely to your appliance using RMM.

**Task**

1. Download the OS installer. To download the installer, follow these steps:
   b. Enter your grant number and the captcha, then click Submit.
   c. Download the OS and Advanced Threat Defense installers.

   - OS Installer: ATD_installer.xxxxx.x86_64.iso
   - Advanced Threat Defense installer: system-4.2.x.xx.xxxxx.msu

2. On your web browser, Logon to the Advanced Threat Defense RMM IP (http://<ATD RMM IP> or https://<ATD RMM IP>) and open the Advanced Threat Defense RMM console. If security settings of browser is blocking the page, do the following:
   - Disable popup blocker for this web page.
   - Add the ATD RMM URL to the Local Windows Machine. Goto Control panel | Java | Security, then add your ATD RMM URL (eg: http://<ATD RMM IP> or https://<ATD RMM IP>) to the Exception Site List.

3. From the Remote Control tab, then click Launch Console.

   Accept the JViewer Launcher security warning and the RMM console for your Advanced Threat Defense appliance is open.

4. On the RMM Console screen click the Device tab, then select Redirect ISO.

5. Browse and select to the OS installer file on your local windows machine.

6. Logon to your Advanced Threat Defense console as cliadmin.

7. Reboot the appliance using the reboot command.

8. During boot up, press F6 to enter the boot menu.

9. From the boot device selection prompt, use the up or down arrow keys on the keyboard to select Virtual CDROM 1.00, then press Enter.

10. The OS installation begins from the ISO image file.

   During the installation, the installer will prompt you to take backup of your data or to proceed with a clean install. Since this is a clean install, any inputs to back up your data will fail. If you want to back up your data, we recommend you upgrade to Advanced Threat Defense 3.8.0 and then migrate to Advanced Threat Defense 4.2. For more information, see McAfee Advanced Threat Defense Migration Guide.

11. Click Cancel on backup notification, then click Yes to proceed for clean install.

The OS installation now begins. Your appliance will reboot during the course of installation. Once the OS installation is complete, you'll see the Log on screen to your appliance.
Install the Advanced Threat Defense software

After the OS installation is complete, you can begin the installation of the latest Advanced Threat Defense software.

**Task**


2. If you have not configured your IP address and Gateway, set them for your appliance with these commands:
   - To set the IP Address
     ```bash
     set appliance ip <xxx.xxx.xxx.xxx> <xxx.xxx.xxx.xxx>
     ```
   - To set the gateway
     ```bash
     set appliance gateway <xxx.xxx.xxx.xxx>
     ```

   For more information on these commands, see *McAfee Advanced Threat Defense Product Guide*.

3. Upload the Advanced Threat Defense installer (system-4.x.x.xxx.msu) to your appliance. Do the following steps to upload the installer:
   - a) Using an FTP client (such as Filezilla), log in to your Advanced Threat Defense Appliance using the default username: atdadmin and password: atdadmin.
   - b) Using SFTP, upload the installer to your appliance.

   Ensure that the transfer mode is binary.

4. Install Advanced Threat Defense using the following command:

   ```bash
   install msu <installer name>.msu 0
   ```

   Replace `<installer name>` with the name of the Advanced Threat Defense installer file.

   After the installation is complete, the appliance will reboot automatically.

5. Post installation, log on to your Advanced Threat Defense web interface to verify the software version.

Installing Virtual Advanced Threat Defense

McAfee Virtual Advanced Threat Defense appliance can be installed and deployed on VMWare ESXi and Microsoft Hyper-V virtual machine environment.

After a successful installation, take a snapshot of the McAfee Virtual Advanced Threat Defense instance in power off state. You might need that later to recover an erroneous installation. There is no USB recovery stick or Remote Management Module available with McAfee Virtual Advanced Threat Defense.
Prepare your sandbox virtual machine
 Activate the product

Requirements
To ensure that your deployment is successful, your environment must meet the minimum requirements.

Virtual system requirements
Make sure that your virtual system meets these requirements.

Total number of virtual CPU and memory requirement depends on the number of deployments on the ESXi or Hyper-V servers.

These are just minimum resource requirements. Make sure that there's enough resource available when multiple virtual machines are running at the same time.

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hypervisor support</td>
<td>• VMware ESXi 5.5 server: Hardware version 9, 10</td>
</tr>
<tr>
<td></td>
<td>• VMware ESXi 6.0 server: Hardware version 9, 10, 11</td>
</tr>
<tr>
<td></td>
<td>• Microsoft Hyper-V</td>
</tr>
<tr>
<td>VM file format</td>
<td>• Open Virtualization Appliance (OVA)</td>
</tr>
<tr>
<td></td>
<td>• Hyper-V Virtual Hard disk (VHDX)</td>
</tr>
<tr>
<td>Virtual CPUs</td>
<td>• Small scale deployment — 16</td>
</tr>
<tr>
<td></td>
<td>• Mid scale deployment — 32</td>
</tr>
<tr>
<td></td>
<td>• Large scale deployment — 48</td>
</tr>
<tr>
<td></td>
<td>• Extra large scale deployment — 64</td>
</tr>
<tr>
<td>Virtual Memory</td>
<td>• Small scale deployment — 32 GB</td>
</tr>
<tr>
<td></td>
<td>• Mid scale deployment — 64 GB</td>
</tr>
<tr>
<td></td>
<td>• Large scale deployment — 128 GB</td>
</tr>
<tr>
<td></td>
<td>• Extra large scale deployment — 256 GB</td>
</tr>
<tr>
<td>Virtual Disk</td>
<td>• Small scale deployment — 750 GB</td>
</tr>
<tr>
<td></td>
<td>• Mid scale deployment — 1.5 TB</td>
</tr>
<tr>
<td></td>
<td>• Large scale deployment — 3 TB</td>
</tr>
<tr>
<td></td>
<td>• Extra large scale deployment — 6 TB</td>
</tr>
<tr>
<td>Physical Network Interface</td>
<td>2 (E1000)</td>
</tr>
<tr>
<td>Virtual Network Interfaces</td>
<td>2 (Management interface—1; Malware interface—1)</td>
</tr>
<tr>
<td>Physical system setting</td>
<td>Enable Virtualization Technology option in BIOS.</td>
</tr>
</tbody>
</table>
Physical server requirements
To deploy McAfee Virtual Advanced Threat Defense on explicit servers, make sure that your server meets these requirements.

On ESXi Servers

<table>
<thead>
<tr>
<th>Appliance model</th>
<th>Number CPU cores</th>
<th>RAM</th>
<th>Disc space</th>
<th>Network interfaces</th>
</tr>
</thead>
<tbody>
<tr>
<td>1008 (Small scale deployment)</td>
<td>8</td>
<td>48 GB</td>
<td>1 TB</td>
<td>2</td>
</tr>
<tr>
<td>1016 (Mid scale deployment)</td>
<td>12</td>
<td>72 GB</td>
<td>2 TB</td>
<td>2</td>
</tr>
<tr>
<td>3032 (Large scale deployment)</td>
<td>16</td>
<td>144 GB</td>
<td>3.5 TB</td>
<td>2</td>
</tr>
<tr>
<td>6064 (Extra large scale deployment)</td>
<td>32</td>
<td>256 GB</td>
<td>6.5 TB</td>
<td>2</td>
</tr>
</tbody>
</table>

On Hyper-V

<table>
<thead>
<tr>
<th>Appliance model</th>
<th>Number CPU cores</th>
<th>RAM</th>
<th>Disc space</th>
<th>Network interfaces</th>
</tr>
</thead>
<tbody>
<tr>
<td>hvATD</td>
<td>16</td>
<td>32 GB</td>
<td>400 GB</td>
<td>2</td>
</tr>
</tbody>
</table>

Install Virtual Advanced Threat Defense on ESXi server
Place an order, download the software, then deploy it on the ESXi server.

Before you begin
- Enable the nested virtualization on the VMware ESXi server. In an SSH session of ESXi server, add this property to the configuration file at /etc/vmware/config.
  
  vhv.enable = "TRUE"

- From the ESX Web GUI or VCenter VM settings, enable Expose hardware assisted virtualization to the guest OS.

  Power off your VM before you change the VM settings.

To upgrade from an existing version of McAfee Virtual Advanced Threat Defense, see the Upgrade the software and Android analyzer VM topic in the McAfee Advanced Threat Defense product guide. If you upgrade from a trial version of the software, obtain the license key and grant number from the McAfee order fulfillment team at licensing@mcafee.com again and activate it.

Task

1. Place a Purchase Order (PO) for McAfee Virtual Advanced Threat Defense, and receive an email with your grant number and license key.

2. Log on to https://secure.mcafee.com/apps/downloads/my-products/login.aspx?region=us with the grant number and download the software.

   Package name: vATD-MIO-4_2_x_xx-xxxxx-xxxxx.ova

3. Deploy the software on an ESXi server.
   a. From a vSphere client, select File | Deploy OVF Template.
   b. Click Browse, locate and select the McAfee Virtual Advanced Threat Defense software, click Open, then click Next.
   c. Type a name the OVF template, then click Next.
d  On Disk Format, select Thin Provision, then click Next.

e  On Network Mapping, select a network, then click Next.

f  Review the deployment settings, select Power on after deployment, then click Finish.

For multiple McAfee Virtual Advanced Threat Defense instances, deploy the OVA again.

Install Virtual Advanced Threat Defense on Hyper-V using the automated script

Place an order, download the software, then use the downloaded script to easily deploy Virtual Advanced Threat Defense on the Hyper-V server.

Before you begin

Ensure that you have enabled Hyper-V (including Hyper-V Management Tools and Hyper-V Platform) from Control Panel | Programs and Features | Turn Windows features on or off | Hyper-V.

Virtual Advanced Threat Defense for Hyper-V is supported on the following platforms:

- Windows 10 Anniversary Update (version 1607) or later
- Windows Server 2016 Datacenter (Server with GUI)

Requirements:

- Disk size: 400 GB
- RAM size: 32 GB
- Virtual CPU Cores: 16

The Hyper-V host and guest must both be on the supported platforms.

Task

Your downloaded package consists of two scripts. This gives you three methods to install Virtual Advanced Threat Defense on Hyper-V.

- Using setup.exe – Run this file as an administrator to create an instance of Virtual Advanced Threat Defense on Hyper-V.

  This VM creation method requires Visual C++ runtime package.

- Using deploy_hvatd.ps1 – Run this PowerShell script to create an instance of Virtual Advanced Threat Defense on Hyper-V.

- Using your own changed deploy_hvatd.ps1 – You can change this PowerShell script according to your needs, then run it to create an instance of Virtual Advanced Threat Defense on Hyper-V.

  deploy_hvatd.ps1 is signed by McAfee. If you change the script, it loses the McAfee signature.

1  Place a Purchase Order (PO) for McAfee Virtual Advanced Threat Defense, and receive an email with your grant number and license key.

2  Log on to https://secure.mcafee.com/apps/downloads/my-products/login.aspx?region=us with the grant number and download the software package.

  Package name: hvATD_MIH_4.2_x_xxxxx_xxxxx_xxxxx.zip
3 Unzip the .zip file to any location on your system.

4 Do one of the following:
   • Run setup.exe as an Administrator.
     The setup automatically creates one instance of Virtual Advanced Threat Defense. The first instance is named hvatd1. You can run setup.exe multiple times depending on the number of Virtual Advanced Threat Defense instances that you require.
   • Run deploy_hvatd.ps1 to create an instance of Virtual Advanced Threat Defense on Hyper-V.
     The script automatically creates one instance of Virtual Advanced Threat Defense. The first instance is named hvatd1. To create multiple instances of Virtual Advanced Threat Defense, create a deploy_hvatd.ps1 for each instance, and run them sequentially.
     You might have to set the execution policy using Set-ExecutionPolicy RemoteSigned.
   • Change deploy_hvatd.ps1 according to your needs, then run it to create an instance of Virtual Advanced Threat Defense on Hyper-V. You can run the changed deploy_hvatd.ps1 multiple times depending on the number of Virtual Advanced Threat Defense instances that you require.
     • deploy_hvatd.ps1 is signed by McAfee. If you change the script, it loses the McAfee signature.
     • If you are running the changed script, you need to enabled nested virtualization. Run the following cmdlet to enable nested virtualization:
       ```powershell
       Set-VMProcessor -VMName <VMName> -ExposeVirtualizationExtensions $true
       ```
       Replace <VMName> with the name of your Hyper-V virtual machine.

5 Add a network interface for the VMs.
   a Open Hyper-V Manager, then select a Virtual Advanced Threat Defense instance.
   b Right-click on the VM, then click Settings.
   c In the navigation pane, click Add Hardware, then choose a network adapter.
   d Click Add, then under Network, select the virtual network you want to connect to.
   e Click OK.

**Install Virtual Advanced Threat Defense on Hyper-V manually**
Place an order, download the software, then deploy it on Hyper-V server.

**Before you begin**
• Ensure that you have enabled Hyper-V (including Hyper-V Management Tools and Hyper-V Platform) from Control Panel | Programs and Features | Turn Windows features on or off | Hyper-V.
• Unzip the Virtual Advanced Threat Defense package that you purchased from McAfee. The package includes hvATD.vhdx. This is the disk image of Virtual Advanced Threat Defense.

**Task**
1 Open Hyper-V Manager, then from the Actions pane, select New | Virtual Machine....
2 Type a name for your virtual machine, then click Next.
   You can also choose to store your virtual machine at an alternate location.
3 In the Specify Generation section, choose **Generation 1**.

4 In the Assign Memory section, set 32 GB.

5 In the Configure Networking section, choose a virtual switch.

6 In the Connect Virtual Hard Disk section, select **Use an existing virtual hard disk**.

7 Click **Browse**, then select **hvATD.vhdx**, and then click **Finish**.

   - If you plan to deploy multiple instances of Virtual Advanced Threat Defense, make a copy of **hvATD.vhdx**.

8 Right click on the VM, then select **Settings** | **Memory** | **Processor**, then set the processor core to **16**.

9 Open PowerShell. Enable nested virtualization using the following command:

   ```powershell
   Set-VMProcessor -VMName <Target VM's name> -ExposeVirtualizationExtensions $true
   ``

   In `<Target VM's name>`, enter the name of the VM that you created.

10 Set Static IP address and Gateway to the VM using Advanced Threat Defense console.

### Deploy Virtual Advanced Threat Defense from Azure Marketplace

You can deploy Virtual Advanced Threat Defense from the Azure Marketplace directly.

**Task**

- **On Azure, Advanced Threat Defense does not support UDP for Syslog. Advanced Threat Defense supports only TCP and TCP/TLS for Syslog.**

1 Login to your Azure Portal (https://portal.azure.com) and from the marketplace search for **McAfee ATD**.

2 Select McAfee Advanced Threat Defense from the search result.

3 In the Basics tab, do the following:
   a In ATD Cluster name, type a cluster name for your ATD.
   b In Cluster Size, choose an appropriate cluster size.
   c From the Subscription drop-down, choose your subscription.
   d In Resource group, choose **Create new**. and type a group name.
   e In Location, choose your location.

   Check your geographic availability of the selected VM Size at the following Azure Blog:

4 In the VM Settings tab, do the following:
   a In the Virtual Machine Size, select a virtual machine.
   b In Storage account, type a name for your storage account.
      Choose appropriate values for **Performance** and **Replication**.
   c In Virtual network, type a name and ATD cluster address space for your virtual network.
   d In Subnets, type a name and ATD cluster subnet address space for your subnets.
5 In the Summary tab, review your settings.

6 In the Buy tab, review the terms and conditions, then click **Create**.

Your Virtual Advanced Threat Defense will now deploy. You can access the VMs through their respective public IPs.

- **SSH access** – Virtual Advanced Threat Defense VMs uses port 2222 for SSH access. Ensure that port 2222 is not blocked. Alternatively, you can have another machine in Azure cloud (ssh port 22) that acts as an intermediate, using which you can SSH into Advanced Threat Defense VMs.

- **Load balancing Advanced Threat Defense VMs on Azure** – The procedure for load balancing your VMs on Azure remains the same as for the appliance or Virtual Advanced Threat Defense.

  - Ensure that you give the private IP address of your primary and secondary node VMs.
  - On Azure, only Primary and Secondary Nodes are supported. Backup node is not supported.

  As an alternate, we support Azure Load Balancer. For more information on how to configure the Load Balancer, see *McAfee Advanced Threat Defense 4.2 Product Guide*.

### Create an analyzer VM on Azure

During dynamic analysis, Advanced Threat Defense executes suspicious files in the analyzer VM, then monitors the file behavior for malicious activities.

**Before you begin**

Ensure that the Windows sandbox images you use is available on the Azure Marketplace.

- You can also install Windows to the VM using your own Windows copy and license.

**Task**

1 Log on to your Azure Portal ([https://portal.azure.com](https://portal.azure.com)) and search for a Windows operating system.

2 Click on the Windows operating system, then click **Create**.

3 In Basics, do the following:
   a Type a name for your VM.
   b In VM Disk type, choose a disk type for your VM.
   c Set a user name and password for your VM.
   d Choose the appropriate subscription.
   e Choose the resource group and location.

4 In Size, choose a size of your choice.

5 In Settings, set the VM settings according to your choice.

6 In Purchase, click **Purchase** and then wait for the VM to deploy and start.
Prepare your sandbox virtual machine
Prepare your Windows environment to capture malware behaviors in the sandbox.

**Task**
1. Connect to your VM using Remote Desktop Connection and log on to your VM.
2. Open Local Users and Groups from the Control Panel.
3. In the left page, click Users.
4. In the right page, select a user and rename it to Administrator.
5. Set the Administrator password to cr@cker42.
6. Restart your VM.
7. Log on to your VM, then open Control Panel | System | Advanced system settings.
8. In the Advanced Tab of the System Properties window, under Performance, select Settings....
9. In the Performance Options windows, select Advanced | Change....
10. In the Virtual Memory windows, select Automatically manage paging file size for all drives, then click OK.
11. Install and configure Adobe Reader.
   a. To analyze PDF files, download Adobe Reader to the native host and install it to the VM.
   b. In Adobe reader, if Adobe Reader Protected Mode message appears, click Open with Protected Mode disabled, then click OK.
   c. If Accessibility Setup Assistance message appears, click Cancel.
   d. Select Edit | Preferences | Updater, select Do not download or install updated automatically, select OK, then select Yes to confirm the changes.
12. Install and configure Java.
   a. Open Registry Editor.
   b. Navigate to HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\JavaSoft\Java Update\Policy\EnableJavaUpdate.
   c. Set its value to 0.
   d. Close the Registry Editor.
13. Install and configure Adobe Flash Player.
   a. Run the command prompt as an Administrator.
   b. Execute the following command:
      ```
      dism.exe /online /add-package /packagepath:"<Adobe-Flash-For-Windows-Package>.mum"
      ```
      Replace <Adobe-Flash-For-Windows-Package> with the name and path of the Adobe Flash for Windows package MUM file.
14. Run the VM Provisioner Tool.
15. Shrink the volume to about between 20 GB and 30 GB and leave the rest unallocated.
16 Download Disk2vhd and extract it on your VM.
   
   You can download Disk2vhd from:
   https://docs.microsoft.com/en-us/sysinternals/downloads/disk2vhd

17 Run the extracted disk2vhd.exe file.

18 Select your primary drive, then click Create.

19 After, the VHDX file is created reduce its virtual size.
   
   a Open PowerShell.
   b Run the following command:
   
   ```bash
   Resize-VHD -Path <path to your vhdx file> -ToMinimumSize
   ```

   Resize-VHD command is available only on systems with the Hyper-V module.

20 Convert your VHDX file to an image file.
   
   For details about how to convert your VHDX file to an image file, see McAfee Advanced Threat Defense Product Guide

**Activate the product**

Activate your McAfee Virtual Advanced Threat Defense software using a temporary or permanent license key.

**Before you begin**

Obtain the license key and grant number from the McAfee order fulfillment team at licensing@mcafee.com.

McAfee Virtual Advanced Threat Defense supports these license key types:

- **30-days trial key** — A temporary license valid for 30 days is obtained on the initial purchase of the product. This license is based on the version of the McAfee Virtual Advanced Threat Defense software that you install.

- **Permanent license key** — A permanent license is purchased for a certain period. At the time of purchase, you can provide the end date of the permanent license. This license is based on the system ID of the McAfee Virtual Advanced Threat Defense instance.

You also need the grant number to activate your product.

**Tasks**

- **Activate the product using the temporary key** on page 36
  
  Activate your McAfee Virtual Advanced Threat Defense software using the temporary license key.

- **Activate the product using the permanent key** on page 37
  
  Obtain a permanent license key and activate your McAfee Virtual Advanced Threat Defense software.

**Activate the product using the temporary key**

Activate your McAfee Virtual Advanced Threat Defense software using the temporary license key.
Task

1. Save temporary license key file to desktop and make a note of grant number from the grant email.
2. Log on to the McAfee Virtual Advanced Threat Defense interface. When you log on for the first time, you would see a message box requesting to activate Advanced Threat Defense instance with a license. Click OK to close the box or click Help for further assistance.
3. Select Manage | ATD Configuration | Licensing.
4. Click Browse, locate and select the temporary license file, then click Open.
5. Type the grant number, then click Activate. Once the process is complete, the license details appear in the License Information section.
6. Check whether:
   1. The license status is Activated.
   2. The validity date is correct.

Activate the product using the permanent key
Obtain a permanent license key and activate your McAfee Virtual Advanced Threat Defense software.

Task

1. Obtain the system ID from the command line interface or web-interface of the McAfee Virtual Advanced Threat Defense software instance.

   Command line interface
   1. Log on to the command line interface with a valid user name.
      The default user name is cliadmin and password is atdadmin.
   2. Run show system id.
   3. From the result, make a note of the System ID from the result.

   Web-interface
   1. Log on to the McAfee Virtual Advanced Threat Defense interface.
   2. Select Manage | ATD Configuration | Licensing | Licensing
   3. From the License Information section, make a note of the Device System ID.
2 Send an email with the System ID to the McAfee order fulfillment team at licensing@mcafee.com.
You can send System IDs of all McAfee Virtual Advanced Threat Defense instances of your purchased SKUs.

<table>
<thead>
<tr>
<th>McAfee Virtual Advanced Threat Defense model</th>
<th>Number of McAfee Virtual Advanced Threat Defense installations</th>
<th>Number of McAfee Virtual Advanced Threat Defense VMs (8 per installation)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1008</td>
<td>1</td>
<td>8</td>
</tr>
<tr>
<td>1016</td>
<td>2</td>
<td>16</td>
</tr>
<tr>
<td>3032</td>
<td>4</td>
<td>32</td>
</tr>
<tr>
<td>6064</td>
<td>8</td>
<td>64</td>
</tr>
</tbody>
</table>

3 After you receive an email with the grant number and license key, register your product on the Manage | ATD Configuration | Licensing page.

4 Click Browse, locate and select the permanent license file, then click Open.

5 Type the grant number, then click Activate.
   Once the process is complete, the license details appear in the License Information section.

6 Check whether:
   1 The license status is Activated.
   2 The validity date is correct.
   3 The system ID is correct.

### Install Email Connector

Email connector is not installed with the Advanced Threat Defense software. You need to install this feature separately, then configure your email gateway to send emails to Advanced Threat Defense for analysis.

Ensure that your appliance does not have an existing atdec user account. This user account is dedicated for Email Connector to communicate with Advanced Threat Defense.

**Task**

1 Download systemex-4.x.x.xx.xxxxx.msu from the McAfee download portal.

2 Upload the package to the appliance using SFTP with the atdadmin account.

3 Log on to the Advanced Threat Defense web interface.

4 On the right pane, select Image & Software | Software.
5 In the Manage tab, under System Software section, from the drop-down select systemex-4.x.x.xx.xxxxxx.msu.

6 Click Install, then follow the on-screen instructions to complete the installation.

- If you have configured a cluster, ensure that you install Email connector in your primary as well as the secondary or back up nodes.
- The Advanced Threat Defense dashboard shows the Systemex version number under the System information monitor. To configure email connector, see McAfee Advanced Threat Defense Product Guide.
Installing the OS, software, and Email Connector
Install Email Connector
Accessing the Advanced Threat Defense web interface

The Advanced Threat Defense web interface is hosted on the Advanced Threat Defense Appliance. You can access the Advanced Threat Defense web interface from a remote machine using a supported browser.

Contents
- McAfee Advanced Threat Defense client requirements
- Log on to the Advanced Threat Defense web interface

McAfee Advanced Threat Defense client requirements

The following are the system requirements for client systems connecting to the Advanced Threat Defense web application.

- Client operating system — Microsoft Windows XP, Microsoft Windows Server 2003, Microsoft Windows Server 2008, Microsoft Windows 7, and Microsoft Windows 8.0
- Browsers — Internet Explorer 10 and 11, Google Chrome 40.0.2214.115 to 48.0.2564.116, and Mozilla Firefox 36.0.4 to 44.0.

Browser settings for HTML5 support

User-interactive mode (XMode) is used for activation of VM images and manual submission of files. This mode works with any browser that support HTML5 Canvas. You do not need to install Java to use the XMode feature.

Google Chrome version 44.0.2403 and higher and Mozilla Firefox version 40.0.3 and higher are supported. Microsoft Internet Explorer is not supported.

You need to modify Firefox settings to use the HTML5 feature.

1. From the Firefox Home page, click Options | Advanced | Certificates | View Certificates.
2. From the Certificate Manager window, click Servers.
3. Click Add Exception... and type https://<Host ATD IP address>:6080 and click Get Certificate.
4. Click Confirm Security Exception and then OK.
5. Click Activation or XMode.
Security settings for Internet Explorer

When you try to access the web application, you might see the *ActiveX control unsafe* pop-up dialog box. Perform these steps to resolve this issue.

1. On your system, search for **Edit Group Policy**. The Local Group Policy Editor window is displayed.

2. From the **Local Computer Policy** tree, go to **Computer Configuration | Administrative Templates | Windows Components** and click **Internet Explorer**.

3. In the right window options, double-click **Turn off the Security Settings Check feature** and select **Enabled**.

4. Click **Apply** and then **OK**.

Log on to the Advanced Threat Defense web interface

To log on to the Advanced Threat Defense web interface for the first time, use the default credentials.

**Task**

1. Open your Internet browser, then use the following to log on to the Advanced Threat Defense web interface:
   - **URL** — https://<Advanced Threat Defense Appliance host name or IP address>
   - **Login ID** — admin
   - **Password** — admin

2. Click **Log In**.

3. Change the default password.
Manage users and performance

Contents
- Manage users
- Add users
- Types of users
- Administrator permissions
- Upgrade the software and Android analyzer VM
- View the Upgrade log

Manage users
Create McAfee Advanced Threat Defense users accounts that assign specific permissions and configuration settings to users in your network.

Add users
Create accounts for users on your network, then assign them permissions.

Task
1. Log on to the Advanced Threat Defense web interface.
2. Click Manage | ATD Configuration | ATD Users, then click New.
3. Configure the user options, then click Save.
   
   You can create up to 128 users on Advanced Threat Defense.

Types of users
To manage Advanced Threat Defense and its integrated products, Advanced Threat Defense uses different user accounts. These user accounts have different sets of administrator responsibilities. For example, the Super administrator user is responsible to configure the Advanced Threat Defense web interface, manage user accounts, and perform software upgrades. The Network Security Platform user is responsible to integrate Network Security Platform with Advanced Threat Defense.

You cannot change the username for these accounts.
Command-line Interface user
To use the Command-line Interface (CLI), you need to log on to CLI using the user cliadmin credentials. Command-line Interface administrator uses the following credentials:
• username — cliadmin
• default password — atdadmin

Super Administrator
You create the Super Administrator account when you install Advanced Threat Defense and log on to the web interface.
The Super Administrator manages the following:
• Initially configure the Advanced Threat Defense web interface
• View and edit all Advanced Threat Defense user accounts
• Schedule database backups
• Software upgrades
Super Administrator uses the following credentials:
• username — admin
• default password — admin

Network Security Platform user
The Network Security Platform user has access to integrate Network Security Platform with Advanced Threat Defense.
Network Security Platform user uses these credentials:
• User name — nsp
• Password — admin

Upload Administrator
The Upload Administrator accesses the Advanced Threat Defense FTP server.
Upload Administrator uses the following credentials:
• User name — atdadmin
• Password — atdadmin

Web Gateway user
Web Gateway users integrate Web Gateway with Advanced Threat Defense.
Web Gateway user uses the following credentials:
• username — mwg
• default password — admin

Email Gateway user
Email Gateway users integrate McAfee Email Gateway with Advanced Threat Defense.
As the McAfee Email Gateway user, you can view and edit the user account.
To edit other accounts, contact your administrator.
Email Gateway user uses the following credentials:
• username — meg
• default password — admin

**TIE user**
TIE users integrate TIE with Advanced Threat Defense.
TIE user uses the following credentials:
• username — tie
• default password — admin

**Virtual Network Security Platform user**
Network Security Platform user uses the following credentials:
• username — vnsp
• password — admin

**Email connector user**
The Email Connector user atdec is used by the Advanced Threat Defense software to communicate with Email Connector and analyze email attachments. As an Advanced Threat Defense user, you do not have to use atdec for any configuration or access.

**Bro Network Sensor user**
Bro user integrates Advanced Threat Defense with one or more Bro Network Sensors. The users are also responsible for submitting files for analysis.

- While you create a Bro user, ensure that you select BRO is user type.
- In a scenario where your Advanced Threat Defense is communicating with multiple Bro Network Sensors, we recommend you create separate Bro users for each Bro Network Sensor.

Bro users can use the following default user credentials or create new users with the BRO user type.
• username—bro
• password—admin
Administrator permissions

You can give permissions to administrators that enable them to access different settings.

**Admin User**
Administrators with **Admin User** permissions have access to all of the settings on the Advanced Threat Defense web interface.

- Create and manage users
- Grant users access to the FTP server
- Access the Advanced Threat Defense web interface RESTful APIs
- Upgrade the Advanced Threat Defense software
- Upgrade the Android analyzer VM
- Convert VMDK or VHDX files to images files
- Manage image files
- View all of the analyzer profiles in the database
- Enable Internet access to samples
- LDAP authentication
- Configure date and time settings
- View the status of all submitted files

**Web Access**
Administrators with the **Web Access** permission have access to the malware analysis capabilities.

- Submit files for analysis only for the analyzer profiles that the Web Access role administrators create
- View the analysis results
- Edit the **Web Access** Administrator accounts
- Create analyzer profiles

**Restful Access**
Administrators with **Restful Access** permissions have access to the RESTful APIs.

- Upload files using the RESTful APIs
- Edit the **Restful Access** account

For more information, see the *McAfee Advanced Threat Defense RESTful APIs Reference Guide*.

**FTP Access permission**
Administrators with **FTP Access** permissions upload the files to the FTP server hosted on the Advanced Threat Defense Appliance.

For **FTP Access**, logon to your Advanced Threat Defense Appliance as atdadmin.
Upgrade the software and Android analyzer VM

Upgrade the Advanced Threat Defense software and Android analyzer VM to the latest versions.

Best practice: Upgrade the Advanced Threat Defense software to the latest version.

When you upgrade the Advanced Threat Defense software:
- You are unable to use the system.msu files to downgrade the Advanced Threat Defense software.
- OpenSSL automatically upgrades.

Prepare for the upgrade

Prepare your environment to upgrade the Advanced Threat Defense software and Android analyzer VM.

Task

To complete a successful upgrade, you must already use Advanced Threat Defense 3.4.8 or later.

1. Log on to the Advanced Threat Defense web interface.

2. Change the administrator account settings.
   a. Click Manage | ATD Configuration | ATD Users.
   b. Select the Advanced Threat Defense administrator, then click Edit.
   c. In the User Credentials configuration area, select Allow Multiple Logins.
   d. In the Roles configuration area, select Web Access.

3. On the LDAP server, make sure the gidNumber value is 1024 for the atdadmin user.

4. Make sure that you have the following logon credentials.
   - Advanced Threat Defense web interface administrator account
   - The Advanced Threat Defense CLI using SSH
   - The SFTP credentials to the Advanced Threat Defense Appliance

Download the product files

Download the Advanced Threat Defense product files from McAfee Downloads page.

Task

1. Go to the McAfee Downloads page.

2. Enter the Grant Number, the letters or numbers displayed, then click Submit.


4. Click and download the installation files to your client computer.

Complete the upgrade

Upgrade the Advanced Threat Defense software and Android analyzer VM to the latest version.
Task

1 Use an FTP client, such as Filezilla, to log on to the Advanced Threat Defense Appliance. Log on as the atdadmin user.

2 Using SFTP, upload these files to the Advanced Threat Defense root directory:
   - Installation file
   - Android .msu file
   Make sure that the transfer mode is binary.

3 Use the following to upgrade the Advanced Threat Defense software, then repeat these steps to upgrade the Android analyzer VM.
   a Log on to the Advanced Threat Defense web interface as the administrator.
   b Click Manage | Image & Software | Software.
   c From the System Software drop-down list, select the file.
   d Make sure that Reset Database is deselected, then click Install.
   e On the installation Status message, click OK.
      If you are unable to view the installation Status message, delete the browser cache.
      The installation takes a minimum of 20 minutes.
      When the installation completes, the Advanced Threat Defense Appliance restarts.
   f On the reboot Status message, click OK.
      If you are unable to view the reboot Status message, delete the browser cache.

4 When the Advanced Threat Defense Appliance starts, log on to the CLI and verify the software version.

5 Log on to the Advanced Threat Defense web interface and verify the following.
   • Software version
   • All data and configuration settings are transferred from the previous Advanced Threat Defense installation

6 Click Dashboard, then verify that the VM Creation status is Successful on the VM Status monitor.
   Advanced Threat Defense automatically re-creates all analyzer VMs. The amount of time it takes to re-create the analyzer VMs depends on the number of analyzer VMs configured in Advanced Threat Defense.

The Advanced Threat Defense Appliance stores the software version on the active disk.
When you upgrade the software, Advanced Threat Defense disables the Whitelist status.

View the upgrade log
When you upgrade Advanced Threat Defense, you can view the upgrade path and version history logs.

Task

1 Log on to the Advanced Threat Defense web interface.

2 Click Manage | Logs | Upgrade.
Upgrade the software incrementally

Upgrade the Advanced Threat Defense software to an available patch version.

This application software upgrade option provides an incremental upgrade of the software to an available patch version. For a complete upgrade of the software, you need to download the software from the McAfee Downloads page. See the respective sections for detailed instructions on the tasks.

Upgrading the application software also upgrades the detection packages. You would not see any previously installed detection packages after this upgrade. Also, the system services and system might restart during the application software upgrade process.

When updates are available for the application software and detection software package, notification messages appear in the toolbar of the Advanced Threat Defense interface.

Tasks

- **Automatically download the latest application software package on page 49**
  Automatically download and install the latest application software in Advanced Threat Defense Appliance.

- **Manually upload the latest application software package on page 49**
  Manually upload and install the latest application software in Advanced Threat Defense.

**Automatically download the latest application software package**

Automatically download and install the latest application software in Advanced Threat Defense Appliance.

**Task**

1. Log on to the Advanced Threat Defense web interface, then do one of these to access the Incremental Updates page.
   - Click **Click to Update Software** from the header.

   ![When multiple notifications are available, select Click to Update Software from the list of notifications.]

   - Click **Manage | Image & Software | Incremental Updates**.

2. Under **Automatic Update**, select **Application Software**, then click **Apply**.

3. Select the **Application Software** tab, then click **Install** against the available software version.

   A confirmation message appears before the installation starts. All Advanced Threat Defense services are restarted. Once the process is complete, a status message appears that provides information about a successful upgrade and a suggestion to log on again to the Advanced Threat Defense interface.

4. Log on to the Advanced Threat Defense interface again, then validate whether the upgrade was successful.

   - From the header on Advanced Threat Defense interface, .

   - Verify that the version is listed as **Current**: Click **Manage | Image & Software | Incremental Updates**, then click the **Application Software** tab.

   In case of any issues with the upgrade, click **Revert** to reverse the software to the previous backed-up version. You won't see the **Revert** option if Advanced Threat Defense software has been upgraded using system.msu.

**Manually upload the latest application software package**

Manually upload and install the latest application software in Advanced Threat Defense.

Advanced Threat Defense allows you to import a maximum of two versions of the application software. The latest uploaded version is the **Current** upload by default, and renders the previous upload as **Backup**.
Task

1 Log on to the Advanced Threat Defense web interface.

2 Click Manage | Image & Software | Incremental Updates.

3 To download the application software package, contact Support.

4 On the Incremental Updates page, click Browse, then select the application software package.

5 Click Upload.
   To reinstate the Backup file as the Current file, click Revert.

Upgrade the Android analyzer VM

Using the Advanced Threat Defense web application, you can upgrade the Android analyzer VM.

Task

1 Log on to the Advanced Threat Defense Appliance using an FTP client such as FileZilla.
   Log on as the atdadmin user.

2 Using SFTP, upload the Android MSU file to the root directory of Advanced Threat Defense.
   Make sure that the transfer mode is binary.

3 After the file is uploaded, log on to the Advanced Threat Defense web application as the admin user and select Manage | Software Management.

4 Under System Software, select the Android MSU file, then click Install.
   Ensure that Reset Database is not selected.

5 Click OK on the confirmation message.
   Advanced Threat Defense web application closes logs out automatically and the status of the installation is displayed in the browser.
   • It takes a minimum of 20 minutes for the system software installation to complete.
   • If you are not able to view these messages, clear the browser cache.
   • When you upgrade Android, the default Android analyzer VM is automatically re-created. This process might take a few minutes to complete.

6 Log on to the web application, and select Manage | System Log.

7 In the System Log page, verify that the vmcreator task is successfully completed for the Android analyzer VM.

View the Upgrade log

To upgrade the McAfee Advanced Threat Defense software version, view the upgrade path and version history logs.

The upgrade log displays details like the current software version, the previous software version, system details.

Following is a sample upgrade log:

Sun Apr 3 05:04:08 PDT 2016 Following version of software are installed
amas build version: 3.6.0.14.55351
android build version 5.0
av-gti: release 3.4.2.32.43041
avengines: release 3.4.2.32.43041
linux-xen: release 3.4.8.96.50610
system-config: release 3.4.2.32.43041
avlabS-xp-v3-3.6.0.13.55348.msi
avlabS-64-v3-3.6.0.13.55348.msi

To view the Upgrade log, go to Manage | Logs | Upgrade.
Manage users and performance
View the Upgrade log
Creating analyzer VMs

Advanced Threat Defense uses secure virtual machines, or analyzer VMs, for dynamic analysis. During dynamic analysis, Advanced Threat Defense executes suspicious files in the analyzer VM, then monitors the file behavior for malicious activities.

The number of analyzer VMs you can create is limited by the following conditions:
- the available Advanced Threat Defense Appliance disk space.
- the disk space occupied by the operating system.

Advanced Threat Defense limits the maximum number of analyzer VMs you can use for analysis.
- ATD-3000 — 29 analyzer VMs
- ATD-6000 — 59 analyzer VMs
- ATD-3100 — 29 analyzer VMs
- ATD-6100 — 59 analyzer VMs

The number of concurrent licenses that you specify affects the number of concurrent active analyzer VMs.

Any security software or low-level utility tool on an analyzer VM can interfere with the dynamic analysis of the sample file. The sample-file execution can be terminated during dynamic analysis. As a result, the reports might not capture the full behavior of the sample file. If you need to find out the complete behavior of the sample file, do not patch the operating system of the analyzer VM or install any security software on it.

Contents
- Create a VM using the VM Builder
- Create a virtual machine on VMWare ESXi
- Create a virtual machine on Hyper-V Manager
- Create a virtual disk file
- Install Microsoft Office on the virtual machine
- Enable PDF file analysis
- Enable JAR file analysis
- Enable Flash file analysis
- Complete the VMDK and VHDX file creation process
- Prepare the virtual disk image for analysis
- Import the virtual disk file
- Convert the VMDK and VHDX file to an image file
- Managing VM profiles
Create a VM using the VM Builder

The VM Builder makes it easier for you to create VMs for VMware ESXi. The tool allows you to include all needed installers and OS ISO, then seamlessly create VMs for you.

**Before you begin**
- Enable SSH on ESXi 6.0 Server.
- Add the following USB Pass-through and reboot ESXi:
  - C600/X79 series chipset USB2 Enhanced Host Controller #1
  - C600/X79 series chipset USB2 Enhanced Host Controller #2
- Copy the following installers to a USB drive. Ensure that the USB driver is formatted with NTFS file system.
  - Adobe Reader
  - Adobe Flash Player
  - Java
  - Microsoft Office
  - Microsoft Visual C++ Redistributable
  - Web browser (Internet Explorer, Chrome, or Firefox)
- Upload the Windows ISO to the ESXi Datastore.
- Download and install Visual C++ 2012 Redistributable (x86) on your local system.

**Task**
1. Download the VM Builder tool:
   a. Log on to Advanced Threat Defense.
   b. Click Manage | Image & Software | Image, then click Download VM Builder Tool.
2. Run the VM Builder Tool as an Administrator.
3. Type the IP address, user name, password, and port of your ESXi, then select the checkbox.
4. Click Test SSH Connection, and then click Next.
   If you are prompted to store the RSA2 key fingerprints, type 'y' and press enter.
5. From the drop-down, select the Datastore from the list, then click Fetch ISO.
   The tool fetches all datastore from $/vmfs/volumes/ on ESXi.
6. From the list of Windows ISO, select an ISO for your Windows VM.
7. From the drop-down, select the OS corresponding to the ISO that you have selected, then click Select OS.
8. Change the VM name if needed, then click Check Availability, click Next.
9. Use the browse icon to select the USB drive where you have copied the installer files.
Choose the installer for the corresponding software.

- Visual C++ 2012 Redistributable (x86) must be installed.
- All installers must be offline installers.
- All installers must be compatible with the respective operating systems.

If you do not want to install any of the other software except VC++, you can leave the respective field blank.

Click Next to continue.

Type the License key for Microsoft Windows and Office, then click Next.

- License key for Windows 10 and Windows Server Edition is mandatory.
- Office is activated automatically only if you enter the license key. An Internet connection is required for activation.

Review the Summary, click Create VM.

Ensure that you connect your USB to the VM in 10 seconds of the VM creation.

Open vSphere Client, and select the VM that you create using VM Builder.

From the toolbar, click the USB icon, and select your USB drive.

Once the USB is connected, your Windows OS automatically begins installation.

If you could not connect the USB drive to the VM in 10 Sec, the VM Builder prompts you to reset the VM. Click Yes and the VM gets reset. Now connect the USB in 10 secs.

- Once the virtual machine is created, the VM Provisioner tool executes automatically. After the VM Provisioner tool completes the checks, review the VM Provisioner log on the C drive of the virtual machine. If you see any issues, correct them and run VM Provisioner tool again.
- If the network is disconnected while the USB is connected to VM, the USB might crash.
  Solution: Restart your local system. You might lose some settings on your VM.
- vSphere Client takes a long time to connect the USB drive.
  Solution: Log on again to vSphere Client, then connect the USB, and reset the VM.

Create a virtual machine on VMWare ESXi

To create the virtual machine, you must complete the New Virtual Machine Wizard.

Task
1. Make sure you have your operating system ISO image and license key.
2. Download and install VMware ESXi 6.0 or 6.5.
3. Start the VMware ESXi.
5 Configure the following options, then click Next on each page.

<table>
<thead>
<tr>
<th>Section name</th>
<th>Configuration options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration</td>
<td>Select Custom.</td>
</tr>
<tr>
<td>Name and Location</td>
<td>Type a name for your virtual machine.</td>
</tr>
<tr>
<td>Resource Pool</td>
<td>Select a resource pool within which you wish to run your virtual machine.</td>
</tr>
<tr>
<td>Storage</td>
<td>Select a location where you’d want to store your virtual machine.</td>
</tr>
<tr>
<td>Virtual Machine Version</td>
<td>Select a virtual machine version to use.</td>
</tr>
<tr>
<td></td>
<td>• For the other platforms choose Virtual Machine Version: 9.</td>
</tr>
<tr>
<td>Guest Operating System</td>
<td>Select the operating system and its version that you plan to install on this virtual machine.</td>
</tr>
<tr>
<td>CPUs</td>
<td>Select the number of CPUs for your virtual machine. We recommend you use the default values.</td>
</tr>
<tr>
<td>Memory</td>
<td>Select an appropriate RAM size for your virtual machine.</td>
</tr>
<tr>
<td>Network</td>
<td>Select the number of network cards for the virtual machine and choose what network it can connect to. We recommend you choose E1000 virtual NIC.</td>
</tr>
<tr>
<td>SCSI Controller</td>
<td>Select LSI Logic SAS.</td>
</tr>
<tr>
<td>Select a Disk</td>
<td>Select Create a new virtual disk.</td>
</tr>
<tr>
<td>Create a disk</td>
<td>Set an appropriate disk space, then select Thin Provision.</td>
</tr>
<tr>
<td>Advanced Options</td>
<td>In Virtual Device Node, select IDE (0:0).</td>
</tr>
<tr>
<td>Ready to Complete</td>
<td>Review the settings you of your new virtual machine. Select Edit the virtual machine settings before, then click Continue.</td>
</tr>
</tbody>
</table>

6 Select your new virtual machine, then click Edit virtual machine settings.

7 In the Virtual Machine Properties page, do the following:
   • Select CD/DVD Drive1.
   • In Device Status, enable Connect at power on.
   • In Datastore ISO File, use Browse to provide the location of the operating system you plan to install in your virtual machine.
   • In Virtual Machine Node, select IDE (1:0).

8 Click Finish.

Create a virtual machine on Hyper-V Manager

This topic explains how to create a virtual machine in Microsoft Hyper-V Manager.

Before you begin
Ensure that you have enabled Hyper-V (including Hyper-V Management Tools and Hyper-V Platform) from Control Panel | Programs and Features | Turn Windows features on or off | Hyper-V.
Advanced Threat Defense does not support the following operating systems on Hyper-V:

- Microsoft Windows XP
- Microsoft Windows Server 2003
- Microsoft Windows 8 32-bit

**Task**

1. Open Hyper-V Manager, then from the **Actions** pane, select **New | Virtual Machine**.
2. Type a name for your virtual machine, then click **Next**.
   You can also choose to store your virtual machine at an alternate location.
3. In the **Specify Generation** section, choose **Generation 1**.
4. In the **Assign Memory** section, type the appropriate RAM size.
5. In the **Configure Networking** section, choose a virtual switch.
6. In the **Connect Virtual Hard Disk** section, select **Create a virtual hard disk**.
   a. Type a name for the hard disk.
   b. Specify the location where you want to save the VHDX file.
   c. Type an appropriate size for the hard disk, then click **Next**.
7. In the **Installation Options** section, select **Install an operating system from a bootable CD/DVD-ROM**.
8. Select **Image file (.iso)**, then browse and select the image file, then click **Next**.
9. In the **Summary page**, review the settings, then click **Finish**.
Create a virtual disk file

Create a virtual disk file of the ISO image on VMWare or Hyper-V.

Tasks

- **Create a virtual disk file for Windows 7 on page 58**
  If you are using Windows 7, use the following steps to create the virtual disk file.

- **Create a virtual disk file for Windows 8 on page 59**
  If you are using Windows 8, use these steps to create the virtual disk file.

- **Create a virtual disk file for Windows XP on page 60**
  If you are using Windows XP, use the following steps to create the virtual disk file.

- **Create a virtual disk file for Windows Server 2003 on page 60**
  If you are using Windows Server 2003, use the following steps to create the virtual disk file.

- **Create a virtual disk file for Windows Server 2008 on page 61**
  If you are using Windows Server 2008, use the following steps to create the virtual disk file.

- **Create a virtual disk file for Windows 8.1 on page 62**
  If you are using Windows 8.1, use these steps to create the virtual disk file.

- **Create a virtual disk file for Windows 10 on page 63**
  If you are using Windows 10, use these steps to create the virtual disk file.

- **Create a virtual disk file for Windows 10 version 1703 (Redstone 2) on page 63**
  If you are using Windows 10 version 1703 (Redstone 2), use these steps to create the virtual disk file.

- **Create a virtual disk file for Windows 2012 on page 64**
  If you are using Windows 2012, use these steps to create the virtual disk file.

- **Create a virtual disk file for Windows 2012 R2 on page 65**
  If you are using Windows 2012 R2, use these steps to create the virtual disk file.

- **Create a virtual disk file for Windows Server 2016 Standard on page 65**
  If you are using Windows Server 2016 Standard, use these steps to create the virtual disk file.

Create a virtual disk file for Windows 7

If you are using Windows 7, use the following steps to create the virtual disk file.

Task

1. From the installation wizard, select the language, time and currency format, keyboard or input method, then click **Next**.

2. Click **Install Now**, then click **Next**.

3. Accept the license terms, then click **Next**.

4. On the Windows Setup page, select **Custom: Install Windows only (advanced)**, leave the default disk space settings, then click **Next**.

5. Use the following credentials to create an account:
   - **User name** — administrator
   - **Password** — cr@cker42

6. In the **Removable Devices** window, select **Do not show this hint again**, then click **OK**. The Windows installation can take up to 15 minutes.
7 In the **Set Network Location** window, select **Public Network**, then close the window.

8 Download and install Microsoft .NET Framework 4.6.1.

**Create a virtual disk file for Windows 8**

If you are using Windows 8, use these steps to create the virtual disk file.

**Task**

1. From the installation wizard, select the language, time and currency format, keyboard or input method, then click **Next**.

2. Click **Install Now**, then click **Next**.

3. Accept the license terms, then click **Next**.

4. On the Windows Setup page, select **Custom: Install Windows only (advanced)**, leave the default disk space settings, then click **Next**.

5. In the Settings window, select **Use Express settings**.

6. In sign in to your PC, select **Sign in without a Microsoft Account**, then select **Local Account**.

7. Use the following credentials to create an account:
   - **User name** — administrator
   - **Password** — cr@cker42

8. Configure Adobe Reader as the default application to open PDF files.
   a. Open the **Control Panel**, then select **Programs | Default Programs | Associate a file type or protocol with a program**.
   b. Double-click **.pdf**, then select **Adobe Reader**.
   c. Click **Close**.

9. In the **Removable Devices** window, select **Do not show this hint again**, then click **OK**.

   The Windows installation can take up to 15 minutes.

10. To log on to the virtual machine Image, use these credentials:
    - Administrator
    - cr@cker42

11. To switch to desktop mode, click the desktop tile.

Create a virtual disk file for Windows XP
If you are using Windows XP, use the following steps to create the virtual disk file.

Task
1 Complete the Windows XP setup.
   a On the **Setup cannot continue until you enter your name. Administrator and Guest are not allowable names to use** message, click **OK**.
   b In the **Windows XP Professional Setup** window, enter the following, then click **Next**.
      • Name — root
      • Organization — Leave blank.
   c If prompted, log on to virtual machine image with the following credentials.
      • User — administrator
      • Password — cr@cker42

2 In the **Virtual Machine Settings** window, select **CD/DVD (IDE)**.

3 Next to the **Use ISO image file** field, click **Browse**, locate the ISO file, then click **OK**.

4 Download and install the following Redistributable Packages and .NET Framework.
   • Microsoft Visual C++ 2005 Redistributable Package (x86)
   • Microsoft Visual C++ 2008 Redistributable Package (x86)
   • Microsoft Visual C++ 2010 Redistributable Package (x86)
   • Microsoft .NET Framework 3.5 Service Pack 1 (x86)

Create a virtual disk file for Windows Server 2003
If you are using Windows Server 2003, use the following steps to create the virtual disk file.

Task
1 In the VMware ESXi, turn on the virtual machine, then install Windows Server 2003.
   • This step can take up to 30 minutes.
   • To format the partition during installation, you can use the NTFS file system.

2 For each Windows setup window, configure the options, then click **Next**.

<table>
<thead>
<tr>
<th>Window name</th>
<th>Configuration options</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Regional and Language Options</strong></td>
<td>Configure the settings for your environment.</td>
</tr>
<tr>
<td><strong>Windows Setup</strong></td>
<td>Enter the following credentials:</td>
</tr>
<tr>
<td></td>
<td>• Name — root</td>
</tr>
<tr>
<td></td>
<td>• Organization — Leave blank</td>
</tr>
<tr>
<td><strong>Your Product Key</strong></td>
<td>Enter the product key.</td>
</tr>
<tr>
<td><strong>Licensing Modes</strong></td>
<td>Select <strong>Per Server</strong>, then enter the number of concurrent connections.</td>
</tr>
</tbody>
</table>
### Configuration options

<table>
<thead>
<tr>
<th>Window name</th>
<th>Configuration options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Computer Name and Administrator Password</td>
<td>Configure the following options:</td>
</tr>
<tr>
<td></td>
<td>• Computer name — Use the default value</td>
</tr>
<tr>
<td></td>
<td>• Administrator password — cr@cker42</td>
</tr>
<tr>
<td></td>
<td>• Confirm password — cr@cker42</td>
</tr>
<tr>
<td>Date and Time Settings</td>
<td>Use the default values.</td>
</tr>
<tr>
<td>Network Settings</td>
<td>Use the default values.</td>
</tr>
<tr>
<td>Workgroup or Computer Domain</td>
<td>Use the default values.</td>
</tr>
</tbody>
</table>

3. To log on to the virtual machine, use these credentials:
   - **User** — administrator
   - **Password** — cr@cker42

4. In the **Windows Server Post-Setup Security Updates** window, click **Finish**.

5. If you are using Windows Server 2003 SP1, complete the following.
   b. Restart your computer.
   c. On the command prompt, enter `tlntsvr /service`, then press **Enter**.

6. Download and install the following Redistributable Packages and .NET Framework.
   - Microsoft Visual C++ 2005 Redistributable Package (x86)
   - Microsoft Visual C++ 2008 Redistributable Package (x86)
   - Microsoft Visual C++ 2010 Redistributable Package (x86)
   - Microsoft .NET Framework 3.5 Service Pack 1 (x86)

### Create a virtual disk file for Windows Server 2008

If you are using Windows Server 2008, use the following steps to create the virtual disk file.

**Task**

1. From the installation wizard, select the language, time and currency format, keyboard or input method, then click **Next**.

2. Click **Install Now**, then click **Next**.

3. Accept the license terms, then click **Next**.

4. On the Windows Setup page, select **Custom (advanced)**, leave the default disk space settings, then click **Next**.

5. Set password for administrator account.

6. In the **Removable Devices** window, select **Do not show this hint again**, then click **OK**.
   The Windows installation can take up to 15 minutes.

7. In the **Initial Configuration Tasks** window, select **Do not show this window at logon**, then click **Close**.
8 Log on to the computer, then download the following packages:
   • Microsoft Visual C++ 2005 Redistributable Package (x86)
   • Microsoft Visual C++ 2008 Redistributable Package (x86)
   • Microsoft Visual C++ 2010 Redistributable Package (x86)
   • Microsoft .NET Framework 4.6.1

Create a virtual disk file for Windows 8.1
If you are using Windows 8.1, use these steps to create the virtual disk file.

Task
1 From the installation wizard, select the language, time and currency format, keyboard or input method, then click Next.
2 Click Install Now, then click Next.
   Installation process is completed in various stages. The setup is first initialized.
3 On the Activate Windows page, enter your Windows product key, or select I don't have a product key to activate it later, then click Next.
4 Accept the license terms, then click Next.
5 On the Windows Setup page, select Custom: Install Windows only (advanced), use the default disk space settings, then click Next.
   The step is completed in five stages. Wait for all stages to complete.
6 In the Settings window, select Use Express settings.
7 For the type of owner, select I own it, then click Next.
8 Asked to enter your Microsoft Account Details, select Skip this step.
9 Asked to create an account, use these credentials, then click Next.
   • User name — administrator
   • Password — cr@cker42
10 Asked about Cortana, select Not now.
11 Wait until the installation is complete, then install the required software.

Log on to your computer and make sure that these redistributable packages are installed.
   • Microsoft Visual C++ 2005 Redistributable Package (x86)
   • Microsoft Visual C++ 2008 Redistributable Package (x86)
   • Microsoft Visual C++ 2010 Redistributable Package (x86)
   • Microsoft .NET Framework 4.6.1
Create a virtual disk file for Windows 10
If you are using Windows 10, use these steps to create the virtual disk file.

Task
1  From the installation wizard, select the language, time and currency format, keyboard or input method, then click Next.

2  Click Install Now, then click Next.
   Installation process is completed in various stages. The setup is first initialized.

3  On the Activate Windows page, enter your Windows product key, or select I don't have a product key to activate it later, then click Next.

4  Accept the license terms, then click Next.

5  On the Windows Setup page, select Custom: Install Windows only (advanced), use the default disk space settings, then click Next.
   The step is completed in five stages. Wait for all stages to complete.

6  In the Settings window, select Use Express settings.

7  For the type of owner, select I own it, then click Next.

8  In the Make it yours window, select Skip this step.

9  In the Create an account for this PC window, use these credentials, then click Next.
   •  User name — admin
   •  Password — cr@cker42

10 In the Choose how you’ll connect window, select Join a local Active Directory domain.

11 In the Meet Cortana windows, select Not now.

12 Wait until the installation is complete, then install the required software.
Log on to your computer and make sure that these redistributable packages are installed.
   •  Microsoft Visual C++ 2005 Redistributable Package (x86)
   •  Microsoft Visual C++ 2008 Redistributable Package (x86)
   •  Microsoft Visual C++ 2010 Redistributable Package (x86)
   •  Microsoft Visual C++ 2012 Redistributable Package (x86)
   •  Microsoft .NET Framework 4.6.2

Create a virtual disk file for Windows 10 version 1703 (Redstone 2)
If you are using Windows 10 version 1703 (Redstone 2), use these steps to create the virtual disk file.

Task
1  From the installation wizard, select the language, time and currency format, keyboard or input method, then click Next.

2  Click Install Now, then click Next.
   Installation process is completed in various stages. The setup is first initialized.
3 On the Activate Windows page, enter your Windows product key, or select I don’t have a product key to activate it later, then click Next.

4 Accept the license terms, then click Next.

5 On the Windows Setup page, select Custom: Install Windows only (advanced), use the default disk space settings, then click Next.
   The step is completed in five stages. Wait for all stages to complete.

6 Choose United States in region, and in primary keyboard, select English (United States).

7 In the Settings window, select Use Express settings.

8 For the type of owner, select I do, then click Next.

9 In the Make it yours window, select Skip this step.

10 In the Meet Cortana windows, select Not now.

11 In the Choose how you’ll connect’ window, select Join a local Active Directory domain.

12 In the Create an account for this PC windows, use these credentials, then click Next.
   • User name — admin
   • Password — cr@cker42

13 In the Choose Privacy settings window, keep the default settings, then click Next.

14 Wait until the installation is complete, then install the required software.

Log on to your computer and make sure that these redistributable packages are installed.

• Microsoft Visual C++ 2005 Redistributable Package (x86)
• Microsoft Visual C++ 2008 Redistributable Package (x86)
• Microsoft Visual C++ 2010 Redistributable Package (x86)
• Microsoft Visual C++ 2012 Redistributable Package (x86)
• Microsoft .NET Framework 4.7

Create a virtual disk file for Windows 2012
If you are using Windows 2012, use these steps to create the virtual disk file.

Task
1 From the installation wizard, select the language, time and currency format, keyboard or input method, then click Next.

2 Click Install Now, accept the license terms, then click Next.

3 Select Custom Install Windows, Windows Server 2012 Datacenter, use the default disk space settings, then click Next.
   Installation process is completed in various stages.

4 Set password for administrator account.
Log on to the computer, then download and install the following redistributable packages and .NET framework.

- Microsoft Visual C++ 2005 Redistributable Package (x86)
- Microsoft Visual C++ 2008 Redistributable Package (x86)
- Microsoft Visual C++ 2010 Redistributable Package (x86)
- Microsoft .NET Framework 4.6.1

**Create a virtual disk file for Windows 2012 R2**

If you are using Windows 2012 R2, use these steps to create the virtual disk file.

**Task**

1. From the installation wizard, select the language, time and currency format, keyboard or input method, then click **Next**.
2. Click **Install Now**, accept the license terms, then click **Next**.
3. Select **Custom Install Windows, Windows Server R2 2012 Datacenter**, use the default disk space settings, then click **Next**.
   
   Installation process is completed in various stages.
4. Set password for administrator account.
5. Log on to the computer, then download and install the following redistributable packages and .NET framework.
   - Microsoft Visual C++ 2005 Redistributable Package (x86)
   - Microsoft Visual C++ 2008 Redistributable Package (x86)
   - Microsoft Visual C++ 2010 Redistributable Package (x86)
   - Microsoft .NET Framework 4.6.1

**Create a virtual disk file for Windows Server 2016 Standard**

If you are using Windows Server 2016 Standard, use these steps to create the virtual disk file.

**Task**

1. From the installation wizard, select the language, time and currency format, keyboard or input method, then click **Next**.
2. Click **Install Now**, accept the license terms, then click **Next**.
3. Select **Custom Install Windows, Windows Server 2016 Standard**, use the default disk space settings, then click **Next**.
   
   Installation process is completed in various stages.
4. Set password for administrator account.
5. Log on to the computer, then download and install the following redistributable packages and .NET framework.
   - Microsoft Visual C++ 2005 Redistributable Package (x86)
   - Microsoft Visual C++ 2008 Redistributable Package (x86)
Install Microsoft Office on the virtual machine

To install Microsoft Office on the virtual machine, you must download the compatibility pack from Microsoft.

Task
1. In the Microsoft Office Setup window, select the following options, then click Next.
   • Microsoft Word
   • Microsoft Excel
   • Microsoft PowerPoint
2. To open Microsoft Office files created in a newer version of Microsoft Office, install the compatibility pack.
   a. Download the required Microsoft Office compatibility pack for Word, Excel, and PowerPoint file formats.
   b. Install the compatibility pack on the virtual machine.
3. In the Compatibility Pack for the 2007 Office system window, select Click here to accept the Microsoft Software License Terms, then click OK.

Enable PDF file analysis

To analyze PDF files, download Adobe Reader to the native host and copy it to the VM.

Task
1. Install Adobe Reader on the virtual machine.
2. Open Adobe Reader, then click Accept on the License Agreement window.

Enable JAR file analysis

To analyze JAR files, download and install Java Runtime Environment (JRE).

Task
1. Download and install the Java SE Development Kit for your computer.
2. On your computer, click Start | Java | Configure Java.
3. On the Java Control Panel, click the Security tab.
4. Change the Security Level to Medium, then click OK.
Enable Flash file analysis

To dynamically analyze Flash files, install Adobe Flash Player or the Flash plug-in.

Task
1. Make sure that Internet Explorer is your default browser.
2. Install Adobe Flash Player or the Flash plug-in on your computer.
   • Download and install Adobe Flash Player, then verify that it is the default flash extension.
   • Download and install Adobe Flash plug-in, then verify that Shockwave Flash Object is enabled.

Complete the VMDK and VHDX file creation process

Task
1. Restart the virtual machine.
2. To shut down virtualMachineImage, select Start | Shut down.
3. Make sure there are not any stale lock files (.lck) associated with the virtual machine.
   The .lck files are located in the same folder as the .vmdk or .vhdx file.

Prepare the virtual disk image for analysis

Prepare your VMDK or VHDX images to capture malware behaviors in the sandbox environment.
We recommend that you run the VM Provisioner Tool that's available in the Advanced Threat Defense interface. However, if the tool doesn't work in your environment, you could also prepare your sandbox environment manually.

Tasks
• Run the VM Provisioner Tool on page 67
  Download the VM Provisioner Tool from the Advanced Threat Defense interface, then run the tool to prepare your virtual disk images to capture malware behaviors in the sandbox environment.
• Prepare your VMDK or VHDX image for analysis manually on page 68
  Prepare your environment manually to capture malware behaviors in the sandbox environment.

Run the VM Provisioner Tool

Download the VM Provisioner Tool from the Advanced Threat Defense interface, then run the tool to prepare your virtual disk images to capture malware behaviors in the sandbox environment. Run the VM Provisioner Tool after installing all required software on all Windows VM images that you create. The VM Provisioner Tool supports operating systems configured for the supported languages: English, Spanish, Japanese, Chinese (Simplified), German, French, Italian.
Creating analyzer VMs
Prepare the virtual disk image for analysis

Task
1. Log on to the Advanced Threat Defense interface.
2. Click Manage | Image & Software | Image.
3. Click Download VM Provisioner Tool.
4. Save the VM Provisioner Tool .exe file on your virtual machine.
5. Make sure that the Visual Studio 2012 C++ Redistributable is installed on the VM.
6. Open and run the VM Provisioner Tool .exe file.

   If the VM Provisioner Tool reports errors, perform the steps manually, then run the tool again to verify.

   To view the log file that contains all executed commands and changed registries, go to C:\VM_Provi.log.
   Before you shut down the virtual machine, copy the log file to another system (outside of the VM) for later reference, then remove the log file.

Prepare your VMDK or VHDX image for analysis manually
Prepare your environment manually to capture malware behaviors in the sandbox environment.

Tasks
• Prepare a Windows XP image for analysis on page 68
  Configure your Windows XP virtual system for analysis.
• Prepare a Windows Server 2003 image for analysis on page 71
  Configure your Windows Server 2003 virtual system for analysis.
• Prepare a Windows 7 image for analysis on page 74
  Configure your Windows 7 virtual system for analysis.
• Prepare a Windows Server 2008 image on page 77
  Configure your Windows Server 2008 virtual system for analysis.
• Prepare a Windows 8 image for analysis on page 79
  Configure your Windows 8 virtual system for analysis.
• Prepare a Windows 8.1 image for analysis on page 83
  Configure your Windows 8.1 virtual system for analysis.
• Prepare a Windows 10 or Windows 10 v1703 (Redstone 2) image for analysis on page 86
  Configure your Windows 10 virtual system for analysis.
• Prepare a Windows 2012 R2 image for analysis on page 90
  Configure your Windows Server 2012 R2 virtual system for analysis.
• Prepare a Windows Server 2016 Standard image for analysis on page 93
  Configure your Windows Server 2016 Standard virtual system for analysis.

Prepare a Windows XP image for analysis
Configure your Windows XP virtual system for analysis.
Task

1. Configure the virtual machine in VMware ESXi or Microsoft Hyper-V:
   a. Right-click on the Windows XP image, then select Settings.
   b. In the Virtual Machine Settings window, select CD/DVD (IDE).
   c. In Use ISO image file, browse to the ISO file that you used and click OK.
   d. In the Welcome to Microsoft Windows XP page, click Exit.

2. Log on to the virtual machine as administrator.

3. Turn off the firewall in the virtual image: Select Start | Control Panel | Security Center | Windows Firewall | OFF.

4. Start the telnet service in the virtual image:
   a. Click Start and right-click My Computer.
   b. Select Manage | Services and Applications | Services, then double-click Telnet.
   c. In the Telnet Properties (Local Computer) page, select Automatic for the Startup type, then select Apply | Start | OK.

5. Enable FTP in the virtual image:
   a. Select Start | Control Panel | Add or remove Programs | Add or remove Windows components.
   b. In the Windows Components wizard, double-click Internet Information Services(IIS).
   c. In the Internet Information Services(IIS) pop-up window, select these entries:
      - File Transfer Protocol (FTP) Service
      - Common Files
      - Internet Information Services Snap-In
   d. Click OK, then click Next.
   e. In the Windows Components wizard, click Finish to finish installing FTP.
   f. In the Insert Disk message, click Cancel.
   g. In the Windows XP Setup message, select OK.

6. Configure FTP settings in the virtual image:
   a. Select Start | Control Panel | Switch to Classic View | Administrative Tools, then double-click Internet Information Services.
   b. In the Internet Information Services page, expand the entry under Internet Information Services, then expand FTP Sites.
   d. Browse to the C:\ drive, select Read, Write, and Log visits.
   e. Click Apply, then OK.
7 Set automatic logon:
   a Select Start | Run, type rundll32 netplwiz.dll,UsersRunDll, then press Enter.
   b In the User Accounts window, deselect Users must enter a user name and password to use this computer and click Apply.
   c In the Automatically log on page, provide these credentials.
      • User name — Administrator
      • Password — cr@cker42
      • Confirm Password — cr@cker42

8 Run the MergeIDE batch file on the virtual machine:
   a Download MergeIDE.zip from https://www.virtualbox.org/attachment/wiki/Migrate_Windows/MergeIDE.zip on the native computer and then copy it to the virtual machine.
   b Extract MergeIDE.zip and run the MergeIDE batch file in the VM.

9 Disable Windows updates:
   a Select Start | Settings | Control Panel.
   b Open System.
   c In the Automatic Updates tab, deselect Keep my computer up to date.
   d Click Apply and then OK.

10 Configure Microsoft Office:
   a To analyze Microsoft Word, Excel, and PowerPoint files, install Microsoft Office 2003 on the virtual machine.
   b Lower the security to run macros for the Office applications. In Microsoft Word 2003 and select Tools | Macro | Security, select Low, then click OK. Do the same for other applications such as Microsoft Excel and PowerPoint.

You need the compatibility pack to open Microsoft Office files that were created in a newer version of Microsoft Office. For example, to open a .docx file using Office 2003, you need the corresponding compatibility pack installed.
   d In the Compatibility Pack for the 2007 Office system dialog, select Click here to accept the Microsoft Software License Terms, then click OK.

11 Configure Adobe Reader:
   a To analyze PDF files, download Adobe Reader to the native host and copy it to the VM.
   b Open Adobe Reader and click Accept.
   c In Adobe Reader, select Edit | Preferences | General, then remove Check for updates.
   d In Adobe Reader, select Help | Check for updates | Preferences, then deselect Adobe Updates.
12 Configure Java:
   a Open Java in the Control Panel.
   b In the Update tab, deselect Check for Updates Automatically.
   c In the Java Update Warning message, select Do Not Check and then click OK.

13 Configure system startup:
   a Run the msconfig command.
   b From the Startup tab, deselect reader_sl and jusched, then click OK.
       reader_sl is available only when Adobe Reader is installed.
   c In the System Configuration message, select Restart.
   d In the System Configuration Utility message, select Don't show this message or launch the System Configuration Utility when Windows start, then click OK.

14 Configure the default browser:
   a In Internet Explorer, select Tools | Internet Options.
   b In Home page select Use Blank or Use new tab based on the version of Internet Explorer.
   c From the Privacy tab, uncheck Turn on Pop-up Blocker.
   d Go to the Advanced tab of the Internet Options and locate Security, then select Allow active content to run in files on My Computer.

Prepare a Windows Server 2003 image for analysis
Configure your Windows Server 2003 virtual system for analysis.

Task

1 Log on to the virtual machine as administrator.
2 If the Windows Server Post-Setup Security Updates page appears, select Finish.
3 If the Manage Your Server window page appears, select Don’t Display the page at logon and close the page.
4 Disable the shutdown event tracker:
   a Select Start | Run, type gpedit.msc, then click OK.
   b In the Group policy object editor page, select Computer Configuration | Administrative Templates | System, then double-click Display Shutdown Event Tracker.
   c Select Disabled, then click OK.
   d Close the Group policy object editor page.
5 Install the hotfix for Windows Server 2003 Service Pack 1 (if applicable).
   - Go to http://support.microsoft.com/hotfix/KBHotfix.aspx?kbnum=899260&kbln=en-us and install the
     hotfix corresponding to your version of Windows Server 2003.
   - Restart the virtual machine.
   - In the Windows command prompt, run the `tlntsvr /service` command.

6 Turn off the firewall in the virtual image: Select Start | Control Panel | Windows Firewall | OFF.

7 Start the telnet service in the virtual image:
   - Click Start and right-click My Computer.
   - Select Manage | Services and Applications | Services, then double-click Telnet.
   - In the Telnet Properties (Local Computer) page, select Automatic for the Startup type, then select Apply | Start | OK.

8 Enable FTP in the virtual image:
   - Select Start | Control Panel | Add or remove Programs | Add or remove Windows components.
   - In the Windows Components wizard, double-click Application Server, then double-click Internet Information Services(IIS).
   - In the Internet Information Services(IIS) pop-up window, select these entries:
     - File Transfer Protocol (FTP) Service
     - Common Files
     - Internet Information Services Manager
   - Click OK, then click Next.
   - In the Windows Components wizard, click Finish when the FTP installation is complete.
   - In the Insert Disk message, click Cancel.
   - In the Windows XP Setup message, select OK.

9 Configure FTP settings in the virtual image:
   - Select Start | Control Panel | Switch to Classic View | Administrative Tools, then double-click Internet Information Services.
   - In the Internet Information Services page, expand the entry under Internet Information Services, then expand FTP Sites.
   - Right-click on Default FTP Site, select Properties | Home Directory.
   - Browse to the C:\ drive, select Read, Write, and Log visits.
   - Click Apply, then click OK.

10 Set automatic logon:
    - Select Start | Run, type rundll32 netplwiz.dll,UsersRunDll, then press Enter.
    - In the User Accounts window, deselect Users must enter a user name and password to use this computer and click Apply.
c In the **Automatically log on** page, provide these credentials.
   - **User name** — Administrator
   - **Password** — cr@cker42
   - **Confirm Password** — cr@cker42

11 Run the MergeIDE batch file on the virtual machine:
   a Download MergeIDE.zip from [https://www.virtualbox.org/attachment/wiki/Migrate_Windows/MergeIDE.zip](https://www.virtualbox.org/attachment/wiki/Migrate_Windows/MergeIDE.zip) on the native computer and then copy it to the virtual machine.
   b Extract MergeIDE.zip and run the MergeIDE batch file in the VM.

12 Disable Windows updates:
   a Select **Start** | **Control Panel** | **System** | **Automatic Updates**.
   b Select **Turn off Automatic Updates**.
   c Click **Apply** and then click **OK**.

13 Configure Microsoft Office:
   a To analyze Microsoft Word, Excel, and PowerPoint files, install Microsoft Office 2003 on the virtual machine.
   b Lower the security to run macros for the Office applications. In Microsoft Word 2003 and select **Tools** | **Macro** | **Security**, select **Low**, then click **OK**. Do the same for other applications such as Microsoft Excel and PowerPoint.
      You need the compatibility pack to open Microsoft Office files that were created in a newer version of Microsoft Office. For example, to open a .docx file using Office 2003, you need the corresponding compatibility pack installed.
   d In the Compatibility Pack for the 2007 Office system dialog, select **Click here to accept the Microsoft Software License Terms**, then click **OK**.

14 Configure Adobe Reader:
   a To analyze PDF files, download Adobe Reader to the native host and copy it to the VM.
   b Open Adobe Reader and click **Accept**.
   c In Adobe Reader, select **Edit** | **Preferences** | **General**, then remove **Check for updates**.
   d In Adobe Reader, select **Help** | **Check for updates** | **Preferences**, then deselect **Adobe Updates**.

15 Configure Java:
   a Open Java in the Control Panel.
   b In the Update tab, deselect **Check for Updates Automatically**.
   c In the Java Update Warning message, select **Do Not Check** and then click **OK**.
16 Configure system startup:
   a Run the `msconfig` command.
   b From the Startup tab, deselect `reader_sl` and `jusched`, then click OK.
      
      *reader_sl* is available only when Adobe Reader is installed.
   c In the System Configuration message, select **Restart**.
   d In the System Configuration Utility message, select **Don't show this message or launch the System Configuration Utility when Windows start**, then click **OK**.

17 Configure the default browser:
   a In Internet Explorer, select **Tools** | **Internet Options**.
   b In **Home page** select **Use Blank** or **Use new tab** based on the version of Internet Explorer.
   c From the Privacy tab, uncheck **Turn on Pop-up Blocker**.
   d Go to the Advanced tab of the Internet Options and locate **Security**, then select **Allow active content to run in files on My Computer**.

**Prepare a Windows 7 image for analysis**
Configure your Windows 7 virtual system for analysis.

**Task**

1 Log on to the virtual machine as administrator.

2 Turn off the firewall in the virtual image:
   a Select **Start** | **Control Panel** | **System and Security** | **Turn on Windows Firewall On or Off**.
   b Select **Turn off Windows Firewall (not recommended) for both Home or work(private) network location settings and Public network location settings**, then click **OK**.

3 Enable required Windows features.
   a Select **Start** | **Control Panel** | **Programs** | **Programs and Features** | **Turn Windows feature on or off**.
   b Select **Internet Information Services** | **FTP server** | **FTP Extensibility**.
   c Select **Internet Information Services** | **Web Management Tools** | **IIS Management Service**.
   d Select **Telnet Server**, then click **OK**.
       This operation might take around 5 minutes to complete.

4 Start the telnet service in the virtual image:
   a Click **Start** and right-click **My Computer**.
   b Select **Manage** | **Services and Applications** | **Services**, then double-click **Telnet**.
   c In the **Telnet Properties (Local Computer)** page, select **Automatic** for the Startup type, then select **Apply** | **Start** | **OK**.
Configure FTP settings in the virtual image:

a Select Start | Control Panel | System and Security | Administrative Tools, then double-click Internet Information Services.

b In the Internet Information Services page, expand the entry under Internet Information Services (IIS) Manager, then expand the tree under host name.

c Select Sites, right-click on Default FTP Site, select Remove, then click Yes to confirm.

d Right-click Sites, select Add FTP Site, then do the following.
   • Provide the FTP site name as root and Physical path as C:\, then click Next.
   • For Bindings and SSL Settings, select No SSL, then click Next.
   • For Authentication and Authorization Information, select Basic under Authentication, select All Users under Allow access to, select both Read and Write under Permissions.
      • Click Finish.

e Close the Internet Information Services (IIS) Manager page.

Set automatic logon:

a Select Start | Run, type netplwiz, then press Enter.

b In the User Accounts window, deselect Users must enter a user name and password to use this computer, then click Apply.

c In the Automatically log on page, provide these credentials.
   • User name — Administrator
   • Password — cr@cker42
   • Confirm Password — cr@cker42

Run the MergeIDE batch file on the virtual machine:

a Download MergeIDE.zip from https://www.virtualbox.org/attachment/wiki/Migrate_Windows/MergeIDE.zip on the native computer and then copy it to the virtual machine.

b Extract MergeIDE.zip and run the MergeIDE batch file in the VM.

Disable Windows updates:

a Select Start | Control Panel | Windows Update | Change settings.

b Under Important updates, select Never check for updates (not recommended).

c Deselect all options under Recommended updates, Who can install updates, Microsoft update, Software notifications.

d Click OK.

Configure Microsoft Office:

a To analyze Microsoft Word, Excel, and PowerPoint files, install Microsoft Office 2003 on the virtual machine.

b Lower the security to run macros for the Office applications. In Microsoft Word 2003 and select Tools | Macro | Security, select Low, then click OK. Do the same for other applications such as Microsoft Excel and PowerPoint.

You need the compatibility pack to open Microsoft Office files that were created in a newer version of Microsoft Office. For example, to open a .docx file using Office 2003, you need the corresponding compatibility pack installed.

d In the Compatibility Pack for the 2007 Office system dialog, select Click here to accept the Microsoft Software License Terms, then click OK.

10 Configure JustSystems Ichitaro word processing software:
   a To analyze JTD and JTDC files, install Ichitaro word processing software.
      Recommended versions Govt8 or Pro3.
   b Disable automatic updates.
   c If you want analyze Microsoft Office files using Ichitaro, manually change the file association.

11 Configure Adobe Reader:
   a To analyze PDF files, download Adobe Reader to the native host and copy it to the VM.
   b Open Adobe Reader and click Accept.
   c In Adobe Reader, select Edit | Preferences | General, then remove Check for updates.
   d In Adobe Reader, select Help | Check for updates | Preferences, then deselect Adobe Updates.

12 Configure Java:
   a Open Java in the Control Panel.
   b In the Update tab, deselect Check for Updates Automatically.
   c In the Java Update Warning message, select Do Not Check and then click OK.

13 Configure system startup:
   a Run the msconfig command.
   b From the Startup tab, deselect reader_sl and jusched, then click OK.

   reader_sl is available only when Adobe Reader is installed.

   c In the System Configuration message, select Restart.
   d In the System Configuration Utility message, select Don't show this message or launch the System Configuration Utility when Windows start, then click OK.

14 Configure the default browser:
   a In Internet Explorer, select Tools | Internet Options.
   b In Home page select Use Blank or Use new tab based on the version of Internet Explorer.
   c From the Privacy tab, uncheck Turn on Pop-up Blocker.
   d Go to the Advanced tab of the Internet Options and locate Security, then select Allow active content to run in files on My Computer.
15 Disable the HTTP auto proxy server: Open command prompt with administrator privilege, then run these commands:
   • `Net stop WinHttpAutoProxySvc`
   • `Sc config WinHttpAutoProxySvc start= disabled`

### Prepare a Windows Server 2008 image

Configure your Windows Server 2008 virtual system for analysis.

**Task**

1. Log on to the virtual machine as administrator.
2. If the Manage Your Server window page appears, select **Don’t Display the page at logon** and close the page.
3. Disable the shutdown event tracker:
   a. Select `Start` | `Run`, type `gpedit.msc`, then click **OK**.
   b. In the Local Group Policy Editor page, select **Computer Configuration** | **Administrative Templates** | **System**, then double-click **Display Shutdown Event Tracker**.
   c. Select **Disabled**, then click **OK**.
   d. Close the Local Group Policy Editor page.
4. Turn off the firewall in the virtual image:
   a. Select `Start` | `Control Panel` | `Windows Firewall` | `Turn on Windows Firewall On or Off`.
   b. Select **Off**, then click **OK**.
5. Install telnet in the virtual image:
   a. Select `Start` | `Administrative Tools` | `Server Manager`.
   b. In the Server Manager window, right-click **Features** and select **Add Features**.
   c. In the **Add Features Wizard**, select **Telnet Server**.
   d. Click **Next**, then **Install**.
   e. Click **Close** after the installation succeeds.
6. Start the telnet service in the virtual image:
   a. Select `Start` | `Administrative Tools` | `Services`, then double-click **Telnet**.
   b. In the **Telnet Properties (Local Computer)** page, select **Automatic** for the Startup type, then select **Apply** | **Start** | **OK**.
7. Configure FTP settings in the virtual image:
   a. Select `Start` | `Administrative Tools` | `Internet Information Services(IIS) Manager`.
   b. In the Internet Information Services Manager page, select **Sites**, select **Add FTP Site**
   c. In the **Add FTP Site** wizard, do the following.
      • Provide the **FTP site name** as **root** and **Physical path** as **C:\**, then click **Next**.
      • For **Bindings and SSL Settings**, select **No SSL**, then click **Next**.
For Authentication and Authorization Information, select Basic under Authentication, select All Users under Allow access to, select both Read and Write under Permissions.

Click Finish.

8 Set automatic logon:
a. Select Start | Run, type netplwiz, then press Enter.
b. In the User Accounts window, deselect Users must enter a user name and password to use this computer, then click Apply.
c. In the Automatically log on page, provide these credentials.
   - User name — Administrator
   - Password — cr@cker42
   - Confirm Password — cr@cker42

9 Run the MergeIDE batch file on the virtual machine:
a. Download MergeIDE.zip from https://www.virtualbox.org/attachment/wiki/Migrate_Windows/MergeIDE.zip on the native computer and then copy it to the virtual machine.
b. Extract MergeIDE.zip and run the MergeIDE batch file in the VM.

10 Disable Windows updates:
b. Under Important updates, select Never check for updates (not recommended).
c. Deselect Recommended updates when downloading, installing, or notifying me about updates.
d. Click OK.

11 Configure Microsoft Office:
b. Lower the security to run macros for the Office applications. In Microsoft Word 2003 and select Tools | Macro | Security, select Low, then click OK. Do the same for other applications such as Microsoft Excel and PowerPoint.
   You need the compatibility pack to open Microsoft Office files that were created in a newer version of Microsoft Office. For example, to open a .docx file using Office 2003, you need the corresponding compatibility pack installed.
d. In the Compatibility Pack for the 2007 Office system dialog, select Click here to accept the Microsoft Software License Terms, then click OK.

12 Configure Adobe Reader:
a. To analyze PDF files, download Adobe Reader to the native host and copy it to the VM.
b. Open Adobe Reader and click Accept.
c In Adobe Reader, select **Edit | Preferences | General**, then remove **Check for updates**.

d In Adobe Reader, select **Help | Check for updates | Preferences**, then deselect **Adobe Updates**.

13 Configure Java:

a Open Java in the Control Panel.

b In the Update tab, deselect **Check for Updates Automatically**.

c In the Java Update Warning message, select **Do Not Check** and then click **OK**.

14 Configure system startup:

a Run the **msconfig** command.

b From the Startup tab, deselect **reader_sl** and **jusched**, then click **OK**.

   **reader_sl** is available only when Adobe Reader is installed.

   **info**

   c In the System Configuration message, select **Restart**.

   d In the System Configuration Utility message, select **Don't show this message or launch the System Configuration Utility when Windows start**, then click **OK**.

15 Configure the default browser:

a In Internet Explorer, select **Tools | Internet Options**.

b In **Home page** select **Use Blank** or **Use new tab** based on the version of Internet Explorer.

c From the Privacy tab, uncheck **Turn on Pop-up Blocker**.

d Go to the Advanced tab of the Internet Options and locate **Security**, then select **Allow active content to run in files on My Computer**.

**Prepare a Windows 8 image for analysis**

Configure your Windows 8 virtual system for analysis.

**Task**

1 From the native system, set up Windows 8 to display in the Desktop mode instead of the default Metro UI mode when it starts.

   a Press the **Windows and R** keys simultaneously, which is the shortcut to open the Run dialog box.

   b In the Run dialog box, type **regedit**, then press **Enter**.

   c In Registry Editor, select **HKEY_LOCAL_MACHINE | SOFTWARE | Microsoft | Windows NT | CurrentVersion | Winlogon**, then double-click on **Shell**.

   d Change **Value data** to **explorer.exe, explorer.exe** (instead of the default value of **explorer.exe**), then click **OK**.

2 Log on to the virtual machine as administrator.
Turn off the firewall in the virtual image:
   a  Press the Windows and X keys simultaneously, then select Control Panel | System and Security | Turn on Windows Firewall On or Off.
   b  Select Turn off Windows Firewall (not recommended) for both Home or work(private) network location settings and Public network location settings, then click OK.

Disable Windows Defender:
   a  Press the Windows and X keys simultaneously, select Control Panel, then select Small Icons under View by.
   b  Select Windows Defender | Settings | Administrators, deselect Turn on Windows Defender, then click Save changes.
   c  Close the Windows Defender message box.

Disable first log on animation:
   a  Press the Windows and X keys simultaneously.
   b  In the Run dialog box, type gedit.msc, then press Enter.
   c  In the Local Group Policy Editor page, select Computer Configuration | Administrative Templates | System | Logon.
   d  Double-click Show first sign-in animation, select Disabled, then click OK.

Enable required Windows features.
   a  Press the Windows and X keys simultaneously, select Control Panel, then select Small Icons under View by.
   b  Select Programs | Programs and Features | Turn Windows feature on or off.
   c  Select Internet Information Services | FTP server | FTP Extensibility.
   d  Select Internet Information Services | Web Management Tools | IIS Management Service.
   e  Select Telnet Server.
   f  Select .NET Framework 3.5(includes .NET 2.0 and 3.0) and then select Windows Communication Foundation HTTP Activation and Windows Communication Foundation Non-HTTP Activation options, then press OK.
   g  If the Windows needs files from Windows Update to finish installing some features message appears, select Download files from Windows Update.
      This operation might take around 5 minutes to complete. A confirmation message is displayed when the operation completes.

Edit the power options:
   a  Press the Windows and X keys simultaneously, select Control Panel, then select Small Icons under View by.
   b  Select Power Options | Choose when to turn off the display, select Never for both Turn off the display and Put the computer to sleep options, then click Save changes.
   c  Select Power Options | Choose what the power buttons do, select Change Settings that are currently unavailable for both Turn off the display and Put the computer to sleep options, then click Save changes.
   d  For shutdown settings, deselect Turn on fast startup and Hibernate options, then click Save changes.
8 Start the telnet service in the virtual image:
   a  Press the Windows and X keys simultaneously, select **Computer Management** | **Services and Applications** | **Services**, then double-click **Telnet**.
   b  In the **Telnet Properties (Local Computer)** page, select **Automatic** for the Startup type, then select **Apply** | **Start** | **OK**.

9 Configure FTP settings in the virtual image:
   a  Press the Windows and X keys simultaneously, select **Control Panel**, then select **Small Icons** under **View by**.
   b  Select **Administrative Tools**, then double-click **Internet Information Services**.
   c  In the **Internet Information Services** page, expand the entry under **Internet Information Services(IIS) Manager**, then expand the tree under host name.
   d  If you see the Do you want to get started with Microsoft Web Platform to stay connected with latest Web Platform Components? message, select **Do not show this message**, then click **Cancel**.
   e  Select **Sites**, right-click on **Default Web Site**, select **Remove**, then click **Yes** to confirm.
   f  Right-click **Sites**, select **Add FTP Site**, then do the following:
      • Provide the **FTP site name** as **root** and **Physical path** as **C:**\, then click **Next**.
      • For **Bindings and SSL Settings**, select **No SSL**, then click **Next**.
      • For Authentication and Authorization Information, select **Basic** under **Authentication**, select **All Users** under **Allow access to**, select both **Read** and **Write** under **Permissions**.
      • Click **Finish**.
   g  Close the Internet Information Services (IIS) Manager page.

10 Turn off automatic updating for Windows:
   a  Press the Windows and R keys simultaneously, type **netplwiz**, then press **Enter**.
   b  In the User Accounts window, deselect Users must enter a user name and password to use this computer, then click **Apply**.

11 Configure Telnet clients
   a  Press the Windows and X keys simultaneously, select **Control Panel**, then select **Small Icons** under **View by**.
   b  Select **Administrator Tools** | **Computer Management**.
   c  Select **Computer Management (Local) | System Tools | Local Users and Groups | Groups**.
   d  Double-click **TelnetClients**.
   e  Click **Add**, type **Administrator**, click **Check Names**, then click **OK**.

12 Set automatic logon:
   a  Press the Windows and R keys simultaneously, type **netplwiz**, then press **Enter**.
   b  In the User Accounts window, deselect Users must enter a user name and password to use this computer, then click **Apply**.
c In the **Automatically log on** page, provide these credentials.
   - **User name** — Administrator
   - **Password** — cr@cker42
   - **Confirm Password** — cr@cker42

13 Run the MergeIDE batch file on the virtual machine:
   a Download MergeIDE.zip from [https://www.virtualbox.org/attachment/wiki/Migrate_Windows/MergeIDE.zip](https://www.virtualbox.org/attachment/wiki/Migrate_Windows/MergeIDE.zip) on the native computer and then copy it to the virtual machine.
   b Extract MergeIDE.zip and run the MergeIDE batch file in the VM.

14 Configure Microsoft Office:
   a To analyze Microsoft Word, Excel, and PowerPoint files, install Microsoft Office 2003 on the virtual machine.
   b Lower the security to run macros for the Office applications. In Microsoft Word 2003 and select **Tools** | **Macro** | **Security**, select **Low**, then click **OK**. Do the same for other applications such as Microsoft Excel and PowerPoint.
      You need the compatibility pack to open Microsoft Office files that were created in a newer version of Microsoft Office. For example, to open a .docx file using Office 2003, you need the corresponding compatibility pack installed.
   d In the Compatibility Pack for the 2007 Office system dialog, select **Click here to accept the Microsoft Software License Terms**, then click **OK**.

15 Configure Adobe Reader:
   a To analyze PDF files, download Adobe Reader to the native host and copy it to the VM.
   b Open Adobe Reader and click **Accept**.
   c In Adobe Reader, select **Edit** | **Preferences** | **General**, then remove **Check for updates**.
   d In Adobe Reader, select **Help** | **Check for updates** | **Preferences**, then deselect **Adobe Updates**.

16 Configure Java:
   a Open Java in the Control Panel.
   b In the Update tab, deselect **Check for Updates Automatically**.
   c In the Java Update Warning message, select **Do Not Check** and then click **OK**.

17 Configure system startup:
   a Run the `msconfig` command.
   b From the Startup tab, then click **Open Task Manager**.
   c Select **Java(TM) Update Scheduler (jusched)** (if listed), then click **Disable**.
   d Select **Adobe Acrobat SpeedLauncher (reader_sl)** (if listed), then click **Disable**.
e In the System Configuration message, select **Restart**.

f In the System Configuration Utility message, select **Don't show this message or launch the System Configuration Utility when Windows start**, then click **OK**.

18 Configure the default browser:

a In Internet Explorer, select **Tools** | **Internet Options**.

b In **Home page** select **Use Blank** or **Use new tab** based on the version of Internet Explorer.

c From the **Privacy tab**, uncheck **Turn on Pop-up Blocker**.

d Go to the Advanced tab of the Internet Options and locate **Security**, then select **Allow active content to run in files on My Computer**.

19 Disable the HTTP auto proxy server: Open command prompt with administrator privilege, then run these commands.

• `Net stop WinHttpAutoProxySvc`

• `Sc config WinHttpAutoProxySvc start= disabled`

### Prepare a Windows 8.1 image for analysis

Configure your Windows 8.1 virtual system for analysis.

**Task**

1 From the native system, set up Windows 8.1 to display in the Desktop mode instead of the default Metro UI mode when it starts.

a Press the **Windows** and **R** keys simultaneously, which is the shortcut to open the Run dialog box.

b In the Run dialog box, type `regedit`, then press **Enter**.

c In **Registry Editor**, select **HKEY_LOCAL_MACHINE** | **SOFTWARE** | **Microsoft** | **Windows NT** | **CurrentVersion** | **Winlogon**, then double-click on **Shell**.

d Change **Value data** to `explorer.exe`, `explorer.exe` (instead of the default value of `explorer.exe`), then click **OK**.

2 Log on to the virtual machine as administrator.

3 Turn off the firewall in the virtual image:

a Press the **Windows** and **X** keys simultaneously, then select **Control Panel** | **System and Security** | **Turn on Windows Firewall On or Off**.

b Select **Turn off Windows Firewall (not recommended)** for both **Home or work (private)** network location settings and **Public network location settings**, then click **OK**.

4 Disable Windows Defender:

a Press the **Windows** and **X** keys simultaneously, select **Control Panel**, then select **Small Icons** under **View by**.

b Select **Windows Defender** | **Settings** | **Administrators**, deselect **Turn on this app**, then click **Save changes**.

c If a Windows Defender message appears, close the message screen.
5 Disable first log on animation:
   a Press the Windows and R keys simultaneously, type gpedit.msc, then press Enter.
   b In the Local Group Policy Editor page, select Computer Configuration | Administrative Templates | System | Logon.
   c Double-click Show first sign-in animation, select Disabled, then click OK.

6 Enable required Windows features.
   a Press the Windows and X keys simultaneously, then select Control Panel | Programs | Programs and Features | Turn Windows feature on or off.
   b Select Internet Information Services | FTP server | FTP Extensibility.
   c Select Internet Information Services | Web Management Tools | IIS Management Service.
   d Select Telnet Server.
   e Select .NET Framework 3.5(includes .NET 2.0 and 3.0) and then select Windows Communication Foundation HTTP Activation and Windows Communication Foundation Non-HTTP Activation options, then press OK.
   f If the Windows needs files from Windows Update to finish installing some features message appears, select Download files from Windows Update.
      This operation might take around 5 minutes to complete. A confirmation message is displayed when the operation completes.

7 Download and install the .NET Framework 4.6 on the VM image.
   If a Blocking Issues message appears, install the suggested components, then select Continue.

8 Edit the power options:
   a Press the Windows and X keys simultaneously, select Control Panel, then select Small Icons under View by.
   b Select Power Options | Choose when to turn off the display, select Never for both Turn off the display, and Put the computer to sleep options, then click Save changes.
   c For shutdown settings, deselect Turn on fast startup and Hibernate options, then click Save changes.

9 Start the telnet service in the virtual image:
   a Press the Windows and X keys simultaneously, select Computer Management | Services and Applications | Services, then double-click Telnet.
   b In the Telnet Properties (Local Computer) page, select Automatic for the Startup type, then select Apply | Start | OK.

10 Configure FTP settings in the virtual image:
   a Press the Windows and X keys simultaneously, select Control Panel | System and Security | Administrative Tools, then double-click Internet Information Services.
   b In the Internet Information Services page, expand the entry under Internet Information Services(IIS) Manager, then expand the tree under host name.
   c If you see the Do you want to get started with Microsoft Web Platform to stay connected with latest Web Platform Components? message, select Do not show this message, then click Cancel.
   d Select Sites, right-click on Default Web Site, select Remove, then click Yes to confirm.
e Right-click Sites, select Add FTP Site, then do the following.
   • Provide the FTP site name as root and Physical path as C:\, then click Next.
   • For Bindings and SSL Settings, select No SSL, then click Next.
   • For Authentication and Authorization Information, select Basic under Authentication, select All Users under Allow access to, select both Read, and Write under Permissions.
   • Click Finish.

f Close the Internet Information Services (IIS) Manager page.

11 Turn off automatic updating for Windows:
   a Press the Windows and X keys simultaneously, then select Control Panel | Windows Update | Change.
   b Select Never check for updates (not recommended), then click OK

12 Configure Telnet clients.
   a Press the Windows and X keys simultaneously, select Control Panel, then select Small Icons under View by.
   b Select Administrative tools | Computer Management.
   c Select Computer Management (Local) | System Tools | Local Users and Groups | Groups.
   d Double-click TelnetClients.
   e Click Add, type Administrator, click Check Names, then click OK.

13 Set automatic logon:
   a Press the Windows and R keys simultaneously, type netplwiz, then press Enter.
   b In the User Accounts window, deselect Users must enter a user name and password to use this computer, then click Apply.
   c In the Automatically log on page, provide these credentials.
      • User name — Administrator
      • Password — cr@cker42
      • Confirm Password — cr@cker42

14 Run the MergeIDE batch file on the virtual machine:
   a Download MergeIDE.zip from https://www.virtualbox.org/attachment/wiki/Migrate_Windows/MergeIDE.zip on the native computer and then copy it to the virtual machine.
   b Extract MergeIDE.zip and run the MergeIDE batch file in the VM.

15 Configure Microsoft Office:
   a To analyze Microsoft Word, Excel, and PowerPoint files, install Microsoft Office 2007 on the virtual machine.
   b Lower the security to run macros for the Office applications. In Microsoft Word 2007, select the Microsoft Office option on the top left corner, then select Word options | Trust Center | Trust Center Settings | Macro Settings, then select Enable all macros (not recommended potentially dangerous code can run). Do the same for other applications such as Microsoft Excel and PowerPoint.
   c On the Welcome to Microsoft Office 2007 page, click Next button.
   d On the Sign-up for Microsoft Update page, select I don't want to use Microsoft Update, then click Finish.
Configure Adobe Reader:
- To analyze PDF files, download Adobe Reader to the native host and install it to the VM.
- In Adobe reader, if Adobe Reader Protected Mode message appears, select Open with Protected Mode disabled, then select OK.
- If Accessibility Setup Assistance message appears, select Cancel.
- Select Edit | Preferences | Updater, select Do not download or install updated automatically, select OK, then select Yes to confirm the changes.

Configure Java:
- Open Java in the Control Panel.
- In the Update tab, deselect Check for Updates Automatically.
- In the Java Update Warning message, select Do Not Check and then click OK.

Configure system startup:
- Run the msconfig command.
- From the Startup tab, then click Open Task Manager.
- Select Java(TM) Update Scheduler (jusched) (if listed), then click Disable.
- Select Adobe Acrobat SpeedLauncher (reader_sl) (if listed), then click Disable.
- In the System Configuration dialog, select Don’t show this message again, then select Restart.

Configure the default browser:
- In Internet Explorer, select Tools | Internet Options.
- In Home page select Use Blank or Use new tab based on the version of Internet Explorer.
- From the Privacy tab, uncheck Turn on Pop-up Blocker.
- Go to the Advanced tab of the Internet Options and locate Security, then select Allow active content to run in files on My Computer.

Disable the HTTP auto proxy server: Open command prompt with administrator privilege, then run these commands.
- Net stop WinHttpAutoProxySvc
- Sc config WinHttpAutoProxySvc start= disabled

Prepare a Windows 10 or Windows 10 v1703 (Redstone 2) image for analysis
Configure your Windows 10 virtual system for analysis.

Task

From the native system, set up Windows 10 to display in the Desktop mode instead of the default Metro UI mode when it starts.
- Press the Windows and R keys simultaneously, which is the shortcut to open the Run dialog box.
- In the Run dialog box, type regedit, then press Enter.
In Registry Editor, select HKEY_LOCAL_MACHINE | SOFTWARE | Microsoft | Windows NT | CurrentVersion | Winlogon, then double-click on Shell.

Change Value data to explorer.exe, explorer.exe (instead of the default value of explorer.exe), then click OK.

Log on to the virtual machine as administrator.

Turn off the firewall in the virtual image:

- Press the Windows and X keys simultaneously, then select Control Panel | System and Security | Turn on Windows Firewall On or Off.
- Select Turn off Windows Firewall (not recommended) for both Home or work (private) network location settings and Public network location settings, then click OK.

Disable Windows Defender:

- Press the Windows and X keys simultaneously, select Control Panel, then select Small Icons under View by.
- Select Windows Defender, then turn off all features on the Windows Defender Settings page.
- If a Windows Defender message appears, close the message screen.

Disable first log on animation:

- Press the Windows and R keys simultaneously.
- In the Run dialog box, type gpedit.msc, then press Enter.
- In the Local Group Policy Editor page, select Computer Configuration | Administrative Templates | System | Logon.
- Double-click Show first sign-in animation, select Disabled, then click OK.

Enable required Windows features.

- Press the Windows and X keys simultaneously, select Control Panel, then select Small Icons under View by.
- Select Programs | Programs and Features | Turn Windows feature on or off.
- Select Internet Information Services | FTP server | Control Panel | FTP Extensibility.
- Select Internet Information Services | Web Management Tools | IIS Management Service.
- Select .NET Framework 4.6 Advanced Services, and ensure that ASP.NET 4.6 is enabled.
- Select WCF Service Library, ensure that TCP Port Sharing is enabled, then select OK.
- If the Windows needs files from Windows Update to finish installing some features message appears, select Download files from Windows Update.
  - This operation might take around 5 minutes to complete. A confirmation message is displayed when the operation completes.

Edit the power options:

- Press the Windows and X keys simultaneously, select Control Panel, then select Small Icons under View by.
- Select Power Options | Choose when to turn off the display, select Never for Turn off the display, then click Save changes.
- For shutdown settings, deselect Turn on fast startup and Hibernate options, then click Save changes.
Configure FTP settings in the virtual image:

a. Press the Windows and X keys simultaneously, select Control Panel, then select Small Icons under View by.

b. Select Administrative Tools, then double-click Internet Information Services.

c. In the Internet Information Services page, expand the entry under Internet Information Services(IIS) Manager, then expand the tree under host name.

d. If you see the Do you want to get started with Microsoft Web Platform to stay connected with latest Web Platform Components? message, select Do not show this message, then click Cancel.

e. Select Sites, right-click on Default Web Site, select Remove, then click Yes to confirm.

f. Right-click Sites, select Add FTP Site, then do the following.
   • Provide the FTP site name as root and Physical path as C:\, then click Next.
   • For Bindings and SSL Settings, select No SSL, then click Next.
   • For Authentication and Authorization Information, select Basic under Authentication, select All Users under Allow access to, select both Read and Write under Permissions.
   • Click Finish.

g. Close the Internet Information Services (IIS) Manager page.

Turn off automatic updating for Windows:

a. Press the Windows and X keys simultaneously, select Control Panel, then select Small Icons under View by.

b. Select Administrative Tools | Services, then double-click Windows Update.

c. Select Startup type as Disabled.

d. Stop the service if the service is running.

e. Press the Windows and X keys simultaneously, then select Control Panel | Windows Update | Change.

f. Select Never check for updates (not recommended), then click OK

Set automatic logon:

a. Press the Windows and R keys simultaneously, type netplwiz, then press Enter.

b. In the User Accounts window, deselect Users must enter a user name and password to use this computer, then click Apply.

c. In the Automatically log on page, provide these credentials.
   • User name — admin
   • Password — cr@cker42
   • Confirm Password — cr@cker42

Run the MergeIDE batch file on the virtual machine:

a. Download MergeIDE.zip from https://www.virtualbox.org/attachment/wiki/Migrate_Windows/MergeIDE.zip on the native computer and then copy it to the virtual machine.

b. Extract MergeIDE.zip and run the MergeIDE batch file in the VM.
12 Configure Microsoft Office:
   a To analyze Microsoft Word, Excel, and PowerPoint files, install Microsoft Office 2007 on the virtual machine.
   b Lower the security to run macros for the Office applications. In Microsoft Word 2007, select the Microsoft Office option on the top left corner, then select Word options | Trust Center | Trust Center Settings | Macro Settings, then select Enable all macros (not recommended potentially dangerous code can run). Do the same for other applications such as Microsoft Excel and PowerPoint.
   c Lower the security to run ActiveX for the Office applications. In Microsoft Word 2007, select the Microsoft Office option on the top left corner, then select Word options | Trust Center | Trust Center Settings | ActiveX Settings, then select Enable all controls without restrictions and without prompting (not recommended potentially dangerous code can run). Do the same for other applications such as Microsoft Excel and PowerPoint.
   d Select Word options | Trust Center | Trusted Center Settings | Trusted Locations, then use the Add new location... button to add C:\ under User Locations. Once added, double click on the entry for C:\, then in the pop-up, select Subfolders of this location are also trusted, then click OK.
   e On the Welcome to Microsoft Office 2007 page, click Next button.
   f On the Sign-up for Microsoft Update page, select I don't want to use Microsoft Update, then click Finish.
   g When you open any of the Microsoft Office 2007 software, you would see the Help Protect and Improve Microsoft Office pop-up. From the pop-up select Don't make changes, then click OK.

13 Configure Adobe Reader:
   a To analyze PDF files, download Adobe Reader to the native host and install it to the VM.
   b In Adobe reader, if Adobe Reader Protected Mode message appears, select Open with Protected Mode disabled, then select OK.
   c If Accessibility Setup Assistance message appears, select Cancel.
   d Select Edit | Preferences | Updater, select Do not download or install updated automatically, select OK, then select Yes to confirm the changes.

14 Configure Java:
   a Open Java in the Control Panel.
   b In the Update tab, deselect Check for Updates Automatically.
   c In the Java Update Warning message, select Do Not Check and then click OK.

15 Configure system startup:
   a Run the msconfig command.
   b From the Startup tab, then click Open Task Manager.
   c Select Java(TM) Update Scheduler (jusched) (if listed), then click Disable.
   d Select Adobe Acrobat SpeedLauncher (reader_sl) (if listed), then click Disable.
   e In the System Configuration dialog, select Don't show this message again, then select Restart.

16 Configure the default browser:
   a In Internet Explorer, select Tools | Internet Options.
   b In Home page select Use Blank or Use new tab based on the version of Internet Explorer.
c From the Privacy tab, uncheck Turn on Pop-up Blocker.

d Go to the Advanced tab of the Internet Options and locate Security, then select Allow active content to run in files on My Computer.

17 Disable the HTTP auto proxy server: Open command prompt with administrator privilege, then run these commands.

   • Net stop WinHttpAutoProxySvc
   • Sc config WinHttpAutoProxySvc start= disabled

Prepare a Windows 2012 R2 image for analysis
Configuring your Windows Server 2012 R2 virtual system for analysis.

Task

1 Log on to the virtual machine as administrator.

2 If the Manage Your Server window page appears, select Don't Display the page at logon and close the page.

3 If the Server Manager window is displayed, select Manage | Server Manager Properties, select Do not start Server Manager automatically at logon, then select OK.

4 Disable the shutdown event tracker:
   a Select Start | Run, type gpedit.msc, then click OK.
   b In the Local Group Policy Editor page, select Computer Configuration | Administrative Templates | System, then double-click Display Shutdown Event Tracker.
   c Select Disabled, then click OK.
   d Close the Local Group Policy Editor page.

5 Turn off the firewall in the virtual image:
   a Select Start | Control Panel | Windows Firewall | Turn on Windows Firewall On or Off.
   b Select Off, then click OK.

6 Install telnet in the virtual image:
   a Select Start | Administrative Tools | Server Manager.
   b In the Server Manager window, select Add Roles and Features.
   c In Add Roles and Features Wizard, select Telnet Server.
   d Click Next, then Install.
   e Click Close after the installation succeeds.

7 Start the telnet service in the virtual image:
   a Select Start | Administrative Tools | Services, then double-click Telnet.
   b In the Telnet Properties (Local Computer) page, select Automatic for the Startup type, then select Apply | Start | OK.
Configure FTP settings in the virtual image:

1. Install IIS Manager if not already present and make sure you check the FTP Server checkbox when installing IIS Manager.
2. From Server Manager page, select Add Roles and Features, then click Next.
3. In the Installation type page, select Role-based or feature-based installation, then click Next.
4. In the Server selection page, select Select a server from the server pool, then click Next.
5. In the Server Roles page, expand the Web Server (IIS) node, expand the FTP Server node, select FTP Service, then click Next.
6. In the Select features page, click Next, then click Install.

Select Start | Administrative Tools | Internet Information Services(IIS) Manager.

In the Internet Information Services Manager page, select Sites, select Add FTP Site

In the Add FTP Site wizard, do the following.

- Provide the FTP site name as root and Physical path as C:\, then click Next.
- For Bindings and SSL Settings, select No SSL, then click Next.
- For Authentication and Authorization Information, select Basic under Authentication, select All Users under Allow access to, select both Read and Write under Permissions.
- Click Finish.

Download and install the .NET Framework 4.6 on the VM image.
If a Blocking Issues message appears, install the suggested components, then select Continue.

Set automatic logon:

a. Select Start | Run, type netplwiz, then press Enter.

b. In the User Accounts window, deselect Users must enter a user name and password to use this computer, then click Apply.

c. In the Automatically log on page, provide these credentials.

- User name — Administrator
- Password — cr@cker42
- Confirm Password — cr@cker42

d. Click OK.

Run the MergeIDE batch file on the virtual machine:

a. Download MergeIDE.zip from https://www.virtualbox.org/attachment/wiki/Migrate_Windows/MergeIDE.zip on the native computer and then copy it to the virtual machine.

b. Extract MergeIDE.zip and run the MergeIDE batch file in the VM.

Disable Windows updates:


b. Under Important updates, select Never check for updates (not recommended).

c. Deselect Recommended updates when downloading, installing, or notifying me about updates.

d. Click OK.
Configure Microsoft Office:


b. Lower the security to run macros for the Office applications. In Microsoft Word 2007, select the Microsoft Office option on the top left corner, then select Word options | Trust Center | Trust Center Settings | Macro Settings, then select Enable all macros (not recommended potentially dangerous code can run). Do the same for other applications such as Microsoft Excel and PowerPoint.

c. Lower the security to run ActiveX for the Office applications. In Microsoft Word 2007, select the Microsoft Office option on the top left corner, then select Word options | Trust Center | Trust Center Settings | ActiveX Settings, then select Enable all controls without restrictions and without prompting (not recommended potentially dangerous code can run). Do the same for other applications such as Microsoft Excel and PowerPoint.

d. On the Welcome to Microsoft Office 2007 page, click Next button.

e. On the Sign-up for Microsoft Update page, select I don't want to use Microsoft Update, then click Finish.

Configure Adobe Reader:

a. To analyze PDF files, download Adobe Reader to the native host and install it to the VM.

b. In Adobe reader, if Adobe Reader Protected Mode message appears, select Open with Protected Mode disabled, then select OK.

c. If Accessibility Setup Assistance message appears, select Cancel.

d. Select Edit | Preferences | Updater, select Do not download or install updated automatically, select OK, then select Yes to confirm the changes.

Configure Java:

a. Open Java in the Control Panel.

b. In the Update tab, deselect Check for Updates Automatically.

c. In the Java Update Warning message, select Do Not Check and then click OK.

Configure system startup:

a. Run the msconfig command.

b. From the Startup tab, deselect reader_sl and jusched, then click OK.

i reader_sl is available only when Adobe Reader is installed.

c. In the System Configuration dialog, select Don't show this message again, then select Restart.

Configure the default browser:

a. In Internet Explorer, select Tools | Internet Options.

b. In Home page select Use Blank or Use new tab based on the version of Internet Explorer.

c. From the Privacy tab, uncheck Turn on Pop-up Blocker.

d. Go to the Advanced tab of the Internet Options and locate Security, then select Allow active content to run in files on My Computer.
Prepare a Windows Server 2016 Standard image for analysis
Configure your Windows Server 2016 Standard virtual system for analysis.

Task
1. Log on to the virtual machine as administrator.
2. If the Manage Your Server window page appears, select Don't Display the page at logon and close the page.
3. If the Server Manager windows is displayed, select Manage | Server Manager Properties, select Do not start Server Manager automatically at logon, then select OK.
4. Disable the shutdown event tracker:
   a. Select Start | Run, type gedit.msc, then click OK.
   b. In the Local Group Policy Editor page, select Computer Configuration | Administrative Templates | System, then double-click Display Shutdown Event Tracker.
   c. Select Disabled, then click OK.
   d. Close the Local Group Policy Editor page.
5. Turn off the firewall in the virtual image:
   a. Select Start | Control Panel | Windows Firewall | Turn on Windows Firewall On or Off.
   b. Select Turn off Windows Firewall (not recommended), for the following, then click OK.
      • Home or work (private) networks
      • Public networks
6. Configure FTP settings in the virtual image:
   a. Install IIS Manager if not already present and make sure you check the FTP Server checkbox when installing IIS Manager.
      1. From Server Manager page, select Add Roles and Features, then click Next.
      2. In the Installation type page, select Role-based or feature-based installation, then click Next.
      3. In the Server selection page, select Select a server from the server pool, then click Next.
      4. In the Server Roles page, expand the Web Server (IIS) node, expand the FTP Server node, select FTP Server, select FTP Service, then click Next.
      5. In the Select features page, click Next, then click Install.
   b. Select Start | Administrative Tools | Internet Information Services(IIS) Manager.
   c. In the Internet Information Services Manager page, select ADMINISTRATOR | Sites, then right-click on Sites and select Add FTP Site.
   d. In the Add FTP Site wizard, do the following.
      • Provide the FTP site name as root and Physical path as C:\, then click Next.
      • For Bindings and SSL Settings, select No SSL, then click Next.
      • For Authentication and Authorization Information, select Basic under Authentication, select All Users under Allow access to, select both Read and Write under Permissions.
      • Click Finish.
7. Ensure that .NET Framework 4.6.2 is installed.

8. Set automatic logon:
   a. Select Start | Run, type `netplwiz`, then press Enter.
   b. In the User Accounts window, deselect Users must enter a user name and password to use this computer, then click Apply.
   c. In the Automatically log on page, provide these credentials.
      - User name — Administrator
      - Password — cr@cker42
      - Confirm Password — cr@cker42

9. Run the MergeIDE batch file on the virtual machine:
   a. Download MergeIDE.zip from https://www.virtualbox.org/attachment/wiki/Migrate_Windows/MergeIDE.zip on the native computer and then copy it to the virtual machine.
   b. Extract MergeIDE.zip and run the MergeIDE batch file in the VM.

10. Disable Windows updates and Windows Defender:
    a. Select Start | Run, type `gpedit.msc`, then press Enter.
    c. On the right pane, double click Configure Automatic Updates, then select Disable.
    d. Click OK.
    e. Select Computer Configuration | Administrative Templates | Windows Components | Windows Defender.
    f. On the right pane, double click Turn off Windows Defender, then select Disable.
    g. Click OK.

11. Configure Microsoft Office 2016:
    a. To analyze Microsoft Word, Excel, and PowerPoint files, install Microsoft Office 2016 on the virtual machine.
    b. Lower the security to run macros for the Office applications. In Microsoft Word, select the Microsoft Office 2016 option on the top left corner, then select Word options | Trust Center | Trust Center Settings | Macro Settings, then select Enable all macros (not recommended potentially dangerous code can run). Do the same for other applications such as Microsoft Excel and PowerPoint.
    c. Lower the security to run ActiveX for the Office applications. In Microsoft Word 2007, select the Microsoft Office option on the top left corner, then select Word options | Trust Center | Trust Center Settings | ActiveX Settings, then select Enable all controls without restrictions and without prompting (not recommended potentially dangerous code can run). Do the same for other applications such as Microsoft Excel and PowerPoint.
    d. On the Welcome to Microsoft Office 2016 page, click Next button.
    e. On the Sign-up for Microsoft Update page, select I don't want to use Microsoft Update, then click Finish.

12. Configure Adobe Reader:
    a. To analyze PDF files, download Adobe Reader to the native host and install it to the VM.
    b. In Adobe reader, if Adobe Reader Protected Mode message appears, select Open with Protected Mode disabled, then select OK.
c  If Accessibility Setup Assistance message appears, select **Cancel**.

d  Select **Edit** | **Preferences** | **Updater**, select **Do not download or install updated automatically**, select **OK**, then select **Yes** to confirm the changes.

13 **Configure Java**:

   a  Open Registry Editor

   b  Navigate to **HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\JavaSoft\Java Update\Policy\EnableJavaUpdate**.

   c  Set its value to **0**.

   d  Close the Registry Editor.

14 **Configure Adobe flash player**:

   a  Run the command prompt as an Administrator.

   b  Execute the following command:

   ```
   dism.exe /online /add-package /packagepath:"<Adobe-Flash-For-Windows-Package>.mum"
   ```

   Replace `<Adobe-Flash-For-Windows-Package>` with the name and path of the Adobe Flash for Windows package MUM file.

   c  Restart the VM.

15 **Configure system startup**:

   a  Select **Start** | **Run**, type `msconfig`, then click **OK**.

   b  From the Startup tab, deselect **reader_sl** and **jusched**, then click **OK**.

   c  In the System Configuration dialog, select **Don’t show this message again**, then select **Restart**.

16 **Configure the default browser**:

   a  In Internet Explorer, select **Tools** | **Internet Options**.

   b  In **Home page** select **Use Blank** or **Use new tab** based on the version of Internet Explorer.

   c  From the Privacy tab, uncheck **Turn on Pop-up Blocker**.

   d  Go to the Advanced tab of the Internet Options and locate **Security**, then select **Allow active content to run in files on My Computer**.

   e  Open Registry Editor.

   f  Navigate to **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Active Setup\Installed Components\{A509B1A7-37EF-4b3f-8CFC-4F3A74704073}**.

   g  Set its value to **0**.

   h  Close the Registry Editor.
Import the virtual disk file

To create an analyzer VM, you must import the corresponding virtual disk file into Advanced Threat Defense.

**Task**

1. Click **Start | Shut down**.

2. Make sure there are no stale lock files (.lck) associated with the virtual machine.
   - The .lck files are located in the same folder as the .vmdk or .vhdx file.

3. Locate the virtual disk file.
   - Make sure the virtual disk file name does not contain any spaces or unsupported characters. If it contains any spaces or unsupported characters, the image file conversion fails.

4. To enable FTP, use the `set ftp enable` CLI command.
   - FTP transfer is faster than SFTP, but less secure. If your Advanced Threat Defense Appliance is in an unsecured network, such as an external network, use SFTP.

5. Open the FTP client.
   - For example, you can use WinSCP or FileZilla.

6. To connect to the FTP server on Advanced Threat Defense, use the following credentials.
   - **Host** — IP address of Advanced Threat Defense
   - **Username** — atdadmin
   - **Password** — atdadmin
   - **Port** — The corresponding port number based on the protocol you want to use.

7. Upload the virtual disk file from the local machine to Advanced Threat Defense.

Convert the VMDK and VHDX file to an image file

To create an analyzer VM, you must convert the VMDK and VHDX file to an image file.

For malware analysis, you can create multiple VMs that run on the same operating system, but with different applications. For example, you can create a Windows 7 SP1 analyzer VM for Internet Explorer 10 and another Windows 7 SP1 analyzer VM for Internet Explorer 9.

Users without administrator permissions are able to convert VMDK and VHDX files to image files.

**Task**

1. Log on to the Advanced Threat Defense web interface.

2. Click **Manage | Image & Software | Image**.

3. From the **VMDK and VHDX Image** drop-down list, select the imported VMDK or VHDX file.
4 In the **Image Name** field, enter the image name that corresponds to your operating system. 

> **Image Name** must not contain a space or any special characters except hyphen (-) or underscores (_).

<table>
<thead>
<tr>
<th>Operating system</th>
<th>Image name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft Windows XP 32-bit Service Pack 2</td>
<td>winXPsp2.img</td>
</tr>
<tr>
<td>Microsoft Windows XP 32-bit Service Pack 3</td>
<td>winXPsp3.img</td>
</tr>
<tr>
<td>Microsoft Windows 7 32-bit Service Pack 1</td>
<td>win7sp1.img</td>
</tr>
<tr>
<td>Microsoft Windows 7 64-bit Service Pack 1</td>
<td>win7x64sp1.img</td>
</tr>
<tr>
<td>Microsoft Windows 8 Professional 32-bit</td>
<td>win8p0x32.img</td>
</tr>
<tr>
<td>Microsoft Windows 8 Professional 64-bit</td>
<td>win8p0x64.img</td>
</tr>
<tr>
<td>Windows 8.1 Enterprise Update 1 version 6.3 build 9600 64-bit</td>
<td>win8p1x64.img</td>
</tr>
<tr>
<td>Windows 10 Enterprise (Redstone 1 and 2, Threshold 2) 64-bit</td>
<td>win10p0x64.img</td>
</tr>
<tr>
<td>Microsoft Windows Server 2003 32-bit Service Pack 1</td>
<td>win2k3sp1.img</td>
</tr>
<tr>
<td>Microsoft Windows Server 2003 32-bit Service Pack 2</td>
<td>win2k3sp2.img</td>
</tr>
<tr>
<td>Microsoft Windows Server 2008 R2 Service Pack 1</td>
<td>win2k8sp1.img</td>
</tr>
<tr>
<td>Windows 2012 Datacenter 64-bit</td>
<td>win2k12.img</td>
</tr>
<tr>
<td>Windows 2012 R2 Datacenter 64-bit</td>
<td>win2k12r2.img</td>
</tr>
</tbody>
</table>

Ensure that you specify whether the OS is a 32-bit or a 64-bit in the **Image Name** field, else the samples will fail submission.

McAfee ePO and OS profiling work only when you use the default name.

5 **Select the Operating System.**

Advanced Threat Defense attaches the name that you provide to the default name.

*Example: You select Windows Server 2003 32-bit Service Pack 1, then enter with _PDF in the **Image Name** field. The image file name is win2k3sp1_with_PDF.*

> The image file name must be an alphabet, number, or underscore (_).

6 **Click Convert.**

7 **On the Info window, click OK.**

8 **View the image conversion logs.**
   - From the **Select Log** drop-down list, select the image name.
   - **Click View.**

---

**Managing VM profiles**

After you convert the imported VMDK or VHDX file to an image file, you create a VM profile for that image file.

> You cannot associate this VM profile with any other image file. Similarly, once associated, you cannot change the VM profile for an image file.
VM profiles contain the operating system and applications in an image file. This enables you to identify the images that you uploaded to Advanced Threat Defense and then use the appropriate image for dynamically analyzing a file. You can also specify the number of licenses that you possess for the operating system and the applications. Advanced Threat Defense factors this in when creating concurrent analyzer VMs from the corresponding image file.

You use the Advanced Threat Defense web application to manage VM profiles.

![Figure 6-1 Configurations in a VM profile](image)

**Create VM profiles**

You must configure each image file that you convert with a single, unused VM profile. You can convert the same virtual disk file image files multiple times. This enables you to create multiple image files from one virtual disk file.

VM profiles contain the operating system and applications in an image file. This enables you to identify the images that you uploaded to Advanced Threat Defense and then use the appropriate image to dynamically analyze files. You can also specify the number of licenses that you possess for the operating system and the applications. Advanced Threat Defense factors this in when creating concurrent analyzer VMs from the corresponding image file.
Task

1. Log on to the Advanced Threat Defense web interface, then select Policy | VM Profile | New.

2. From the Image drop-down list, select the image, then click Activate.

   Based on your browser settings, the activation window opens in a new tab or window.

   - Ensure the pop-up blocker for your browser is not blocking the pop-up window. Add the ATD appliance IP under your pop-up blocker exceptions.
   - Ensure that ports 6000 and higher (port 6000 to 6000 + number of VMs existing on ATD appliance) are open between the ATD Client and ATD Appliance. Check that the client’s firewall allows connections on these ports. All firewalls between ATD and the client must allow connections through these ports.

3. Activate Windows on the VM.
   a. Click Start | Control Panel | Windows Activation | Activate Windows now.
   b. Open Microsoft Word, then click Activate.
   c. On the Microsoft Office Activation Wizard, follow the on-screen prompts.
   d. Shut down the VM, then click Disconnect.


5. Close the Sn. flash not exist OK message.

6. Download Flash Player.
   a. To run the original virtual disk image, use VMware ESXi or Microsoft Hyper-V.
   b. On the running VM, download Flash Player.
   c. Unzip the file.
   d. From the command line, run the following commands, then press Enter.
      - flashplayerX_X_X_win.exe
      - flashplayerX_X_X_win_debug.exe
      - flashplayerX_X_X_win_sa_debug.exe
   e. Close the Flash Player window.
   f. Stop the VM, then copy the virtual disk image to the Advanced Threat Defense Appliance.

   To view the image validation log, click . If the validation fails, create a new virtual disk file with the correct settings, then create the analyzer VM.

7. Click Check Status, then verify that the following validation tests are successful on the Image Validation Log window.
   - FTP connect to <VM IP address> OK
   - FTP login OK
   - FTP file upload OK
   - Telnet login successful
• OS winxp
• Multiprocessing OK
• FTP OK
• TELNET OK
• AUTOLOGON OK
• ADMINISTRATOR OK
• FIREWALL OK
• Sigcheck OK
• Scan Complete

If the validation tests fail, create a new virtual disk file, then create the analyzer VM.

8 Create the VM profile.
   a Configure the options.
   b Click Save.

9 On the Information window, click OK.
   • To monitor the VM creation progress, click Dashboard. The VM creation progress appears on the VM Status monitor.
   • To view the VM creation logs, click Manage | System.
Configuring ATD for malware analysis

Contents
- Configuring Advanced Threat Defense for malware analysis
- High-level steps to configure malware analysis
- Configure the McAfee Virtual Advanced Threat Defense network information
- Configure the security and performance options
- Configure proxy servers for Internet connectivity
- Configure DNS setting
- Configure the syslog settings
- Configuring the TAXII settings
-Configure the date and time
- Add the Advanced Threat Defense logon banner
- Configure telemetry
- Enable telemetry
- Configure Common Settings
- Configuring Email Connector
- Uploading certificates

Configuring Advanced Threat Defense for malware analysis

To configure Advanced Threat Defense or Virtual Advanced Threat Defense for malware analysis, log on to the Advanced Threat Defense web interface.

Ensure that you change the password for cliadmin from the Command-line interface and atdadmin from the web interface for the configurations to be successful. Some of the configurations might fail if you continue using the default password.
High-level steps to configure malware analysis

This section provides the high-level steps on how to configure Advanced Threat Defense for malware analysis and reporting.

1. Set up the Advanced Threat Defense Appliance and ensure that it is up and running.
   - Based on your deployment option, make sure the Advanced Threat Defense Appliance has the required network connections. For example, if you integrate it with Network Security Platform, make sure the Sensor, Manager, and the Advanced Threat Defense Appliance are able to communicate with each other.
   - Make sure the required static analysis modules, such as the McAfee Gateway Anti-Malware Engine are up-to-date.

2. Create the analyzer VMs and the VM profiles.

3. Create the analyzer profiles that you need.

4. If you want Advanced Threat Defense to upload the results to an FTP server, configure it and have the details with you before you create the profiles for the corresponding users.

5. Create the required user profiles.

6. Log on to Advanced Threat Defense web application using the credentials of a user you created and upload a sample file for analysis. This is to check if you have configured Advanced Threat Defense as required.

7. In the Analysis Status page, monitor the status of the analysis.

8. After the analysis is complete, view the report in the Analysis Results page.

Configure the McAfee Virtual Advanced Threat Defense network information

Manage the McAfee Virtual Advanced Threat Defense from virtual machine manager.

Task

1. From your client virtual machine, access the virtual machine console with these credentials.
   - User name — cliadmin
   - Password — atdadmin

2. Change your password: Provide the old password as atdadmin, followed by the new password, then re-enter the new password to confirm.
3 In the command prompt, configure the McAfee Virtual Advanced Threat Defense:
   a Set a name for McAfee Virtual Advanced Threat Defense.
      For example, set appliance name matd_appliance_1.
      The password must be an alphanumeric character string up to 25 characters. The string must begin with a letter, and can include hyphens, underscores, and periods, but not spaces.
   b Set the McAfee Virtual Advanced Threat Defense management port IP address and subnet mask.
      For example, set appliance IP xx.xx.x.x 255.255.255.0.
      Do not assign this class C network IP addresses: 192.168.55.0/24
   c Set the default gateway IP address.
      For example, set appliance gateway xx.xx.x.x.
   d Set the management port speed and duplex settings using one of the following commands:
      • set mgmtport auto — Sets the management port in auto mode for speed and duplex.
      • set mgmtport speed (10|100) duplex (full|half) — Sets the speed to 10 Mbps or 100 Mbps in full or half-duplex mode.
   e Verify the configuration.
      • To view the configuration details, run the show command.
      • To check the network connectivity, run the ping <IP address> command.
      One of these messages appears:
         • host <ip address> is alive — When the server is reachable.
         • failed to talk to <ip address> — When the host server is not reachable.
4 Restart the McAfee Virtual Advanced Threat Defense.

Configure the security and performance options
To ensure that Advanced Threat Defense runs securely and efficiently, configure the Global Settings.

Task

1 Log on to the Advanced Threat Defense web interface.
2 Click Manage | ATD Configuration | Global Settings.
3 Configure the settings, then click Save.
   To return the settings to the default configuration, click Reset Settings to Default.
Configure proxy servers for Internet connectivity

Advanced Threat Defense connects to different proxy servers for Internet connectivity. Based on the source of the traffic, Advanced Threat Defense determines the proxy server on which the Internet access requests from the traffic have to be routed.

These proxy servers can be configured on Advanced Threat Defense to handle Internet access requests:

- **GTI HTTP Proxy** — This setting is relevant for those analyzer profiles which have GTI Reputation enabled in their Analyzing Options. Advanced Threat Defense sends a query to a McAfee GTI server to fetch McAfee GTI score for the suspicious file being analyzed. If the customer network is protected under proxy, specify the proxy server details here so that the McAfee GTI queries can be sent out.

- **Malware Site Proxy** — This setting is applicable when samples being analyzed at analyzer VMs request Internet access. The proxy server specified under Malware Site Proxy handles the request. Because the traffic from an analyzer VM might be malicious, you might want to segregate this traffic from your production network.

**Tasks**

- **Configure Advanced Threat Defense to communicate with McAfee GTI on page 104**
  To use McAfee GTI with Advanced Threat Defense, configure the options.

- **Enable the malware site proxy on page 104**
  Allow analyzer VMs to connect to the internet for sample analysis.

**Configure Advanced Threat Defense to communicate with McAfee GTI**

To use McAfee GTI with Advanced Threat Defense, configure the options.

**Task**

1. Log on the Advanced Threat Defense web interface.
2. Verify that the GTI File Reputation option is enabled.
   a. Click Policy | Analyzer Profile.
   b. Select the analyzer profile, then click Edit.
   c. Select GTI File Reputation.
3. Click Manage | ATD Configuration | Proxy.
4. Configure the GTI HTTP Proxy options, then click Test.
5. Click Submit.

**Enable the malware site proxy**

Allow analyzer VMs to connect to the internet for sample analysis.

**Task**

1. Log on the Advanced Threat Defense web interface.
2. Click Manage | ATD Configuration | Proxy.
3. Configure the Malware Site Proxy options, then click Test.
4. Click Submit.
Configure DNS setting

When you execute files, the files can send DNS queries to resolve names. DNS queries are an attempt by malware to determine if they are being run in a sandbox environment. If the DNS query fails, the file might take an alternate path. When Advanced Threat Defense dynamically analyzes such a file, you might want to provide a proxy DNS service in order to bring out the actual behavior of the file.

**Before you begin**

- The DNS server is required to have access to a public domain or the internet.
- Ensure that the IP configured for DNS should be resolved by the DNS server using reverse lookup.

Malware DNS is used during VM activation, and also for any name resolution requests originating from the analyzer VM.

**Task**

1. Log on to the Advanced Threat Defense web interface.
2. Click Manage | ATD Configuration | DNS.
3. In DNS Setting, complete these settings, then click Apply.
   - Domain — Type your domain name.
   - Preferred DNS Server — Type IP address of the primary DNS server.
   - Alternate DNS Server — Type IP address of the secondary DNS server.
4. In Malware DNS Setting, type IP address of the DNS server to resolve name resolution queries originated from the sandbox environment, then click Apply.

Configure the syslog settings

The syslog mechanism transfers the Advanced Threat Defense events over the syslog channel to Security Information and Event Management (SIEM) or a logging server.

You can configure up to two external syslog server to which the following information are sent based on your configuration:

- **Analysis Results** (Malicious only or All)
- **CPU Utilization** (above a threshold percentage)
- **Memory Utilization** (above a threshold percentage)
- **HDD Utilization** (above a threshold percentage)
- **Interface Status**
- **User Login/Logout**
- **Audit Log**
- **HTTPS Session Log**
Once the user-defined threshold limit exceeds for CPU Utilization, Memory Utilization and HDD Utilization, syslog events are generated and sent to SIEM receiver. Minimum threshold level supported is 30%. Maximum threshold level supported is 90%. By default, the threshold percentage displayed under **Syslog Setting** page is 75%.

Whenever the interface link goes down or comes up, syslog events are generated and sent to SIEM receiver. Analysis results and logon/logoff events are sent to the SIEM receiver.

After syslog events are generated and sent to SIEM receiver, the information are parsed and sent to ESM. The summary is then displayed on the ESM user interface.

The SIEM receiver and ESM can be on separate appliances or can be together in a virtual environment.

**Task**

1. Log on to the Advanced Threat Defense web interface.
2. Click **Manage** | **ATD Configuration** | **Syslog**, then select **Enable Logging**.
3. In the **Statistic to Log** section, make these selections and entries as per requirement.
   - Select **Analysis Results**, then select a level from the **Severity Level** drop-down list.
   - Select **CPU Utilization** and specify the threshold level in the respective **Threshold** drop-down.
   - Select **Memory Utilization** and specify the threshold level in the respective **Threshold** drop-down.
   - Select **HDD Utilization** and specify the threshold level in the respective **Threshold** drop-down.
   - Select **Interface Status** to receive information regarding interface link status.
   - If you want to store the logon/logoff information with a time stamp, select **User Login/Logout**.
   - Select **Audit Log** to view logs for administrative actions performed on Advanced Threat Defense. **Audit Log** is selected by default.
   - Select **HTTPS Session Log** to view logs for every session established or terminated. This option is only available when **Common Criteria Mode** is enabled in **Advanced Security Settings**.
     - When **HTTPS Session Log** is enabled, Advanced Threat Defense web performance is impacted.
4. From the drop-down, select the communication protocol between your Syslog server and Advanced Threat Defense.
   - If you select **TCP/TLS Encryption**, then ensure that you upload a valid root CA certificate. You can upload the certificate from **Manage** | **Security** | **Manage Certificates** | **Trusted CA certificate**.
   - Advanced Threat Defense validates the certificates for the following.
     - CA Flag is TRUE.
     - Certificate is not expired.
     - Signature algorithm is SHA256 with RSA.
     - Certificate is not revoked.
     - Key length is 2048 bits or greater.
5 You can configure up to two syslog servers on Advanced Threat Defense. To configure the System Log Server options, do the following:
   a Enable Syslog.
   b Type the IP address or hostname of the logging server.
      In CC mode, hostname validation is done based on the logging server certificates. The communication will fail if there is a discrepancy between the hostname of the logging server and the certificate.
   c Type the port number on which the logging server is listening.
   d Enable Validate Syslog Server Certificate, to perform security checks on the syslog server certificates.
      This checkbox is available only if you chose TCP/TLS Encryption in the communication protocol.
6 Click Test Connection. When the "Test connection successful" message appears, click OK.
   When you select UDP as the Protocol from the drop-down list then Test Connection tab is disabled as UDP uses a simple connectionless transmission model rendering the connection status, unverifiable.
7 Click Submit.

### Configuring the TAXII settings

Trusted Automated eXchange of Indicator Information (TAXII™) is a transport mechanism which allows you to automate the exchange of threat information. The information is shared in the form of a STIX report to the TAXII server.

Advanced Threat Defense generates STIX report when malicious files are detected and then the report sent to your TAXII server. For Advanced Threat Defense to do so, you need to configure your TAXII server information on Advanced Threat Defense.

**Supported versions**

STIX - version 1.2

TAXII - version 1.x

Advanced Threat Defense only supports HTTPS while communicating with the TAXII server.

**Enable and configure TAXII settings**

Advanced Threat Defense generates the STIX report which is then sent to the TAXII server.

**Before you begin**

Ensure that you have configured an inbox service and set a data collection name on the TAXII server.

**Task**

1. Log on to the Advanced Threat Defense interface, then click Manage | ATD Configuration | Global Settings and select Generate STIX report.
2. Click Manage | ATD Configuration | TAXII, then select Enable TAXII Communication.
3. In URL, type the address of your TAXII server.

4. Choose None or Basic based on the authentication requirement set for your server.

   If you choose Basic, type the user name and password for authentication.

5. If your TAXII server requires TAXII client authentication, select Certificate Authentication Required.

6. Use Browse to select a certificate, then click Upload.

   - The certificate must be in PEM format.
   - Merge the private key with your certificate.
   - Ensure that the certificate key-length is 2048 bytes or above.

7. Select Enable Discovery and do the following:

   a. In Discover Service URL, type the URL for the discover service.

      This allows Advanced Threat Defense to check for available TAXII services on the TAXII server.

   b. In Collection URL, type the URL for the data collection service.

      This allows Advanced Threat Defense to request information about available Data Collections on the TAXII server.

8. In Inbox Path, type the path of the managed inbox of your TAXII server.

   Inbox Path can be read from response obtained from Discover Services.

9. In Collection Name, type the name of the collection where the STIX reports are delivered.

   Collection Name can be read from response obtained from Discover Collection.

10. Click Test Connection to check the status of the connection between Advanced Threat Defense and the TAXII server.

    The check returns the status of the following:

    - Inbox service on collection name.
    - Discovery service (if enabled)
    - Collection Service (if enabled)

11. Click Apply to save your configuration.

Once Advanced Threat Defense starts communicating with the TAXII server, the TAXII Status changes to the following:

- UP – Last attempt to send STIX report to the TAXII server was successful.

- DOWN – Last attempt to send STIX report to the TAXII server was unsuccessful. This status can also appear if the TAXII settings are not configured or incorrect.

- UNKNOWN – Connection status is not yet verified by Advanced Threat Defense.
**Configure the date and time**

Advanced Threat Defense uses the date and time that you configure for all its functional and display purposes. The date and time displays on the Advanced Threat Defense web interface, reports, log files, and CLI.

To use the Network Security Protocol server domain names, make sure you have configured the DNS servers.

You can either manually specify the date and time or configure Network Time Protocol (NTP) servers as the time source for Advanced Threat Defense. If you specify NTP servers, you can configure up to 3 Network Time Protocol (NTP) servers. In this case, Advanced Threat Defense acts as an NTP client and synchronizes with the highest priority NTP server that is available.

- By default, synchronization with NTP servers is enabled in Advanced Threat Defense. Also, pool.ntp.org is configured as the default NTP server. The default time zone is Pacific Standard Time (UTC-8).
- When you upgrade from a previous version without selecting the **Reset Database** option, the date and time settings from the previously installed version are preserved. If you upgrade with the **Reset Database** option selected, the default date and time settings as described above are set.
- At any point in time, there must be at least one valid NTP server specified in the **Date and Time Settings** page of Advanced Threat Defense. You can add, edit, or delete the list of NTP servers specified in Advanced Threat Defense.
- Based on the access available to Advanced Threat Defense, you can specify public NTP servers or the ones locally on your network.
- You can specify the domain name or the IPv4 address of NTP servers. If you specify the domain names, then you must have configured DNS settings in Advanced Threat Defense.

> If you specify public NTP servers, then using the domain names instead of IP addresses is recommended. The domain of a public NTP server might resolve to different IP addresses based on various factors.

- Whether you enable NTP server synchronization or manually set the date and time, you must select the required time zone in the **Date and Time Settings** page. If you configure an NTP server, Advanced Threat Defense considers only the date and time from the NTP server. But for the time zone, it relies on what is specified in the Date and Time Settings page.
- The date and time on a Advanced Threat Defense client has no impact on the timestamps that are displayed. Consider that the current time on the Advanced Threat Defense Appliance is 10 am PST (UTC-8). Regardless of the time zone from which you access this Advanced Threat Defense Appliance, all the timestamps are displayed in PST only. That is, the timestamps are not converted based on a client's date and time.
- When the current date and time settings are changed, the timestamp for all the older records are also changed accordingly. Consider that the current time zone is PST (UTC-8) and you change it to Japan Standard Time (UTC+9). Then the timestamp for the older records are all converted as per Japan Standard Time (JST). For example, if the timestamp displayed for a record in the **Analysis Status** page was 0100 hours (1 am) PST before you changed the time zone. After you change the time zone to JST, the timestamp for the same record is 1800 hours JST.
- The date and time settings of all the analyzer VMs are immediately synchronized to the date and time on the Advanced Threat Defense Appliance.

**Task**

1. Log on to the Advanced Threat Defense web interface.
2. Click **Manage | ATD Configuration | Date & Time**.
3. Configure the **Date and Time Settings**, then click **Submit**.
Add the Advanced Threat Defense logon banner

Upload custom text to the Advanced Threat Defense logon page.

**Task**

1. Log on to the Advanced Threat Defense web interface.
2. Click Manage | Security | Advanced Security Settings.
3. Select Display Login Banner.
4. In the Banner Message field, enter the logon message.
   
   ![Information icon] You can only use the ASCII character set. The maximum number of characters you can use is 1024.

5. Click Save.

Configure telemetry

Telemetry allows Advanced Threat Defense to collect data about malware and the Advanced Threat Defense Appliance.

The data contains useful information about threat trends and product feature usage. The data is retained for 6 months, then deleted. Metadata, such as summary of the threat trends and feature usage, are maintained indefinitely. McAfee Advanced Threat Defense Telemetry data is collected and aggregated in the USA, then stored with our research team in India.

![Information icon] The data collected do not include personally identifiable information (PII) of the customer or end user.

Advanced Threat Defense captures these two categories of data.
### Table 7-1 Category definitions

<table>
<thead>
<tr>
<th>Category</th>
<th>Definition</th>
</tr>
</thead>
</table>
| Telemetry data that Advanced Threat Defense uses for the Advanced Threat Defense Appliance. | Advanced Threat Defense collects Advanced Threat Defense Appliance telemetry data to:  
• Improve Advanced Threat Defense  
• Understand how the Advanced Threat Defense Appliance is used  
The system data that Advanced Threat Defense collects includes:  
• Serial number  
• Software version  
• Whether Syslog is enabled  
• Whether LDAP is enabled  
• Whether McAfee ePO is enabled  
• Whether SNMP is enabled  
• Whether proxy settings are configured  
• Whether Load Balancing is enabled  
• Whether TIE is enabled  
• Number of documents submitted  
• Number of flash files submitted  
• Number of Microsoft Word files submitted  
• Number of PDF files submitted  
• Number of files scanned by McAfee Gateway Anti-Malware  
• Number of files scanned by McAfee GTI  
• Number of files scanned by VirusScan Enterprise  
• Number of files scanned by YARA  
• Number of files analyzed by the sandbox  
• Number of files submitted to the sandbox  
• Version of the Detection Package downloaded |
| Telemetry data for:  
• McAfee GTI  
• McAfee Labs | McAfee Labs requires the analysis results from Advanced Threat Defense telemetry data to:  
• Update the McAfee Labs databases  
• Categorize the samples and malware that Advanced Threat Defense analyzes  
Telemetry data contains information about the analyzed samples, and includes:  
• SHA-1 of sample  
• SHA-256 of sample  
• MD5 hash value of sample  
• Advanced Threat Defense detection score  
• Digital signature data from sample  
• Parent metadata corresponding to dropped files  
• Advanced Threat Defense product information |
Table 7-1  Category definitions (continued)

<table>
<thead>
<tr>
<th>Category</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Advanced Threat Defense analyzing option scores</td>
</tr>
<tr>
<td></td>
<td>• URL visited by file</td>
</tr>
<tr>
<td></td>
<td>• IPv4 address visited by file</td>
</tr>
<tr>
<td></td>
<td>• Product version that the sample belongs to</td>
</tr>
<tr>
<td></td>
<td>• Publisher name of the sample</td>
</tr>
<tr>
<td></td>
<td>• Product name that the sample belongs to</td>
</tr>
<tr>
<td></td>
<td>• File version of the sample, OS name, and OS version on which the file was found on</td>
</tr>
</tbody>
</table>

**Enable telemetry**

Advanced Threat Defense sends system telemetry data only when you allow automatic updates.

**Task**

1. Log on to the Advanced Threat Defense interface.
2. Click **Manage** | **Image & Software** | **Content Update**.
3. Under **Allow Automatic Update**, click **Apply**, then click **OK**.
4. Click **Manage** | **ATD Configuration** | **Telemetry**.
5. Ensure that the following options are selected, then click **Submit**.
   - Send feedback to McAfee about system information in order to improve the product.
   - Send feedback to McAfee about potential malicious files and urls.

   *These options are enabled by default.*

**Configure Common Settings**

Configure the **Max Wait-Time Threshold** for analyzing samples received from Email Gateway. Also, you can use this page to enable **Common Criteria (CC)** mode in Advanced Threat Defense.

**Configure maximum threshold wait time**

Advanced Threat Defense allows you to configure the maximum wait time for analyzing samples received from McAfee Email Gateway. If the average analysis time of samples in Advanced Threat Defense is more than the threshold set, the samples submitted by McAfee Email Gateway are rejected.

*In a load-balancing scenario, the threshold wait time is 3 hours.*
Follow the steps below to configure the maximum wait time for analyzing samples received from McAfee Email.

1. Go to Manage | ATD Configuration | Global Settings.
2. In the Performance Tuning area, set the threshold wait time.

**Enable Common Criteria (CC) mode**

You can enable Common Criteria (CC) mode in Advanced Threat Defense. On enabling the CC mode, you will see various security warning which you can either accept or fix the security warning by reviewing the Security Logs.

### Before you begin

Enable logging to enable Common Criteria mode in Advanced Threat Defense.

In Common Criteria (CC) mode:
- the minimum TLS version is set to 1.2.
- FTP Access, HTTP Port, and Force HTTPS options are disabled.
- Advanced Threat Defense uses only SSL connections with NSP.
- Web server and Syslog server certificates are strictly validated. Ensure the following:
  - Root CA certificate for Web server and syslog server are uploaded in Trusted CA certificate. The root CA should be trusted by Advanced Threat Defense for any communication with syslog server and web server, else the communication will fail.
  - Certificate validation checks for valid certificate validity, key length, signature algorithm, chain validation, extended purpose and revocation.
  - Syslog server, Web server, and all intermediate certificates must have either OCSP or CRL (only HTTP URL is supported) information included else chain validation will fail.
  - Syslog server, Web server, and all intermediate certificate have Authority Information Access extension information of issuer CA (only HTTP URL is supported).

### Task

1. Log on to the Advanced Threat Defense web interface.
2. Click Manage | ATD Configuration | Syslog, then select Enable Logging.
3. Configure the System Log Server options, then click Test connection to test the connection.
4. In the Statistics to Log area, make sure Audit Log is checked. By default Audit Log is enabled.
5. Click Submit.
   
   Audit function starts as Advanced Threat Defense boots up and stops with Advanced Threat Defense shutdown. The function restarts in the following two scenarios.
   - Change in Syslog certificate
   - Manual change in Date and Time information
Enable account lock out

You can configure Advanced Threat Defense to lock accounts after a defined number of invalid logon attempts. You can also define the time period the account remains locked. During this time, the user cannot log on to Advanced Threat Defense until the lock out period is elapsed.

Task

1. Log on to the Advanced Threat Defense web interface.
2. Click Manage | Security | Advanced Security Settings.
3. Select Enabled Account Lock Out, then set the lock out duration and the number of allowed incorrect logon attempts.
   - Duration of Lock Out in Minutes – Set the duration of the lock out period in minutes.
   - Maximum Login Retries – Set the number of allowed incorrect logon attempts, after which the account is locked.

Configuring Email Connector

Email Connector protects you from email borne threats by analyzing email attachments through Advanced Threat Defense.

- Email Connector is not installed with Advanced Threat Defense. For more information on installing Email Connector, see McAfee Advanced Threat Defense Installation Guide.
- If you have configured a cluster, ensure that you install Email connector in your primary as well as the backup nodes.
- Ensure that you have reset your cliadmin password. If you continue using the default password, the configurations might fail.

Advanced Threat Defense receives emails from a secure email gateway, performs an analysis on the email attachments, adds a verdict in the email header and sends it back to the email server. You can view the analysis report from Analysis | Email Reports on your Advanced Threat Defense web interface.

While you view the reports, the maximum number of reports you can navigate to are one million. If you want to view the reports beyond one million, use the search filter to reduce the result of the number of reports.

You need to configure your email gateway to send emails to the Advanced Threat Defense for analysis. You can add filters such as send the ones with attachment only and so on. We recommend you configure your SEG to send emails for analysis to Advanced Threat Defense only when your SEG’s AV analysis have returned an inconclusive result.

Enable and configure Email Connector

Enable Email Connector and configure options for the Secure Email Gateway (SEG) from where the emails are received, file analysis settings, and destination SEG or message transfer agent (MTA) to which the emails with analysis headers are forwarded.
Task

1. Log on to the Advanced Threat Defense interface, then click Manage | Email Connector | Configuration.

2. In Email Connector Configuration, select Enable Email Connector, and then choose:
   - **Inline Mode (hold email until decision made)** – Emails are delivered to an onward SEG or MTA after Advanced Threat Defense scan.
   - **Offline Mode (send copy of email to ATD for analysis)** – Emails are discarded from Advanced Threat Defense after a scan. The email and analysis reports are maintained on Advanced Threat Defense.

   *Smart host need not be configured if you choose Offline Mode.*

3. In Receiving Email, complete these settings.
   - **Listen Port** — Type the port number to use for receiving emails. The default port number is 25.
   - **Use TLS Connection** — Select one of the three options from the drop-down to use TLS-secured communication, when available, always, or not use at all for receiving emails.
   - **Permitted Hosts** — From the drop-down, select the Host type as IP address, Hostname, or Network, then enter the IP addresses, host name, or network address of the source SEG for Advanced Threat Defense to receive emails. Click Add to add an IP address.

4. In Sending Email, complete these settings.
   - **Smart Host Hostname** — Type the IP address or hostname of the destination SEG or MTA.

   *This is usually the same as the Permitted Host.*

   - **Smart Host Port** — Type the port number of the destination email server. The default port number is 25.
   - **Use TLS Connection** — Select one of the three options from the drop-down to use TLS-secured communication, when available, always, or not use at all for sending emails.
   - **Test Connection** — Click Test Connection to ensure that the configured email server is reachable.

5. In Scanning Email, complete these settings.
   - **Maximum time per email to wait for all scans to complete** — The maximum time (in seconds) within which the analysis must complete. The analysis times-out when the time exceeds the time specified and the email is queued in the SEG. Default is 600.
   - **Scan these file types** — File types of the email attachments that can be scanned. Select All or a minimum one of the file types.
   - **Skip Protected Files** — Ignores protected files from the scanning.
   - **Action when system is overloaded** — Choose whether to deliver emails without scanning or drop SMTP connections when the system is overloaded.

   *If you've selected Deliver emails unscanned, then the emails are delivered with the X-ATD-VERDICT as -8.*

6. In Attachment Profiling, complete these settings.
   - **Enable Profiling Mode (Attachments will not be scanned in this mode)** – Enables email profiling. This option disables scanning the email attachments. Only email count is incremented and sent to the transporting email server.

   *If you enable this option, the header X-ATD-VERDICT -7 is added to the emails.*
• **Document Format** – Select the format in which you want your profiling report to get generated.

• **Reporting Period** – Select the period for which you want the emails to be profiled.

• **Granularity** – Select the period in a granular level.

• **Download Report** – Downloads a report about the overall email attachment profiling.

7 Click **Apply**.

You can view the total number of emails and attachments analyzed in the **Email Counter** monitor from the **Dashboard**.

**Configuring your Secure Email Gateway for Email Connector**

For optimal performance, it is important that you configure your Secure Email Gateway.

Advanced Threat Defense does not accept emails from the sending Secure Email Gateway (SEG), until:

1. the scan is complete

2. the message is delivered to the configured smart host if you chose **Inline mode** or is deleted if you chose **Offline mode**.

**Setting up SEG timeout**

When attachments are required a full Sandbox scan, emails sent to Advanced Threat Defense could take several minutes to scan.

Setting the right timeout on your SEG is important, so that it waits until the Advanced Threat Defense scan is complete. A suitable value for timeout depends on the settings for the analyzer profile configured for your Email Connector.

If the timeout is too short and an Advanced Threat Defense scan is in progress, Advanced Threat Defense doesn't accept the email. At such times, the source SEG would requeue the message for delivery back to the ATD for a later time. Depending on the retry period set on your SEG and the load on Advanced Threat Defense, cached results can be available at the time a subsequent delivery attempt is made. This could lead to the timeout to not trigger again. The default timeout value is 10 minutes.

**Setting Advanced Threat Defense as a permitted host in your SEG**

Depending on your SEG and its configuration, you might be required to include the IP address of the Advanced Threat Defense appliance to your SEG. This allows Advanced Threat Defense to deliver the scanned messages to your SEG.

**Setting up SEG functions**

Your SEG is expected to perform all anti-spam, anti-virus, or other blocking and filtering functions. Advanced Threat Defense does not perform any of these SEG functions. Messages to Advanced Threat Defense must be redirected only when the SEG:

• is not sure about the content of the email

• requires an Advanced Threat Defense verdict to enforce a policy accordingly.

**Configure Email Connector filtering rules**

Create rules to exclude email attachments from analysis.
Task

1. Log on to the Advanced Threat Defense interface, then click **Manage** | **Email Connector** | **Filtering Rules**.

2. Type a name for the rule, then select one or a combination of these filtering options.
   - **File Name** — Add file names separated by semi-colons (;). * and ? can be used as wildcard characters.
   - **File Size** — Select less than or greater than criteria, type the file size, then select the unit.
   - **File Type** — Select the file types to exclude.

3. Click **Add Rule**.

   The rule is added in the Filtering Rules table.

**Understanding Email Headers with analysis status**

After analyzing the email attachment for threats, Advanced Threat Defense updates adds these headers of the respective emails with the observations, and sends the emails to the configured transporting email server or MTA.

<table>
<thead>
<tr>
<th>Header</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>X-ATD-FILENAME</td>
<td>Lists the names of all attachments of the email separated by comma(,)</td>
</tr>
<tr>
<td>X-ATD-ALTFILENAME</td>
<td>Lists the alternate names of scanned attachments that have the same hash value as determined during the earlier scans. For example, if after scanning a file (file1), another attachment with the same hash but a different file name (file2) is detected, the X-ATD-ALTFILENAME header is added with the value file1, file 2.</td>
</tr>
<tr>
<td>X-ATD-FILEHASHES</td>
<td>Adds the hashes of all email attachments. For example, MD5, SHA-256.</td>
</tr>
<tr>
<td>X-ATD-FILEVERDICTS</td>
<td>Adds the verdict for each email attachment that was submitted for analysis.</td>
</tr>
<tr>
<td></td>
<td>• 5 — Very high (risk)</td>
</tr>
<tr>
<td></td>
<td>• 4 — Malicious</td>
</tr>
<tr>
<td></td>
<td>• 3 — Likely to be malicious</td>
</tr>
<tr>
<td></td>
<td>• 2 — Low activities</td>
</tr>
<tr>
<td></td>
<td>• 1 — Very low activity</td>
</tr>
<tr>
<td></td>
<td>• 0 — Informational</td>
</tr>
<tr>
<td></td>
<td>• -1 — Clean</td>
</tr>
<tr>
<td></td>
<td>• -2 — Failed to scan (because of unsupported file type)</td>
</tr>
<tr>
<td></td>
<td>• -3 — Scan Timed out</td>
</tr>
<tr>
<td></td>
<td>• -4 — Filtered by the File Type Configuration</td>
</tr>
<tr>
<td></td>
<td>• -5 — Filtered by File Filtering Rules</td>
</tr>
<tr>
<td>Header</td>
<td>Values</td>
</tr>
<tr>
<td>------------------</td>
<td>--------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>X-ATD-VERDICT</td>
<td>Adds the overall verdict for an email.</td>
</tr>
<tr>
<td></td>
<td>• 5 — Very high (risk)</td>
</tr>
<tr>
<td></td>
<td>• 4 — Malicious</td>
</tr>
<tr>
<td></td>
<td>• 3 — Likely to be malicious</td>
</tr>
<tr>
<td></td>
<td>• 2 — Low activities</td>
</tr>
<tr>
<td></td>
<td>• 1 — Very low activity</td>
</tr>
<tr>
<td></td>
<td>• 0 — Informational</td>
</tr>
<tr>
<td></td>
<td>• -1 — Clean</td>
</tr>
<tr>
<td></td>
<td>• -2 — Failed to scan (because of unsupported file type)</td>
</tr>
<tr>
<td></td>
<td>• -3 — Scan timed out</td>
</tr>
<tr>
<td></td>
<td>• -6 — No file attachments was scanned</td>
</tr>
<tr>
<td></td>
<td>• -7 — Silent Mode (When Advanced Threat Defense is set to disable file scanning, where the</td>
</tr>
<tr>
<td></td>
<td>emails attachment are not scanned and only email count is incremented for every email)</td>
</tr>
<tr>
<td></td>
<td>• -8 — Advanced Threat Defense is too busy to service new scanning requests. At least one</td>
</tr>
<tr>
<td></td>
<td>attachment has not been scanned and does not have a cached result (see X-ATD-TOOBUSY)</td>
</tr>
<tr>
<td></td>
<td>• -100 — Advanced Threat Defense failed to receive or deliver the emails</td>
</tr>
<tr>
<td>X-ATD-SILENtmODE</td>
<td>Adds the value of 1 if an email was scanned in silent mode. Otherwise this header is not added.</td>
</tr>
<tr>
<td>X-ATD-TOOBUSY</td>
<td>Adds this header to all messages that pass through Advanced Threat Defense while it is:</td>
</tr>
<tr>
<td></td>
<td>• processing new attachments for scanning</td>
</tr>
<tr>
<td></td>
<td>• configured in Email pass-through mode.</td>
</tr>
</tbody>
</table>

The X-ATD-TOOBUSY value is always 1. Since Advanced Threat Defense includes a results cache, the X-ATD-VERDICT should be referenced to determine whether the attachments were scanned in a previous submission.

## Uploading certificates

For authentication, Advanced Threat Defense requires you to upload trusted CA and web certificates.

The certificate must have a key in PEM format. The key length must be 2,048 bits or above, and the signature algorithm must be SHA256 minimum standards with an RSA encryption. If Advanced Threat Defense is unable to detect the key, you'd be prompted to upload a valid key. If your certificate has a valid key but fails validation, the Certificate is invalid message appears, and you'd be prompted to upload a valid certificate or continue with the existing certificate. Upon uploading a valid certificate that passes the validation, the web server restarts, and you must log back in to the Advanced Threat Defense web interface.

When you upload a certificate, Advanced Threat Defense checks for the certificate and key in the same PEM file (certificate and private key concatenation), then validates the metadata. Post validation, you might see security warnings as a result of the validation which you may accept or fix.
**Trusted CA Certificates**

Upload all trusted root and intermediate CA certificates in the Trusted CA Certificates section. Certificate chain validation will pass only if the root CA is in the trusted CA certificates.

![](warning)
Ensure that you first upload the root CA certificate first, before you upload any intermediate CA certificates.

**Web Certificates**

Upload all web server certificates in the Web Certificates section. Certificate will be validated for basic checks in non-CC mode and strict checks in CC mode.

![](warning)
Ensure that you have uploaded all root CA certificates before you upload the web server certificates.

**Upload trusted CA certificates**

Upload trusted root and intermediate CA certificates.

**Task**

1. Log on to the Advanced Threat Defense web interface.
2. Click Manage | Security | Manage Certificate.
3. In the Trusted CA Certificate Upload section, click Browse.
   ![](info)
   You can only upload one certificate at a time.
4. Locate and select the certificate, then click Open, and then click Upload.

   Once the certificate is uploaded, Advanced Threat Defense validates the CA certificate for validity, CA flag, signature algorithm, revocation, extended usages, and chain validation (if not a root CA).

**Upload web certificates**

For web server authentication, Advanced Threat Defense requires you to upload web server certificates.

**Before you begin**

Ensure that you have uploaded the root CA certificate before uploading the web server certificate.

**Task**

1. Log on to the Advanced Threat Defense web interface.
2. Click Manage | Security | Manage Certificate.
3. Click Browse next to the following:
   - Web Certification
   - CA Certificate
   ![](info)
   If you have already uploaded the Trusted CA Certificate, you need not upload CA Certificate.
4 Locate and select the certificate, then click **Open**.

5 Click **Upload**.

> In non-CC mode, the certificates are validated for basic check. In CC mode, the certificates are validated strictly.
Index

A
 Account
  lock out period 114
 analysis status 117
 analyzer VM
  creating 53

C
 clean install 25, 27
 Common Criteria 113
 configure
  email connector 114
 Configure SEG 116
 custom YARA rules 112

D
 date and time 109
 DNS settings configuration 105, 110

E
 Email Connector
  Overview 114
 Email headers 117

G
 global settings, configuration 103

H
 hardware specifications 15

I
 install
  advance threat defense software 28
  Email Connector 38
  OS 25, 27
  Remotely 27
  through RMM 27
 Internet proxy server 104

L
 logon banner, customize 110

M
 malware analysis configuration
  high-level steps 102
  overview 101
 McAfee Advanced Threat Defense
  deployment options 7
  software import 47
  upgrade 47

P
 package details
  Advanced Threat Defense software 24
  Email Connector 24
  OS 24
  Virtual Advanced Threat Defense software 24
 port numbers used 18

S
 Secure Email Gateway Configuration 116
 SEG timeout 116
 system requirements
  client 9, 41

T
 telemetry
  enable 112
 type of users
  atdec 45
  command-line interface admin 44
  email gateway admin 44
  super admin 44
  tie admin 45
  virtual nsp admins 45
  web gateway admin 44

U
 Upload certificates
  CA Certificate 119
  Trusted CA Certificate 119
  Web Certificate 119
 users management 43
Index

V
VM profile
  adding 98
  creating 98
  deleting 98
  editing 98
  management 97, 98
  viewing 98
VMDK file
  image conversion 96
VMDK file, create 67
VMDK or VHDX file
  importing 96

W
warnings 20
web interface
  accessing 42

X
Xmode 41

Y
YARA rules 112