Addendum

McAfee Virtual Advanced Threat Defense 4.0

Contents

Contents

1 Using McAfee Virtual Advanced Threat Defense

McAfee® Virtual Advanced Threat Defense is a virtual appliance version of the on-premise McAfee® Advanced Threat Defense software.

The McAfee Virtual Advanced Threat Defense inherits most of the features from the on-premise version of the McAfee Advanced Threat Defense software. This document provides information about the McAfee Virtual Advanced Threat Defense specific installation steps, deployment requirements, McAfee Advanced Threat Defense features that are supported and not supported, and how to access the McAfee Virtual Advanced Threat Defense interface. For information about all common features, see *McAfee Advanced Threat Defense Product Guide*. For information about McAfee Advanced Threat Defense APIs, see *McAfee Advanced Threat Defense API Reference Guide*.

Contents

Key features

McAfee Virtual Advanced Threat Defense provides these features.

The McAfee Virtual Advanced Threat Defense inherits most of the features from the on-premise version of the McAfee Advanced Threat Defense software.

Feature	Description
Detection of file downloads	Detects when a user tries to download a file from an external resource.
Analysis of the file for malware	Verifies if the file contains any known malware.
Block future downloads of the same file	Prevents future downloads of the file or its variants if the file is found to be malicious.
Identify and remediate affected hosts	Identifies the host that executed the malware, and also detects the hosts to which it has spread. Then, it must provide an option to quarantine the affected hosts until they are clean.
Local blacklist	Checks for a known malware using a local blacklist.
Cloud-lookups	Integrates with the McAfee® Global Threat Intelligence™ (McAfee GTI) to detect malware that has already been identified by organizations throughout the globe.
Emulation capabilities	Integrates with McAfee® Gateway Anti-Malware Engine for emulation capabilities.
Signature-based detection	Includes the McAfee® Anti-Malware Engine for signature-based detection.

Feature	Description
Sandboxing capability (Dynamic analysis)	Analyzes the file by executing it in a virtual sandbox environment to determine whether the file is malicious.
VMWare Tool	Enhances the performance of the VM operating systems and improves management of the virtual systems. The VMWare utility is pre-installed with McAfee Virtual Advanced Threat Defense.

How it works

McAfee Virtual Advanced Threat Defense is a 64-bit virtual software version of the on-premise McAfee Advanced Threat Defense software that facilitates detection and prevention of malware.

The files are first checked for known malware, then run in a sandbox environment. The sandbox provides a controlled environment where Network access is usually disallowed or heavily restricted.

You can deploy it on a VMware ESXi virtual machine environment. Once the virtual appliance is deployed and set up, you can manage McAfee Virtual Advanced Threat Defense through its web-interface in a browser from your management computer.

Unsupported features in the virtual deployment

These McAfee Advanced Threat Defense features are not supported in the virtual appliance.

Except these features, all other features of the on-premise McAfee Advanced Threat Defense software are supported with McAfee Virtual Advanced Threat Defense. For information about the rest of the features and how to use them, see *McAfee Advanced Threat Defense 4.0 Product Guide* and *McAfee Virtual Advanced Threat Defense 4.0 Addendum*.

ATD feature	Description
CLI commands	These command line interface commands are not supported with McAfee Virtual Advanced Threat Defense: • `show rmm info`

2 Installation, deployment, and upgrade

McAfee Virtual Advanced Threat Defense is a 64-bit virtual appliance version of the on-premise McAfee Advanced Threat Defense software. Deploy it on a VMware ESXi 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.

Contents

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 server.

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

Requirement	Details
Hypervisor support	• VMware ESXi 5.5 server: Hardware version 9, 10 • VMware ESXi 6.0 server: Hardware version 9, 10, 11
VM file format	Open Virtualization Appliance (OVA)
Virtual CPUs	• Small scale deployment — 16 • Mid scale deployment — 32 • Large scale deployment — 48 • Extra large scale deployment — 64

Requirement	Details
Virtual Memory	• Small scale deployment — 32 GB • Mid scale deployment — 64 GB • Large scale deployment — 128 GB • Extra large scale deployment — 256 GB
Virtual Disk	• Small scale deployment — 750 GB • Mid scale deployment — 1.5 TB • Large scale deployment — 3 TB • Extra large scale deployment — 6 TB
Physical Network Interface	2 (E1000)
Virtual Network Interfaces	2 (Management interface—1; Malware interface—1)
Physical system setting	Enable Virtualization Technology option in BIOS.

Physical server requirements

To deploy McAfee Virtual Advanced Threat Defense on explicit servers, make sure that your server meets these requirements.

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

Install a McAfee Virtual Advanced Threat Defense instance

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_0_2_42-61882-60905.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.

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 9
  Activate your McAfee Virtual Advanced Threat Defense software using the temporary license key.
- *Activate the product using the permanent key* on page 10
  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.

McAfee Virtual Advanced Threat Defense model	Number of McAfee Virtual Advanced Threat Defense installations	Number of McAfee Virtual Advanced Threat Defense VMs (8 per installation)
1008	1	8
1016	2	16
3032	4	32
6064	8	64

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.

3 Cluster Deployment

When you have a heavy load of files to be analyzed for malicious content, you can cluster two or more Virtual Advanced Threat Defense Appliances. So, the analysis load is efficiently balanced between the Virtual Advanced Threat Defense Appliances (nodes) in the cluster.

Cluster Requirement

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

- Use the Virtual 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 same EXSi server. The Secondary nodes can be on same or a different ESXi server.

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

Create the Virtual Advanced Threat Defense cluster

Before you begin

- You have admin-user rights for the primary node's web application.
- The primary and secondary nodes are not part of any other cluster.
- The software version (active version) of all nodes that you plan to use are an exact match.

Task

1 Identify a Virtual Advanced Threat Defense Appliance as the primary node and log on to its web application.

Use a user name that has admin rights.

2 Select **Manage** | **Load Balancing.**

The **Load Balancing Cluster Setting** page displays.

3 In the **Node IP address** field, enter the management port IP address of the primary node, select **Primary** from the drop - down and click **Add Node.**

4 Confirm if you want to create the cluster.

Virtual Advanced Threat Defense sets itself as the primary node for the cluster.

5 In the **Node IP address** field, enter the management port IP address of a secondary node, select **Secondary** and click **Add Node.**

6 Click **Yes** to add the secondary node.

When you click **Yes** in the confirmation message box, the primary node saves its configuration in a file and sends this to the secondary node. This file contains those configurations, which this document refers to as synchronized configuration. See *How does the Advanced Threat Defense cluster work?* in the *McAfee Advanced Threat Defense Installation Guide*. for information on synchronized configuration. The secondary uses this configuration file to overwrite the corresponding configuration in its database. So, make sure that you have taken a backup of the secondary's configuration before you proceed. When you remove the secondary from the cluster, it retains the primary node's configuration.

7 Following a similar procedure, add the other secondary nodes.

8 In the **Cluster IP address** field, enter cluster IP address and click **Save**. Select **Backup** from the drop - down and enter the management port IP address of the Backup node in the **Node IP address** field. Click on **Add Node**, Backup node will now be added.

Configuring or changing Cluster IP resets all SFTP services.

9 The details of all nodes in the cluster are displayed in a table. Similar to other tables in the Virtual Advanced Threat Defense web application user-interfaces, you can sort the columns as well as hide or display the required columns.

Except for **ATD ID, IP Address, Role,** and **Withdraw From Cluster**, none of the options are available in the **Load Balancing Cluster Setting** page for the secondary nodes.

Table 3-1 Option definitions

Option	Definition
Node IP address	Enter the management port IP address of the Virutal Advanced Threat Defense Appliance that you want to add to the cluster.
Drop - Down	Select Primary / Backup / Secondary as per the requirement.
Add Node	Click to add the primary, secondary and backup node to the cluster. The primary node or secondary node IP address is the IP address that you use to access the Advanced Threat Defense web application.
Cluster IP address	Enter the cluster IP address to be used by Active node (Primary node or Backup node).
Save	Click to save the cluster IP before adding Backup node.

Table 3-1 Option definitions *(continued)*

Option	Definition
	Indicates the status of a node. •  : Indicates that the node is up and ready. If it is a secondary, it also means that the primary node is receiving the secondary's heartbeat signal. •  : Indicates that the node is up but needs your attention. For example, the configuration might not be in sync with that of the primary. •  : Indicates that the primary node is not receiving the secondary node's heartbeat signal. Also indicates VM synchronization failure in the node. The primary node distributes files only to those nodes, which are in the green status. If the status of a secondary node turns red midway of a file transfer, the primary node allocates the file to the next node in queue. If all the secondary nodes are in overloaded state, then samples get distributed among the nodes in round robin fashion, even when the nodes are in amber status.
ATD ID	This is a system-generated integer value to identify the nodes in a cluster. The primary node generates this unique value and assigns it to the nodes in the cluster. This ID is displayed in the Analysis Status and Analysis Results left-hand-side tree structure on the primary node. This enables you to identify the node that analyzed a specific sample. The uniqueness of the ATD ID is based on the IP address of a node as stored in the primary node's database. Consider that you have 3 nodes in the cluster. You remove the secondary node with ATD ID 2 from the cluster and add it back again to the cluster. Then this secondary node is assigned the same ATD ID of 2 if all these conditions are met: • You have not changed the IP address of the node's eth-0 interface (management port). • The primary node's database still has a record for the secondary's IP address.
IP Address	The management port IP address of the node.
Model	The Virtual Advanced Threat Defense appliance model type. It could be either 1008, 1016, 3032, or 6064.
Role	Indicates if a node is a primary or a secondary or a backup node. It also indicates which node is currently behaving as Active node.
Config Version	When you save any of the synchronized configuration, the primary node sends its configuration file to the secondary nodes and also versions this configuration file for reference. For each node, the version number of its latest configuration file is displayed. If the version number of a secondary node does not match with that of the primary, it indicates a possible difference in how the secondary node is configured. So, the status color for that secondary node turns to amber. The reason is also mentioned in the **State** column. Also, the primary node automatically pushes its configuration file to that node. This ensures that all nodes are configured similarly concerning synchronized configuration.
S/W Version	Indicates the Virtual Advanced Threat Defense software version of the nodes. The complete software version must exactly match for all nodes. If not, the status turns to amber for the corresponding nodes.

Table 3-1 Option definitions *(continued)*

Option	Definition
State	Indicates the status of node and any critical information related to that node. Some possible states are: • Up and Ready: Indicates that the node is ready to receive samples • Heartbeat not received • Node is on different config version • Node Overloaded: Indicates that the total amount of average processing time for all the samples submitted exceeds Max Wait-Time Threshold (780 seconds, by default). The threshold value can be configured using the following path. Select **Manage** | **Common Settings** | **Performance Tuning**. Use CLI command `show filequeue` to check the current average processing time of the submitted samples.
Remove Node	Select a node and click to remove the node from the cluster. The configuration from the primary node is retained even when you remove a secondary node from the cluster. You cannot remove a primary node or a Backup node, if it is in active state, before you remove all secondary nodes. This option is not available for a secondary node.
Sync All Nodes	Click **Sync All** to trigger the configuration-synchronization for all secondary nodes in the cluster. When you add a secondary node or when you save any of the synchronized configuration in the primary node, the primary automatically triggers a synchronization to all secondary nodes in green and amber state. Details of the configuration sync are displayed for each node based on the success or failure of the synchronization.
Sync All VMs	Manually triggers the synchronization of primary node and secondary node VMs in a cluster. This function is applicable only when you have a synchronization error between primary node and secondary node VMs. Synchronizing VMs should be carried out during downtime, as it will trigger synchronization of VMs in all the nodes in cluster and nodes will not participate in sample analysis.
Withdraw from Cluster	This button is relevant only for secondary nodes. Click to withdraw a secondary node from the cluster and to use the secondary node as a standalone Virtual Advanced Threat Defense Appliance. Recall that if the primary and Backup nodes are down simultaneously, the load-balancing cluster is down. In the aforementioned case, click **Withdraw from Cluster** in the secondary nodes to withdraw from the cluster and to use the secondary nodes as stand-alone appliances.

4 Upgrading the software

Upgrade the Virtual Advanced Threat Defense software

When you upgrade the Virtual Advanced Threat Defense software:

- Post upgrade, you cannot to use system.msu to downgrade the Virtual Advanced Threat Defense software.
- OpenSSL automatically upgrades.

Contents

Download the product files

Download the Advanced Threat Defense product files from Intel Security Downloads page.

Task

1 Go to the McAfee Downloads page.

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

3 Click **Network Security Reseller Support** | **Advanced Threat Defense Software**.

Package name: system-4.0.2.42.61877.msu

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

Complete the upgrade

Upgrade the Virtual Advanced Threat Defense software.

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 the upgrade package to the Virtual Advanced Threat Defense root directory.

Installation package: system-4.0.2.42.61877.msu

Ensure that the transfer mode is binary.

3 Use the following to upgrade the Virtual Advanced Threat Defense software, then repeat these steps to upgrade the Android analyzer VM.

   a Log on to the Virtual Advanced Threat Defense web interface as the `admin`.

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

   c From the **System Software** drop-down list, select the upgrade package.

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

5 Log on to the VirtualAdvanced 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.

   Virtual 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 your Virtual Advanced Threat Defense.

View the upgrade log

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

Task

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

2 Click **Manage** | **Logs** | **Upgrade**.

5 Configuring the McAfee Virtual Advanced Threat Defense software

Set up your environment for McAfee Virtual Advanced Threat Defense software, then access its interface in a web browser same as that of the McAfee Advanced Threat Defense interface.

This section provides information about setting up your software and accessing the McAfee Virtual Advanced Threat Defense interface. For information about advanced configurations and how to use the software, see *McAfee Advanced Threat Defense 3.8.2 Product Guide*.

Contents

Configure the McAfee Virtual Advanced Threat Defense network information

Manage the McAfee Virtual Advanced Threat Defense from ESXI client/server.

Task

1. From the EXSI client, 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 the following class C network IP addresses:

- 192.168.55.0/24
- 192.168.122.0/24

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 Internet Explorer security settings

When you try to access the web interface, you might see the *ActiveX control unsafe* pop-up dialog box.

Task

1 On your computer, search for **Edit Group Policy**.

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

3 On the right window, double-click **Turn off the Security Settings Check feature**, then select **Enabled**.

4 Click **Apply**, then click **OK**.

Change your browser settings

To activate VM images and access manually submitted files, you must enable user-interactive mode (XMode). XMode works with any browser that supports HTML5 Canvas. You do not need to install Java to use XMode.

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 the Firefox settings to use the HTML5 feature.

Task

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**.

Log on to the McAfee Virtual Advanced Threat Defense interface

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

Task

1 From an Internet browser, access the McAfee Virtual Advanced Threat Defense URL.
https://<McAfee Virtual Advanced Threat Defense host name or IP address>

2 Log on to the Advanced Threat Defense interface using the default credentials.
- **Login ID** — `admin`
- **Password** — `admin`

3 Change the default password.