Microsoft Antimalware for Azure Cloud Services and Virtual Machines

Microsoft

Abstract

This paper provides an architectural overview of Microsoft Antimalware for Azure, including supported scenarios and configurations for enabling, configuring, and deploying protection for Azure Cloud Services and Virtual Machines. We will cover basic configuration, management, and monitoring functionality accessible through Microsoft Azure service management API's, PowerShell scripts, the Azure Management Portal and Visual Studio.

NOTE: Certain recommendations contained herein may result in increased data, network, or compute resource usage resulting in additional license or subscription costs.

Published October 2014

Acknowledgements

Contributors:

- Microsoft Azure Security and Compliance Engineering
- Microsoft Malware Protection Engineering
- Microsoft Azure Engineering Systems

This document is provided "as-is." Information and views expressed in this document, including URL and other Internet Web site references, may change without notice. You bear the risk of using it. Some examples are for illustration only and are fictitious. No real association is intended or inferred.

This document does not provide you with any legal rights to any intellectual property in any Microsoft product. You may copy and use this document for your internal, reference purposes.

Table of Contents

1 Overview

The modern threat landscape for cloud environments is extremely dynamic, increasing the pressure on business IT cloud subscribers to maintain effective protection in order to meet compliance and security requirements. Microsoft Antimalware for Azure Cloud Services and Virtual Machines is a real-time protection capability that helps identify and remove viruses, spyware, and other malicious software, with configurable alerts when known malicious or unwanted software attempts to install itself or run on your Azure systems.

The solution is built on the same antimalware platform as Microsoft Security Essentials [MSE], Microsoft Forefront Endpoint Protection, Microsoft System Center Endpoint Protection, Windows Intune, and Windows Defender for Windows 8.0 and higher. Microsoft Antimalware for Azure is a single-agent solution for applications and tenant environments, designed to run in the background without human intervention. You can deploy protection based on the needs of your application workloads, with either basic secure-by-default or advanced custom configuration, including antimalware monitoring.

When you deploy and enable Microsoft Antimalware for Azure for your applications, the following core features are available:

Real-time protection - monitors activity in Cloud Services and on Virtual Machines to detect and block malware execution.

Scheduled scanning - periodically performs targeted scanning to detect malware, including actively running programs.

Malware remediation - automatically takes action on detected malware, such as deleting or quarantining malicious files and cleaning up malicious registry entries.

Signature updates - automatically installs the latest protection signatures (virus definitions) to ensure protection is up-to-date on a pre-determined frequency.

Antimalware Engine updates – automatically updates the Microsoft Antimalware engine.

Antimalware Platform updates – automatically updates the Microsoft Antimalware platform.

Active protection - reports telemetry metadata about detected threats and suspicious resources to Microsoft Azure to ensure rapid response to the evolving threat landscape, as well as enabling real-time synchronous signature delivery through the Microsoft Active Protection System (MAPS).

Samples reporting - provides and reports samples to the Microsoft Antimalware service to help refine the service and enable troubleshooting.

Exclusions – allows application and service administrators to configure certain files, processes, and drives to exclude them from protection and scanning for performance and/or other reasons.

Antimalware event collection - records the antimalware service health, suspicious activities, and remediation actions taken in the operating system event log and collects them into the customer’s Azure Storage account.

2 Architecture

The Microsoft Antimalware for Azure Cloud Services and Virtual Machines solution includes the Microsoft Antimalware Client and Service, Antimalware Service Management Extension, Antimalware PowerShell cmdlets and Azure Diagnostics Extension. The Microsoft Antimalware solution is supported on Windows Server 2008 R2, Windows Server 2012, and Windows Server 2012 R2 operating system families. It is not supported on the Windows Server 2008 operating system. At this time, Windows Server Technical Preview is not supported and we intend to support it in the future.

The Microsoft Antimalware Client and Service is installed by default in a disabled state in all supported Azure guest operating system families in the Cloud Services platform.

The Microsoft Antimalware Client and Service is not installed by default in the Virtual Machines platform and is available as an optional feature through the Azure Management Portal and Visual Studio Virtual Machine configuration under Security Extensions.

2.1 Microsoft Antimalware Workflow

The Azure service administrator can enable Antimalware for Azure with a default or custom configuration for your Virtual Machines and Cloud Services using the following options:

- Virtual Machines – In the Azure Management Portal, under Security Extensions
- Virtual Machines – Using the Visual Studio virtual machines configuration in Server Explorer
- Virtual Machines and Cloud Services – Using the Antimalware service management APIs (SMAPI)
- Virtual Machines and Cloud Services – Using Antimalware PowerShell cmdlets

The Azure Management Portal or PowerShell cmdlets push the Antimalware extension package file to the Azure system at a pre-determined fixed location. The Azure Guest Agent (or the Fabric Agent) launches the Antimalware Extension, applying the Antimalware configuration settings supplied as input. This step enables the Antimalware service with either default or custom configuration settings. If no custom configuration is provided, then the antimalware service is enabled with the default configuration settings. Refer to the Antimalware configuration section later in this document for more details.

Once running, the Microsoft Antimalware client downloads the latest protection engine and signature definitions from the Internet and loads them on the Azure system. The Microsoft Antimalware service writes service-related events to the system OS events log under the “Microsoft Antimalware” event source. Events include the Antimalware client health state, protection and remediation status, new and old configuration settings, engine updates and signature definitions, and others.

You can enable Antimalware monitoring for your Cloud Service or Virtual Machine to have the Antimalware event log events written as they are produced to your Azure storage account. The Antimalware Service uses the Azure Diagnostics extension to collect Antimalware events from the Azure system into tables in the customer’s Azure Storage account.

The deployment workflow including configuration steps and options supported for the above scenarios are documented in Antimalware deployment scenarios section of this document.

Figure 1 shows the workflow involved in enabling the antimalware solution for Azure Cloud Services (Web Role and Worker Role) and Virtual Machines.

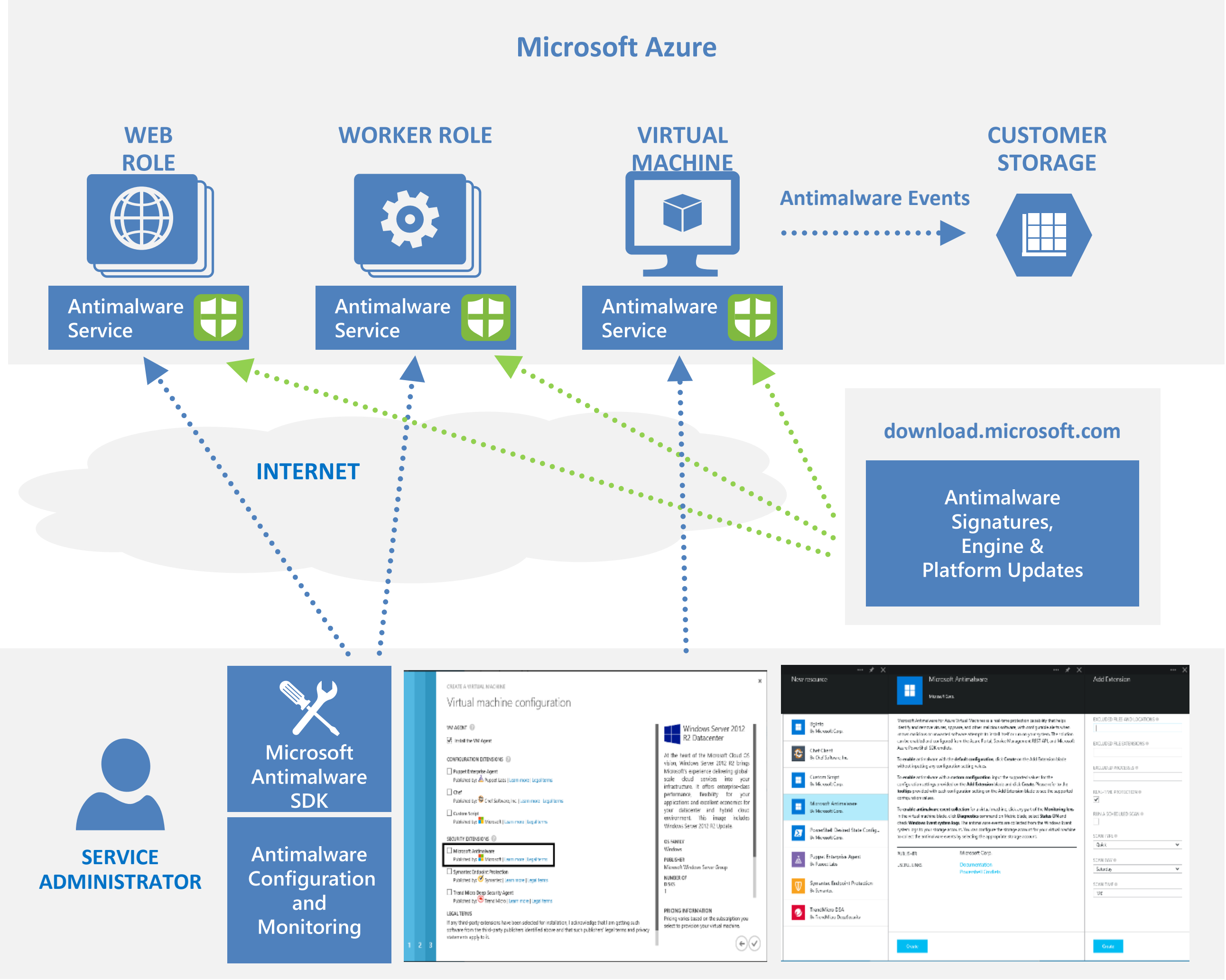


Figure 1: Microsoft Antimalware in Azure workflow - enable, configure, and monitor.

2.2 Default and Custom Antimalware Configuration

The default configuration settings are applied to enable Antimalware for Azure Cloud Services or Virtual Machines when you do not provide custom configuration settings. The default configuration settings have been pre-optimized for running in the Azure environment. Optionally, you can customize these default configuration settings as required for your Azure application or service deployment and apply them for other deployment scenarios.

The following table summarizes the configuration settings available for the Antimalware service. The default configuration settings are marked under the column labelled "Default" below.

Setting	Options	Default	Description
Enable Antimalware	true (lower case sensitive)	None	true - Enables the Antimalware service false – not supported **Note** – This is a required configuration setting to enable the Antimalware service
Exclusions Extensions	extension1, extension2, … …	None	List of file extensions to exclude from scanning. Example: gif, log, txt excludes files with the .gif, .log, or .txt extension from being scanned. Each excluded file extension should be added as a separate row element value in your antimalware XML configuration or semicolon separated in antimalware JSON configuration
Exclusions Paths	path1, path2 … …	None	List of paths to files or folders to exclude from scanning. Example: e:\approot\worker.dll, e:\approot\temp excludes the file worker.dll in the e:\approot folder and anything under the folder e:\approot\temp from being scanned. **Note**: For antimalware JSON configuration for virtual machines, use two backslashes (\\) instead of one to escape properly. For example: e:\\approot\\worker.dll Each excluded path should be added as a separate row element value in your antimalware XML configuration or semicolon separated in antimalware JSON configuration
Exclusions Processes	process1, process2, … …	None	List of process exclusions. Any file opened by an excluded process will not be scanned (the process itself will still be scanned – to exclude the process itself, use the ExcludedPaths option). Example: C:\Program Files\MyApp.exe excludes any files opened by MyApp.exe from being scanned.

			Each excluded process should be added as a separate row element value in your antimalware XML configuration or semicolon separated in antimalware JSON configuration
RealtimeProtectionEnabled	true false (lower case sensitive)	true	true – Enables real-time protection false – Disables real-time protection Default = true when AntimalwareEnabled = true
ScheduledScanSettings isEnabled	true false (lower case sensitive)	false	Enables or disables a periodic scan for active malware on the system Default = false

ScheduledScanSettings Day	0 – 8	7	0 – scan daily, 1 – Sunday, 2 – Monday, 3- Tuesday…, 7 – Saturday, 8 – disabled
			Default = 7 if only ScheduledScanSettings
			isEnabled = true

ScheduledScanSettings Time	0 – 1440	120	Hour at which to begin the scheduled scan. Measured in 60 minute increments from midnight 60 mins = 1:00 AM 120 mins = 2:00 AM … 1380 mins = 11:00 PM Default = 120 mins if ScheduledScanSettings isEnabled = true
ScheduledScanSettings Scan Type	Quick/Full	Quick	Default = Quick if ScheduledScanSettings isEnabled = true
Monitoring	ON OFF	OFF	ON - Enable Antimalware event collection to user subscription storage using Azure Diagnostics extension OFF – Disable Antimalware event collection to user subscription storage by removing antimalware monitoring configuration in Azure Diagnostics extension if it was previously turned ON
StorageAccountName	Storage Account Name	None	Storage account name for your Azure store table to collect antimalware events in storage **Note -** Storage account name is required if monitoring is specified as ON

3 Antimalware Deployment Scenarios

The scenarios to enable and configure antimalware, including monitoring for Azure Cloud Services and Virtual Machines, are discussed in this section.

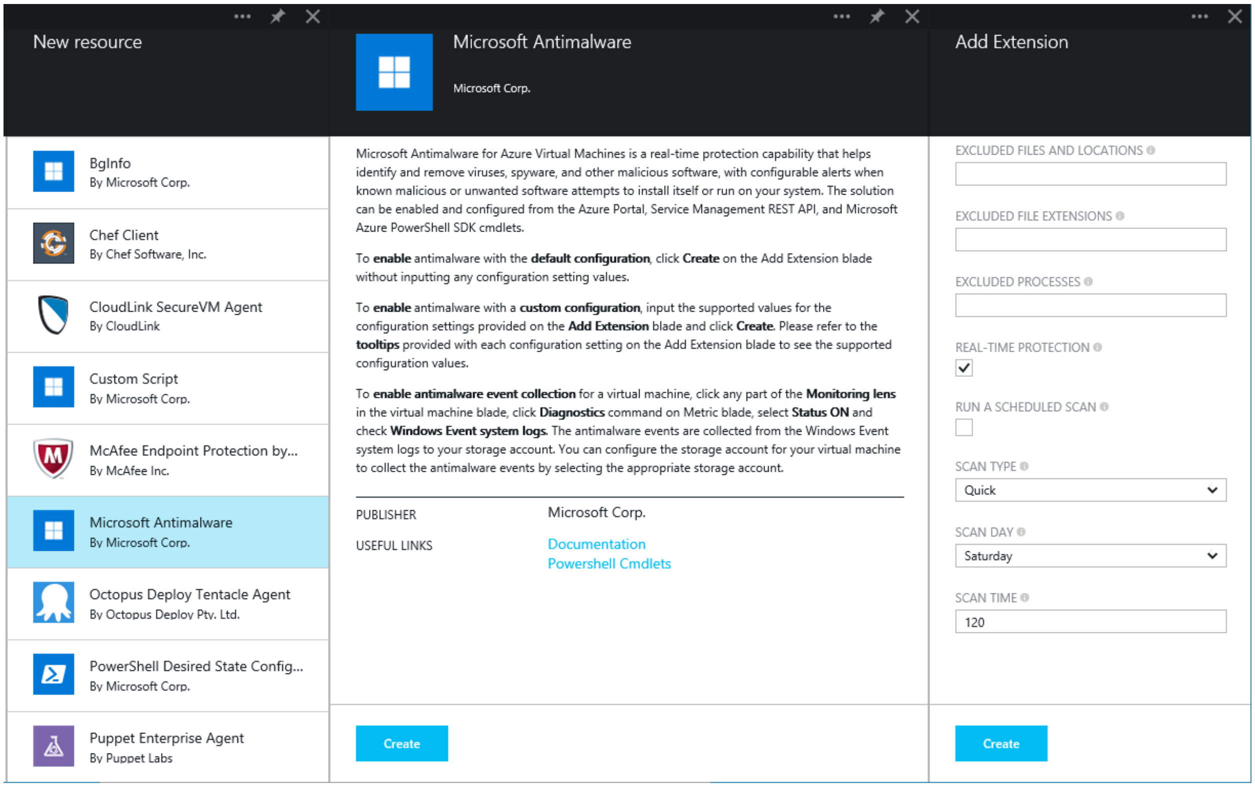
3.1 Virtual Machines - Enable and Configure Antimalware

3.1.1 Deployment using Azure Preview Portal

To enable and configure Microsoft Antimalware for Azure Virtual Machines using the Azure Preview Portal, follow the steps below:

1) Log onto Azure preview portal at https://portal.azure.com/
2) Create virtual machine using virtual machine creation menu or browse to existing virtual machine
3) Inside the virtual machine configuration blade, click the **Extensions** part of the **Configure** lens

To enable the Antimalware service, click **Add** on the Extensions blade, select **Microsoft Antimalware** on the New resource blade, click **Create** on the Microsoft Antimalware blade. Click **Create** without inputting any configuration values to enable Antimalware with the default settings, or enter the Antimalware configuration settings for the Virtual Machine configured as shown in Figure 2 below. Please refer to the **tooltips** provided with each configuration setting on the Add Extension blade to see the supported configuration values.



New resource

BgInfo
By Microsoft Corp.

Chef Client
By Chef Software, Inc.

CloudLink SecureVM Agent
By CloudLink

Custom Script
By Microsoft Corp.

McAfee Endpoint Protection by...
By McAfee Inc.

Microsoft Antimalware
By Microsoft Corp.

Octopus Deploy Tentacle Agent
By Octopus Deploy Pty. Ltd.

PowerShell Desired State Config...
By Microsoft Corp.

Puppet Enterprise Agent
By Puppet Labs

Microsoft Antimalware
Microsoft Corp.

Microsoft Antimalware for Azure Virtual Machines is a real-time protection capability that helps identify and remove viruses, spyware, and other malicious software, with configurable alerts when known malicious or unwanted software attempts to install itself or run on your system. The solution can be enabled and configured from the Azure Portal, Service Management REST API, and Microsoft Azure PowerShell SDK cmdlets.

To **enable** antimalware with the **default configuration**, click **Create** on the Add Extension blade without inputting any configuration setting values.

To **enable** antimalware with a **custom configuration**, input the supported values for the configuration settings provided on the **Add Extension** blade and click **Create**. Please refer to the **tooltips** provided with each configuration setting on the Add Extension blade to see the supported configuration values.

To **enable antimalware event collection** for a virtual machine, click any part of the **Monitoring lens** in the virtual machine blade, click **Diagnostics** command on Metric blade, select **Status ON** and check **Windows Event system logs**. The antimalware events are collected from the Windows Event system logs to your storage account. You can configure the storage account for your virtual machine to collect the antimalware events by selecting the appropriate storage account.

PUBLISHER Microsoft Corp.

USEFUL LINKS Documentation
Powershell Cmdlets

Create

Add Extension

EXCLUDED FILES AND LOCATIONS

EXCLUDED FILE EXTENSIONS

EXCLUDED PROCESSES

REAL-TIME PROTECTION
☑

RUN A SCHEDULED SCAN
☐

SCAN TYPE
Quick

SCAN DAY
Saturday

SCAN TIME
120

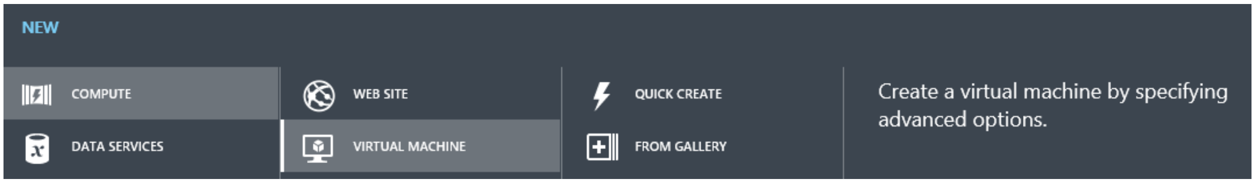
Create

Figure 2: Virtual Machine configuration settings for the Microsoft sAntimalware service.

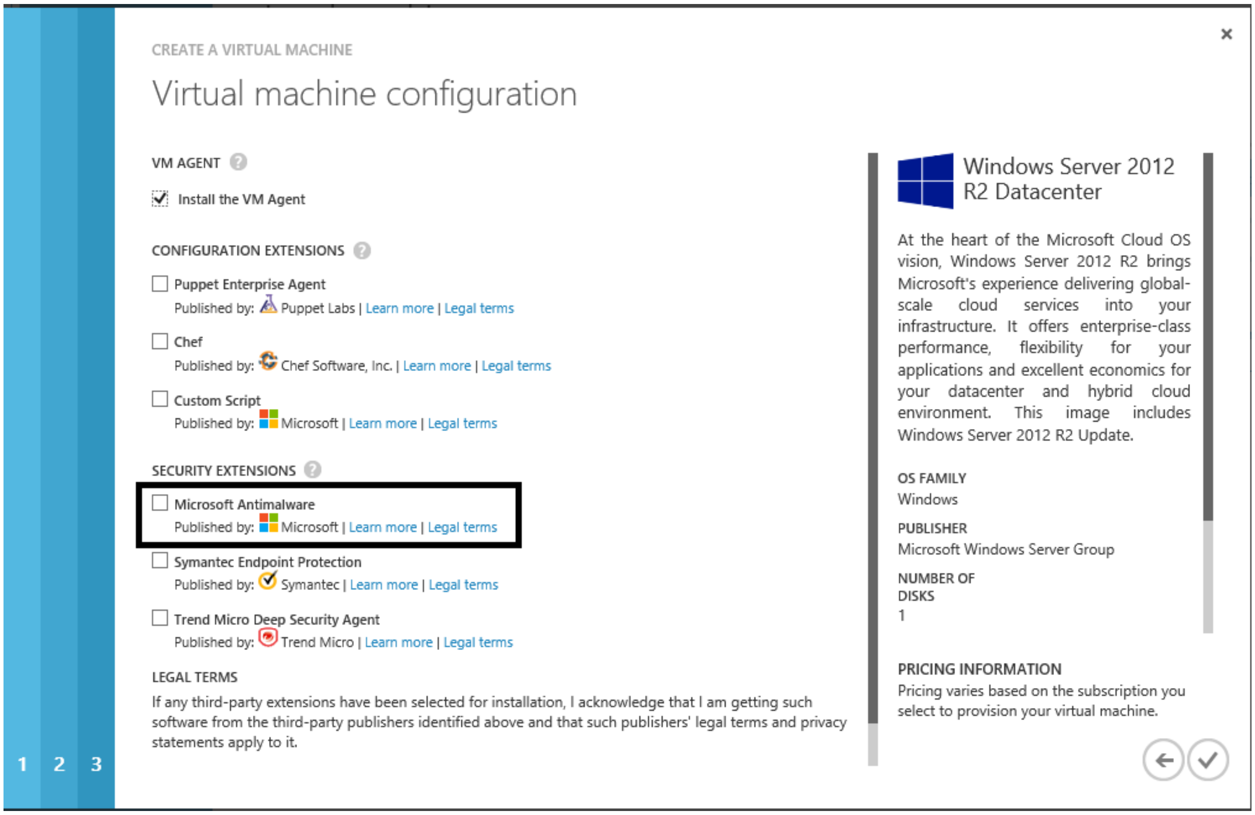
3.1.2 Deployment Using the Azure Management Portal

To enable and configure Microsoft Antimalware for Azure Virtual Machines using the Azure Management Portal while provisioning a Virtual Machine, follow the steps below:

1) Log onto the Azure Management Portal at https://manage.windowsazure.com
2) To create a new virtual machine, click **New**, **Compute**, **Virtual Machine**, **From Gallery** (do not use Quick Create) as shown below:



3) Select the **Microsoft Windows Server** image on the **Choose an Image** page.
4) Click the right arrow and input the Virtual Machine configuration.
5) Check the **Microsoft Antimalware** checkbox under **Security Extensions** on the Virtual Machine configuration page.
6) Click the Submit button to enable and configure Microsoft Antimalware for Azure Virtual Machines with the default configuration settings.



CREATE A VIRTUAL MACHINE

Virtual machine configuration

VM AGENT

☑ Install the VM Agent

CONFIGURATION EXTENSIONS

□ Puppet Enterprise Agent
Published by: Puppet Labs | Learn more | Legal terms

□ Chef
Published by: Chef Software, Inc. | Learn more | Legal terms

□ Custom Script
Published by: Microsoft | Learn more | Legal terms

SECURITY EXTENSIONS

□ Microsoft Antimalware
Published by: Microsoft | Learn more | Legal terms

□ Symantec Endpoint Protection
Published by: Symantec | Learn more | Legal terms

□ Trend Micro Deep Security Agent
Published by: Trend Micro | Learn more | Legal terms

LEGAL TERMS

If any third-party extensions have been selected for installation, I acknowledge that I am getting such software from the third-party publishers identified above and that such publishers' legal terms and privacy statements apply to it.

Windows Server 2012 R2 Datacenter

At the heart of the Microsoft Cloud OS vision, Windows Server 2012 R2 brings Microsoft's experience delivering global-scale cloud services into your infrastructure. It offers enterprise-class performance, flexibility for your applications and excellent economics for your datacenter and hybrid cloud environment. This image includes Windows Server 2012 R2 Update.

OS FAMILY
Windows

PUBLISHER
Microsoft Windows Server Group

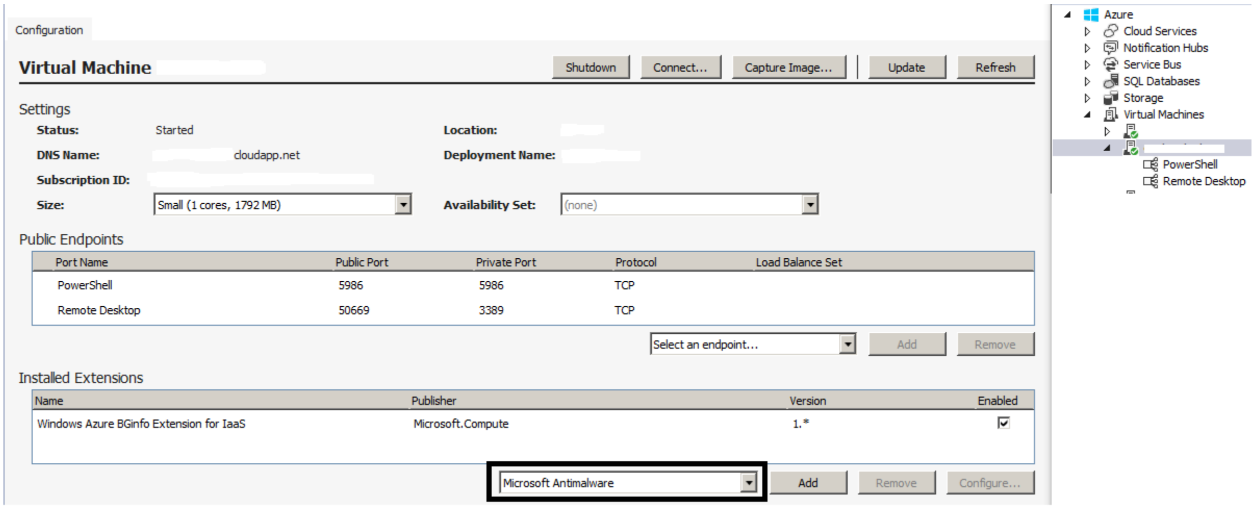
NUMBER OF DISKS
1

PRICING INFORMATION
Pricing varies based on the subscription you select to provision your virtual machine.

3.1.3 Deployment Using the Visual Studio Virtual Machine Configuration

To enable and configure the Microsoft Antimalware service using Visual Studio:

1) Connect to Microsoft Azure in Visual Studio.
2) Choose your Virtual Machine in the **Virtual Machines** node in **Server Explorer**



Settings

Status: Started
Location:
DNS Name: cloudapp.net
Deployment Name:
Subscription ID:
Size: Small (1 cores, 1792 MB)
Availability Set: (none)

Public Endpoints

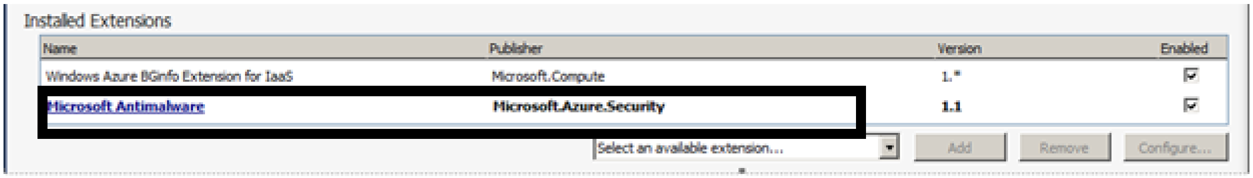
Port Name	Public Port	Private Port	Protocol	Load Balance Set
PowerShell	5986	5986	TCP	
Remote Desktop	50669	3389	TCP	

Installed Extensions

Name	Publisher	Version	Enabled
Windows Azure BGinfo Extension for IaaS	Microsoft.Compute	1.*	☑

Microsoft Antimalware

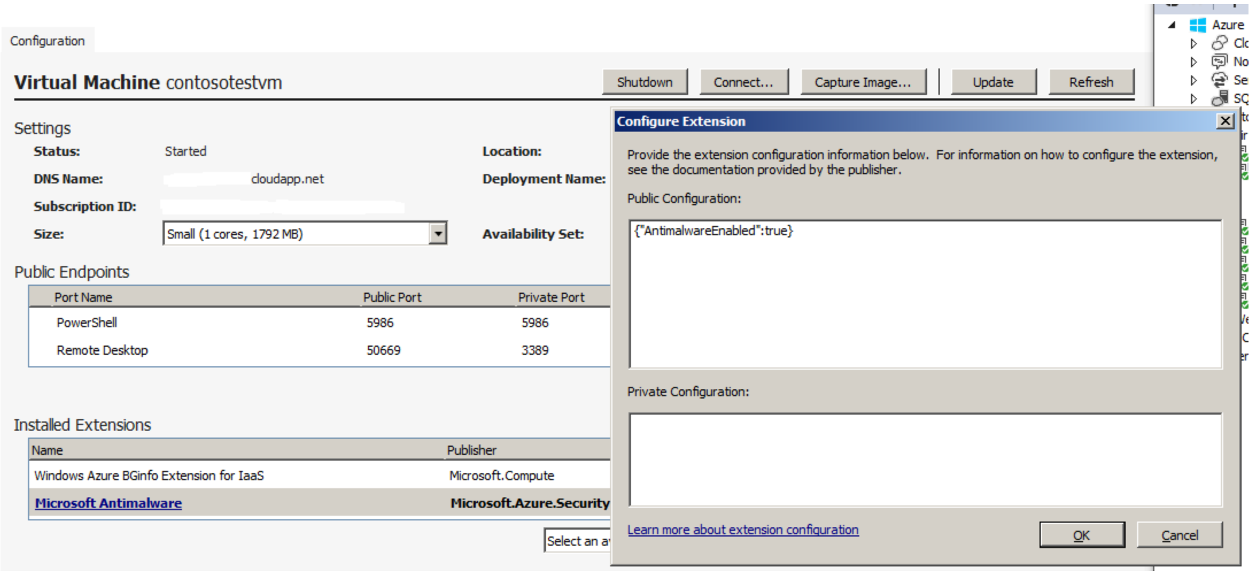
3) Right click **configure** to view the Virtual Machine configuration page
4) Select **Microsoft Antimalware** extension from the dropdown list under **Installed Extensions** and click **Add** to configure with default antimalware configuration.



Installed Extensions

Name	Publisher	Version	Enabled
Windows Azure BGinfo Extension for IaaS	Microsoft.Compute	1.*	☑
Microsoft Antimalware	Microsoft.Azure.Security	1.1	☑

5) To customize the default Antimalware configuration, select (highlight) the Antimalware extension in the installed extensions list and click **Configure**.
6) Replace the default Antimalware configuration with your custom configuration in supported JSON format in the **public configuration** textbox and click OK.
7) Click the **Update** button to push the configuration updates to your Virtual Machine.



Virtual Machine contosotestvm

Settings

Status:	Started
DNS Name:	[redacted] cloudapp.net
Subscription ID:	[redacted]
Size:	Small (1 cores, 1792 MB)
Location:	
Deployment Name:	
Availability Set:	

Public Endpoints

Port Name	Public Port	Private Port
PowerShell	5986	5986
Remote Desktop	50669	3389

Installed Extensions

Name	Publisher
Windows Azure BGinfo Extension for IaaS	Microsoft.Compute
Microsoft Antimalware	**Microsoft.Azure.Security**

Configure Extension

Provide the extension configuration information below. For information on how to configure the extension, see the documentation provided by the publisher.

Public Configuration:

```
{"AntimalwareEnabled":true}
```

Private Configuration:

Learn more about extension configuration

Note: The Visual Studio Virtual Machines configuration for Antimalware supports only JSON format configuration. The Antimalware JSON configuration settings template is included in the Appendix section of this whitepaper, showing the supported Antimalware configuration settings.

3.1.4 Deployment Using PowerShell cmdlets

An Azure application or service can enable and configure Microsoft Antimalware for Azure Virtual Machines using PowerShell cmdlets.

To enable and configure Microsoft antimalware using antimalware PowerShell cmdlets:

1. Set up your PowerShell environment - Refer to the documentation at https://github.com/Azure/azure-sdk-tools#get-started
2. Use the Set-AzureVMMicrosoftAntimalwareExtension Antimalware cmdlet to enable and configure Microsoft Antimalware for your Virtual Machine as documented at http://msdn.microsoft.com/en-us/library/azure/dn771718.aspx

Note: The Azure Virtual Machines configuration for Antimalware supports only JSON format configuration. The Antimalware JSON configuration settings template is included in the Appendix section of this whitepaper, showing the supported Antimalware configuration settings.

3.2 Cloud Services – Enable and Configure Antimalware Using PowerShell cmdlets

An Azure application or service can enable and configure Microsoft Antimalware for Azure Cloud Services using PowerShell cmdlets. Note that Microsoft Antimalware is installed in a disabled state in the Cloud Services platform and requires an action by an Azure application to enable it.

To enable and configure Microsoft Antimalware using PowerShell cmdlets:

1. Set up your PowerShell environment - Refer to the documentation at https://github.com/Azure/azure-sdk-tools#get-started
2. Use the Set-AzureServiceAntimalwareExtension Antimalware cmdlet to enable and configure Microsoft Antimalware for your Cloud Service as documented at http://msdn.microsoft.com/en-us/library/azure/dn771718.aspx

The Antimalware XML configuration settings template is included in the Appendix section of this whitepaper, showing the supported Antimalware configuration settings.

3.3 Cloud Services and Virtual Machines - Configuration Using PowerShell cmdlets

An Azure application or service can retrieve the Microsoft Antimalware configuration for Cloud Services and Virtual Machines using PowerShell cmdlets.

To retrieve the Microsoft Antimalware configuration using PowerShell cmdlets:

1. Set up your PowerShell environment - Refer to the documentation at https://github.com/Azure/azure-sdk-tools#get-started
2. **For Virtual Machines**: Use the Get-AzureVMMicrosoftAntimalwareExtension Antimalware cmdlet to get the antimalware configuration as documented at http://msdn.microsoft.com/en-us/library/azure/dn771719.aspx
3. **For Cloud Services**: Use the Get-AzureServiceAntimalwareConfig Antimalware cmdlet to get the Antimalware configuration as documented at http://msdn.microsoft.com/en-us/library/azure/dn771722.aspx

3.4 Remove Antimalware Configuration Using PowerShell cmdlets

An Azure application or service can remove the Antimalware configuration and any associated Antimalware monitoring configuration from the relevant Azure Antimalware and diagnostics service extensions associated with the Cloud Service or Virtual Mmachine.

To remove Microsoft Antimalware using PowerShell cmdlets:

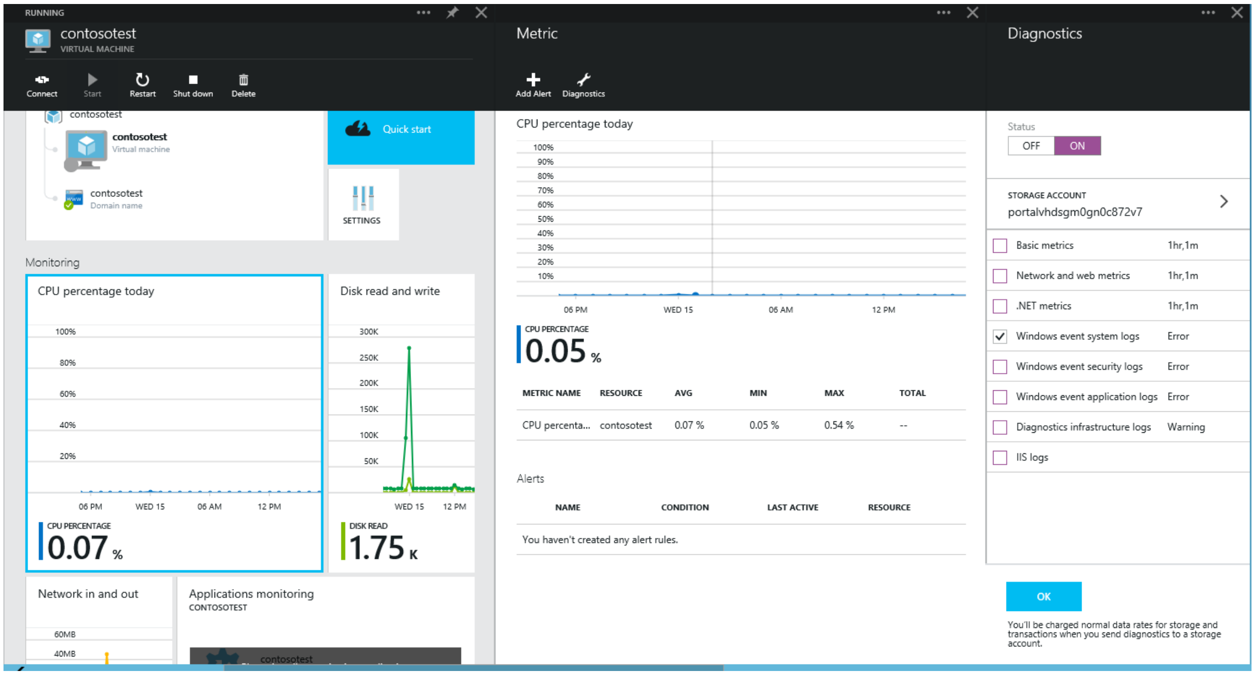
1. Set up your PowerShell environment - Refer to the documentation at https://github.com/Azure/azure-sdk-tools#get-started
2. **For Virtual Machines**: Use the Remove-AzureVMMicrosoftAntimalwareExtension Antimalware cmdlet as documented at http://msdn.microsoft.com/en-us/library/azure/dn771720.aspx
3. **For Cloud Services:** Use the Remove-AzureServiceAntimalwareExtension Antimalware cmdlet as documented at http://msdn.microsoft.com/en-us/library/azure/dn771717.aspxVirtual Machines - Enable and Configure Antimalware Monitoring Using the Azure Preview Portal

To **enable** antimalware event collection for a virtual machine using the Azure Preview Portal:

1) Click any part of the Monitoring lens in the Virtual Machine blade
2) Click the Diagnostics command on Metric blade

3) Select **Status** ON and check the option for Windows event system logs. You can choose to uncheck all other options in the list, or leave them enabled per your application service needs.
4) The Antimalware event categories "Error", "Warning", "Informational", etc., are captured in your Azure Storage account.

Antimalware events are collected from the Windows event system logs to your Azure Storage account. You can configure the Storage Account for your Virtual Machine to collect Antimalware events by selecting the appropriate storage account.



METRIC NAME	RESOURCE	AVG	MIN	MAX	TOTAL
CPU percenta...	contosotest	0.07 %	0.05 %	0.54 %	--

NAME	CONDITION	LAST ACTIVE	RESOURCE

You haven't created any alert rules.

Diagnostics

Status
OFF [✓ ON]

STORAGE ACCOUNT
portalvhdsgm0gn0c872v7

□	Basic metrics	1hr,1m
□	Network and web metrics	1hr,1m
□	.NET metrics	1hr,1m
☑	Windows event system logs	Error
□	Windows event security logs	Error
□	Windows event application logs	Error
□	Diagnostics infrastructure logs	Warning
□	IIS logs	

OK

You'll be charged normal data rates for storage and transactions when you send diagnostics to a storage account.

3.5 Enable and Configure Antimalware Monitoring Using PowerShell cmdlets

You can enable collection of Microsoft Antimalware events for your Cloud Service or Virtual Machine using Azure Diagnostics through Antimalware PowerShell cmdlets. The Azure Diagnostics extension can be configured to capture events from the System event log source "Microsoft Antimalware" to your Azure Storage account. The Antimalware event categories "Error", "Warning", "Informational", etc., are captured in your Azure Storage account.

To enable Antimalware event collection to your Azure Storage account using PowerShell cmdlets:

1. Set up your PowerShell environment - Refer to https://github.com/Azure/azure-sdk-tools#get-started
2. **For Virtual Machines** - Use the Set-AzureVMMicrosoftAntimalwareExtension Antimalware cmdlet with Monitoring ON option as documented at http://msdn.microsoft.com/en-us/library/azure/dn771716.aspx

3. **For Cloud Services** - Use the Set-AzureServiceAntimalwareExtension Antimalware cmdlet with Monitoring ON option as documented at http://msdn.microsoft.com/en-us/library/azure/dn771718.aspx

You can view the Antimalware raw events by looking at the WADWindowsEventLogsTable table in your Azure Storage account that you configured to enable Antimalware monitoring. This can be useful to validate that Antimalware event collection is working, including getting insight into the Antimalware service’s health. For more details, including sample code on how to extract Antimalware events from your storage account, refer to Appendix B.

4 Appendix A: Microsoft Antimalware Configuration

4.1 *XML Template*

NOTE – The following Antimalware configuration template settings must be adjusted for your **Azure Cloud Service application** per your application requirements. Only supported Antimalware configuration settings are allowed. The XML configuration is only supported for Azure Cloud Services.

The XML antimalware configuration must include, at a minimum, the following content to enable the Microsoft Antimalware extension with default configuration:

```
<AntimalwareConfig>
    <AntimalwareEnabled>true</AntimalwareEnabled>
</AntimalwareConfig>
```

You can enable and configure Microsoft Antimalware with a custom configuration using the below sample XML configuration template, which shows additional configuration settings supported beyond the default configuration.

```
<AntimalwareConfig>
    <AntimalwareEnabled>true</AntimalwareEnabled>
    <RealtimeProtectionEnabled>true</RealtimeProtectionEnabled>
    <ScheduledScanSettings isEnabled="true" day="7" time="120" scanType="Quick"/>
    <Exclusions>
        <Extensions>
              <Extension>.ext1</Extension>
              <Extension>.ext2</Extension>
        </Extensions>
        <Paths>
              <Path>c:\excluded-path-1</Path>
              <Path>c:\excluded-path-2</Path>
        </Paths>
        <Processes>
              <Process>excludedproc1.exe</Process>
              <Process>excludedproc2.exe</Process>
        </Processes>
    </Exclusions>
    <Monitoring>ON</Monitoring>
    <StorageAccountName>contosostorage</StorageAccountName>
</AntimalwareConfig>
```

4.2 *JSON Template*

NOTE – The following Antimalware configuration template settings must be adjusted for your **Azure Virtual Machine application** per your application requirements. Only supported Antimalware configuration settings are allowed. The JSON configuration is only supported for Azure Virtual Machines.

The JSON Antimalware configuration must include, at a minimum, the following content to enable the Microsoft Antimalware extension with the default configuration:

```
{

        "AntimalwareEnabled": true

}
```

You can enable and configure Microsoft Antimalware with a custom configuration using the sample JSON configuration template below, which shows additional configuration settings supported beyond the default configuration. It is recommended to check your JSON configuration using a javascript validation tool prior to deploying it.

```
{
        "AntimalwareEnabled": true,
        "RealtimeProtectionEnabled": true,
        "ScheduledScanSettings": {
                "isEnabled": true,
                "day": 7,
                "time": 120,
                "scanType": "Quick"
         },
         "Exclusions": {
                "Extensions": ".ext1;.ext2",
                "Paths": "c:\\excluded-path-1;c:\\excluded-path-2",
                "Processes": "excludedproc1.exe;excludedproc2.exe"
      }
   }
```

Note:

For JSON configuration for Virtual Machines:

- For exclusion paths, use two backslashes (\\) instead of one backslash to escape properly. For Example: `c:\\excluded-path-1`
- Monitoring and StorageContext are provided as Antimalware cmdlet parameters to enable Antimalware monitoring, and are not specified in the JSON configuration.

5 Appendix B: Sample Code to Extract Antimalware Events from Azure Storage

The example below shows one of several ways to extract Antimalware events from your Azure Storage account. To extract Antimalware events into a file:

```
#Enter the storage account name
$storage_account_name = ""
#Enter the full path of the output file
$csv_output_file = ""
$storage_context = New-AzureStorageContext -StorageAccountName $storage_account_name -
StorageAccountKey (Get-AzureStorageKey $storage_account_name).Primary
$keys = Get-AzureStorageKey -StorageAccountName $storage_account_name
$storage_account_key = $keys.Primary
$tableName = (Get-AzureStorageTable -Prefix "WADWindowsEventLogs" -Context
$storage_context).Name;
if ($tableName)
{
    $endpoint_suffix = "core.windows.net"
    $storage_credentials = (New-Object
Microsoft.WindowsAzure.Storage.Auth.StorageCredentials($storage_account_name,
$storage_account_key))
    $use_https = 1
    $stg = New-Object Microsoft.WindowsAzure.Storage.CloudStorageAccount(
        $storage_credentials,
        $endpoint_suffix,
        $use_https)
    $cloudTableClient = $stg.CreateCloudTableClient()
    $cloudTableData = $cloudTableClient.GetTableReference($tableName)
    $query = New-Object Microsoft.WindowsAzure.Storage.Table.TableQuery
    $response = $cloudTableData.ExecuteQuery($query)
    #extract out the relevant information
    $results = New-Object System.Collections.ArrayList
    foreach ($row in $response)
    {
        $obj = new-object psobject
        Add-Member -InputObject $obj -MemberType NoteProperty -Name "Timestamp" -Value
$row.Properties.TIMESTAMP.PropertyAsObject.ToOADate()
        Add-Member -InputObject $obj -MemberType NoteProperty -Name "EventId" -Value
$row.Properties.EventId.Int32Value
        Add-Member -InputObject $obj -MemberType NoteProperty -Name "Role" -Value
$row.Properties.Role.StringValue
        Add-Member -InputObject $obj -MemberType NoteProperty -Name "RoleInstance" -
Value $row.Properties.RoleInstance.StringValue
```

```
        Add-Member -InputObject $obj -MemberType NoteProperty -Name "Description" -
Value $row.Properties.Description.StringValue.replace("`n","").replace("`r","")
        $total = $results.Add($obj)
    }
    Write-Host $total 'rows exported to csv output file (' $csv_output_file ')'
    #export to csv
    $results | Export-Csv -path $csv_output_file -NoTypeInformation
}
else
{
    Write-Host 'no data found in storage account'
}
```

6 References and Further Reading

The following resources are available to provide more general information about Microsoft Azure and related Microsoft services, as well as specific items referenced in the main text:

- Microsoft Azure Home – general information and links about Microsoft Azure
  - http://www.microsoft.com/windowsazure/
- Microsoft Azure Documentation Center – developer guidance and information
  - http://msdn.microsoft.com/en-us/windowsazure/default.aspx
- Microsoft Azure Trust Center
  - http://azure.microsoft.com/en-us/support/trust-center/
- Microsoft Security Response Center [where Microsoft security vulnerabilities, including issues with Microsoft Azure, can be reported]
  - http://www.microsoft.com/security/msrc/default.aspx
  - Or via email to secure@microsoft.com.
- Microsoft Azure PowerShell SDK tools and SDK releases
  - https://github.com/Azure/azure-sdk-tools#get-started
  - https://github.com/Azure/azure-sdk-tools/releases
- Microsoft Antimalware PowerShell Cmdlets for Azure virtual machines and cloud services
  - http://msdn.microsoft.com/en-us/library/azure/dn771715.aspx
- Recommended File and Folder Exclusions
  - http://support.microsoft.com/kb/943556
  - http://support.microsoft.com/kb/2962341
- Microsoft Antimalware Event Information
  - http://technet.microsoft.com/en-us/library/hh144989.aspx
- Visual Studio virtual machine configuration
  - http://msdn.microsoft.com/en-us/library/azure/dn794167.aspx
  - http://msdn.microsoft.com/en-us/library/azure/dn569263.aspx
  - http://azure.microsoft.com/blog/2014/08/04/announcing-release-of-visual-studio-2013-pdate-3-and-azure-sdk-2-4/
- Managing Microsoft Antimalware for Azure Virtual Machines via SCCM

  For those customers licensed and using System Center Endpoint Protection on-premises to manage Microsoft Endpoint Protection, who also want to extend management to Microsoft Antimalware for Azure Virtual Machines, more information is available here:
  - http://blogs.technet.com/b/configmgrteam/archive/2013/10/23/configmgr-and-endpoint-protection-support-for-windows-azure-vms.aspx covers the overall support.

  For information on Endpoint Protection settings:
  - http://technet.microsoft.com/en-us/library/gg682067.aspx#BKMK_EndpointProtectionDeviceSettings