

How to set up VMware Unified Access Gateway with OPSWAT MetaAccess Client

About This Guide.....	2
Part 1: Enforce MetaAccess client installation	3
Part 2: Enforce device compliance	5

About This Guide

OPSWAT MetaAccess (formerly Metadefender Endpoint Management) is a cloud based next generation network access control solution that helps organizations enforce endpoint compliance and prevent contamination of cloud applications by blocking risky devices from accessing SaaS applications. More information on MetaAccess can be found at

<https://www.opswat.com/products/metaaccess>

MetaAccess can be leveraged by VMware Unified Access Gateway (UAG) 3.1 and newer to provide enhanced compliance checking capabilities for Horizon Client access to virtual desktops and RDS hosted applications. This guide specifically illustrates :

1. how to establish MetaAccess policy checks by setting up UAG Endpoint Compliance Check Provider Settings to enforce installation of the MetaAccess client on Horizon client devices and
2. how to check for device compliance before allowing access to virtual desktops or RDS hosted applications.

Part 2: Enforce device compliance

In this section, the steps will guide you in configuring UAG to enforce device compliance with MetaAccess policies before and during network access.

Before configuring UAG, configure your device policy in MetaAccess to indicate what you consider an issue or critical issue. UAG will deny access from any endpoint that has one or more critical issues.

The screenshot displays the OPSWAT MetaAccess interface. On the left is a dark blue navigation sidebar with the OPSWAT logo and menu items: Dashboard, Inventory, Access Control, Policies (highlighted), Event Log, and Settings. The main content area shows the 'Policy' section for 'Default'. Below this, there are tabs for 'Windows & macOS Devices', 'Linux Devices', and 'Android & iOS Devices'. The 'Posture Check' tab is active, showing a table of compliance rules. The table has columns for 'Consider an issue if', 'Critical', and device types: 'All', 'Desktops', 'Laptops', 'VMS', and 'Servers'. Under the 'Anti-Malware' section, several rules are listed with checkboxes and dropdown menus for configuration.

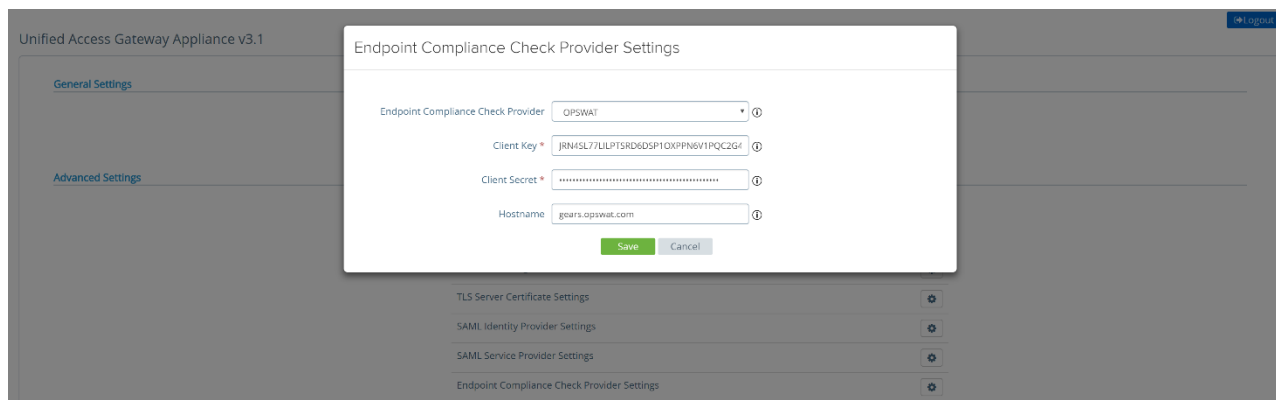
Consider an issue if	Critical	All	Desktops	Laptops	VMS	Servers
<input checked="" type="checkbox"/> No anti-malware application is installed <input checked="" type="checkbox"/> Real-time protection is disabled <input type="checkbox"/> Attempt to enable real-time protection in approved products <input checked="" type="checkbox"/> Signature definition is updated at least every 7 day(s) <input checked="" type="checkbox"/> Attempt to update definitions for approved anti-malware products <input checked="" type="checkbox"/> No successful full system scan in the last 7 day(s) <input checked="" type="checkbox"/> Any threats have been detected within the last 3 day(s)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Encryption	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Step 1:

Configure Endpoint Compliance Check Provider Settings in UAG. This can either be done through the UAG Admin GUI or through settings in your PowerShell .ini file for UAG.

From the UAG Admin console in *Advanced Settings*, go to *Endpoint Compliance Check Provider Settings*. Click *Add*. From the *Endpoint Compliance Check Provider* dropdown list, select *OPSWAT*.

Copy and paste the client_id and client_secret values that you obtained in step 1, leave the hostname set to the default of `gears.opswat.com` and click *Save*.



In General Settings select *Show* next to *Edge Service Settings*. Select *Horizon Settings* and then under *More*, go to *Endpoint Compliance Check Provider*.

Horizon Settings

Enable Horizon	<input checked="" type="checkbox"/> YES	i
Identifier *	<input type="text" value="VIEW"/>	i
Connection Server URL *	<input type="text"/>	i
Proxy Destination URL Thumb Prints	<input type="text"/>	i
Auth Methods	No auth methods configured	i
Health Check URL	<input type="text" value="/favicon.ico"/>	i
PCOIP Enabled	<input checked="" type="checkbox"/> YES	i
PCOIP External URL	<input type="text" value="192.168.0.129:4172"/>	i
Blast Enabled	<input checked="" type="checkbox"/> YES	i
Blast External URL	<input type="text" value="https://192.168.0.129:443"/>	i
BSG UDP Tunnel Server	<input checked="" type="checkbox"/> YES	i
Tunnel Enabled	<input checked="" type="checkbox"/> YES	i
Tunnel External URL	<input type="text" value="https://192.168.0.129:443"/>	i
Endpoint Compliance Check Provider	<input type="text" value="OPSWAT"/>	i
Proxy Pattern	<input type="text" value="(\/ \/view-client(.*) \/portal(.*) \/appblast(.*))"/>	i

In the dropdown list select *OPSWAT* and then click *Save*.

UAG is now configured to enforce endpoint compliance for VMware Horizon client access. For more information, or if you have any questions about the steps above, please log into the OPSWAT Portal at <https://portal.opswat.com> and submit a ticket to request assistance from our support team.