OPSWAT.

How to set up F5® BIG-IP® Access Policy Manager® (APM®) with OPSWAT MetaAccess®

Document last updated 2019-02-12

About This Guide:

MetaAccess prevents risky devices from accessing local networks and cloud applications such as Office 365, Salesforce and Dropbox. Using OPSWAT's industry-leading endpoint security and advanced threat prevention technologies, MetaAccess performs extensive security and compliance checks as well as remediation before allowing devices to access corporate data.

MetaAccess can be leveraged by F5 BIG-IP APM to provide enhanced compliance checking capabilities. Once you have deployed the MetaAccess to your devices and configured your compliance policy through the MetaAccess console, the MetaAccess will store the device's compliance status within the Windows Registry or Mac OS p-list. The F5 BIG-IP APM can access and use this information through a simple access policy, and can be used to determine if a device should be granted network access, or on a continuous basis to ensure that a device should retain network access based on the predefined security and compliance policies established by the organization.

Access Policy

An F5 BIG-IP APM appliance can be configured to utilize MetaAccess for advanced threat detection and compliance enforcement for remote users. These checks will ensure that endpoint devices connecting to the network are meeting all compliance requirements established by the organization.

The policies can be easily configured via the MetaAccess console, and will enable an administrator to ensure that the security and compliance requirements of an organization are met on a continuous basis.

Step 1:

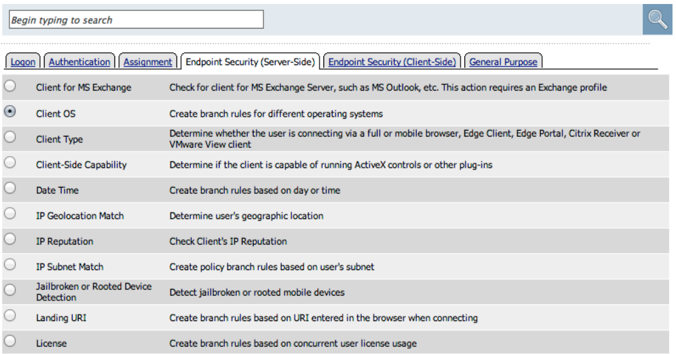
To create a new *Access Policy*, navigate to *Access Policy –> Access Profiles –> Access Profiles List* . Create a new policy, and under General Properties add the following:

- Name: "MetaAccess_Assessment"
- Parent Profile: access
- Profile Type: SSL-VPN

Go to your *Access Profile List* and select the Access Profile you just created - "MetaAccess_Assessment", select *Edit* under *Access Policy*. This will take you to the visual policy editor for your new *Access Policy*.

Step 2:

Click on *+,* next to the *Start*, then select the *Endpoint Security (Server-Side)* tab – then click on *Client OS*. This allows you to create a branch rule based on the type of operating system on the endpoint. This is useful as the path is different between the different Windows devices (32-bit versus 64-bit) and Mac.



○	Client for MS Exchange	Check for client for MS Exchange Server, such as MS Outlook, etc. This action requires an Exchange profile
●	Client OS	Create branch rules for different operating systems
○	Client Type	Determine whether the user is connecting via a full or mobile browser, Edge Client, Edge Portal, Citrix Receiver or VMware View client
○	Client-Side Capability	Determine if the client is capable of running ActiveX controls or other plug-ins
○	Date Time	Create branch rules based on day or time
○	IP Geolocation Match	Determine user's geographic location
○	IP Reputation	Check Client's IP Reputation
○	IP Subnet Match	Create policy branch rules based on user's subnet
○	Jailbroken or Rooted Device Detection	Detect jailbroken or rooted mobile devices
○	Landing URI	Create branch rules based on URI entered in the browser when connecting
○	License	Create branch rules based on concurrent user license usage

Select *Add Item*.

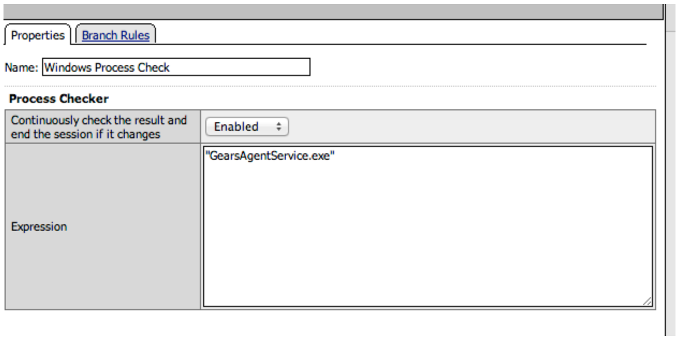
For simplicity you can remove the operating systems that you are not checking for at this time (i.e. Windows RT, Linux, IOS, and Android).

Step 3:

Before checking for the policy state of the device, confirm that the MetaAccess is running on the endpoint. This can be performed simply through a Process Check.

Click on *+,* next to *Windows* and then click on the *Endpoint Security (Client-Side)* tab. Once there, select *Windows Process*. This will open up a window to configure the Windows Process Checker properties.

- Name: "Windows Process Check"
- Registry Checker: Select *Enabled* next to "Continuously check the result and end the session if it changes" section, if you wish to provide an ongoing policy check on the endpoint state. If you wish to only have a check when the device logs in, then select *Disabled*.
- Expression:
  - If you are using the persistent, installed MetaAccess agent, use "GearsAgentService.exe"
  - If you are using the on demand, portable MetaAccess agent, use "opswat-gears-od.exe"



Name: Windows Process Check

Process Checker

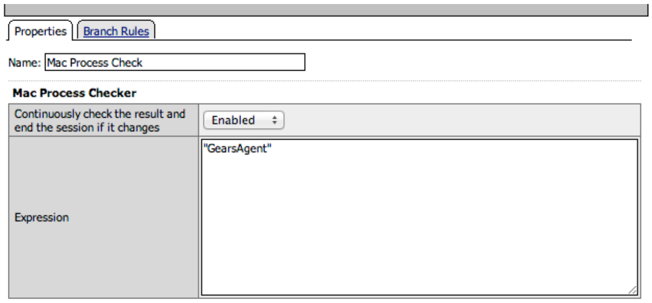
Continuously check the result and end the session if it changes	Enabled
Expression	"GearsAgentService.exe"

Select *Save*.

Step 4:

Next create a process check for Mac devices. Click on *+,* next to *MacOS* and then click on the *Endpoint Security (Client-Side)* tab. Once there, select *Mac Process*. This will open up a window to configure the Mac Process Checker Process properties.

- Name: "Mac Process Check"
- Registry Checker: Select *Enabled* next to "Continuously check the result and end the session if it changes" section, if you wish to provide an ongoing policy check on the endpoint state. If you wish to only have a check when the device logs in, then select *Disabled*.
- Expression:
  - If you are using the persistent, installed MetaAccess agent, use "GearsAgent"
  - If you are using the on demand, portable MetaAccess agent, use "opswat-gears-od"



Name: Mac Process Check

Mac Process Checker

Continuously check the result and end the session if it changes	Enabled
Expression	"GearsAgent"

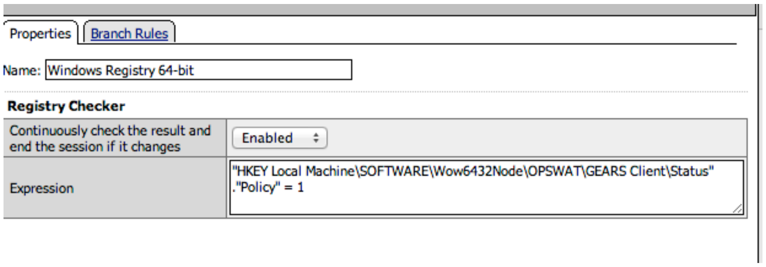
Select *Save*.

Step 5:

Create two Windows Registry checks, one for 32-bit and one for 64-bit. Make sure the logic of the flow handles the unique paths for each registry; the configuration steps below are set up to check the 64-bit registry setting first, and upon failure check the 32-bit registry setting.

Click on *+,* next to *Windows* and then click on the *Endpoint Security (Client-Side)* tab. Once there, select *Windows Registry*. This will open up a window to configure the Windows Registry properties.

- Name: "Windows Registry 64-bit"
- Registry Checker: Select*Enabled* next to "Continuously check the result and end the session if it changes" section, if you wish to provide an ongoing policy check on the endpoint state. If you wish to only have a check when the device logs in, then select *Disabled*.
- Expression:
  - If you are using the persistent, installed MetaAccess agent, use "HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\OPSWAT\Gears Client \Status" ."Policy" = 1
  - If you are using the on demand, portable MetaAccess agent, use "HKEY_CURRENT_USER\Software\OPSWAT\Gears OnDemand\Config" ."Policy" = 1



Name: Windows Registry 64-bit

Registry Checker

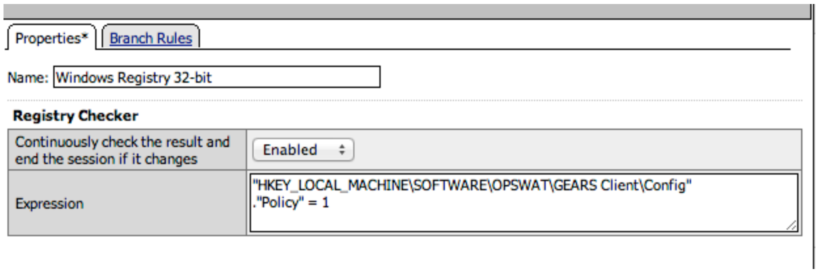
Continuously check the result and end the session if it changes	Enabled
Expression	"HKEY Local Machine\SOFTWARE\Wow6432Node\OPSWAT\GEARS Client\Status" ."Policy" = 1

Select *Save*.

Step 6:

Click on *+,* next to *Windows* and then click on the *Endpoint Security (Client-Side)* tab. Once there, select *Windows Registry*. This will open up a window to configure the Windows Registry properties.

- Name: "Windows Registry 32-bit"
- Registry Checker: Select *Enabled* next to "Continuously check the result and end the session if it changes" section, if you wish to provide an ongoing policy check on the endpoint state. If you wish to only have a check when the device logs in, then select *Disabled*.
- Expression:
  - If you are using the persistent, installed MetaAccess agent, use "HKEY_LOCAL_MACHINE\SOFTWARE\OPSWAT\Gears Client\Status" ."Policy" = 1
  - If you are using the on demand, portable MetaAccess agent, use "HKEY_CURRENT_USER\Software\OPSWAT\Gears OnDemand\Config" ."Policy" = 1



Name: Windows Registry 32-bit

Registry Checker

Continuously check the result and end the session if it changes	Enabled
Expression	"HKEY_LOCAL_MACHINE\SOFTWARE\OPSWAT\GEARS Client\Config" ."Policy" = 1

Select *Save*.

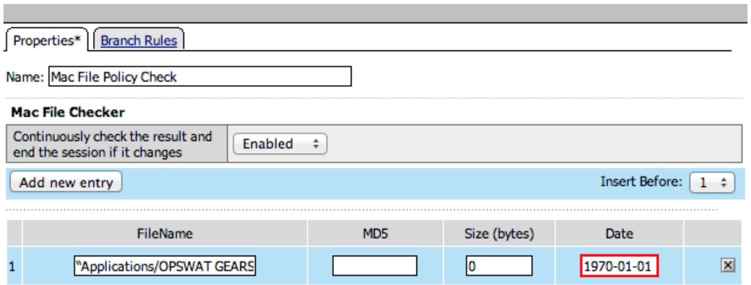
Step 7:

To configure the policy check for the Mac devices, the path is a bit different than the Windows devices. The configuration steps below combine the License Key and policy value into a single file value to allow for the same policy check on the Mac devices. This allows you to validate the policy state on the Mac, as well as confirm that the License Key matches the account administered by your organization.

Click on *+,* next to *MacOS* and then click on the *Endpoint Security (Client-Side)* tab. Once there, select *Mac File*. This will open up a window to configure the Mac File properties.

- Name: "Mac File Policy Check"
- Mac File Checker: Select *Enabled* next to "Continuously check the result and end the session if it changes" section, if you wish to provide an ongoing policy check on the endpoint state. If you wish to only have a check when the device logs in, then select *Disabled*.
- FileName:

    - If you are using the persistent, installed MetaAccess agent, use "*Applications/OPSWAT GEARS Client/Policies/GEARS_<license key>_1.txt*"
        - The *<license key>* value will be **your** *MetaAccess License Key.* You can find this information at Settings > Global Settings
        - The "1" represents the Policy Value of a device that passes the policy defined in MetaAccess console.
    - If you are using the on demand, portable MetaAccess agent, use "*/Users/<username>/Documents/OPSWAT/GEARS OnDemand/ GEARS_<license key>_1*"
        - The *<license key>* value will be **your** *MetaAccess License Key. You can find this information at Settings > Global Settings*
        - The "1" represents the Policy Value of a device that passes the policy defined in MetaAccess console.
- Date: 1970-01-01 00:00:00
    - This is the default date, which is the same as specifying no file check date



Name: Mac File Policy Check

Mac File Checker

Continuously check the result and end the session if it changes: Enabled

Insert Before: 1

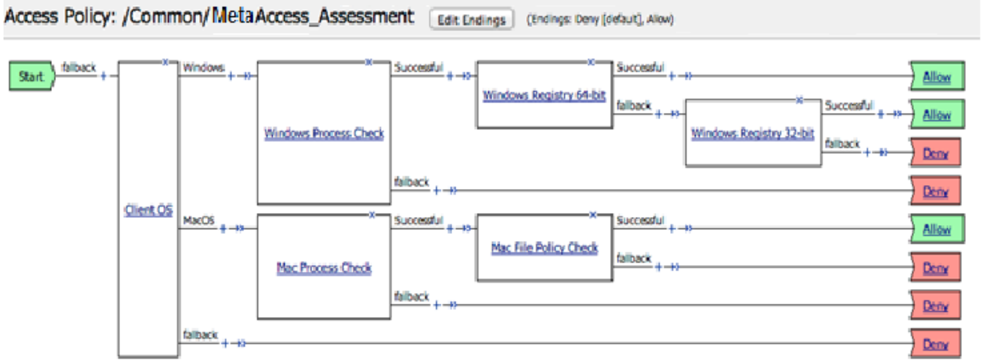
	FileName	MD5	Size (bytes)	Date	
1	"Applications/OPSWAT GEARS		0	1970-01-01	☒

Click *Save*.

Step 8:

Once you have configured for the policy checks for Windows and Mac, modify the response based on *Successful* or *Failure* outcome – Allow or Deny.

Your final policy should look like this:



Access Policy: /Common/MetaAccess_Assessment (Endings: Deny [default], Allow)

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.