

# PowerShell Sensor - Guideline

Please find below couple guidelines whenever you want to use the Microsoft Powershell Sensor for custom scripts.

## Custom scripts (Standard Powershell, Exchange, Sharepoint)

Custom script must be enclosed as a function definition.

E.g.

```
function doStuff()  
{  
    param($param1)  
    custom script  
}
```

A function definition must be saved in a file e.g. dostuff.ps1

In GL enter dostuff in the field "Script Filename" excluding the file extension ".ps1".

doStuff -param1 parameterValue in the field "Parameters"

### Restrictions:

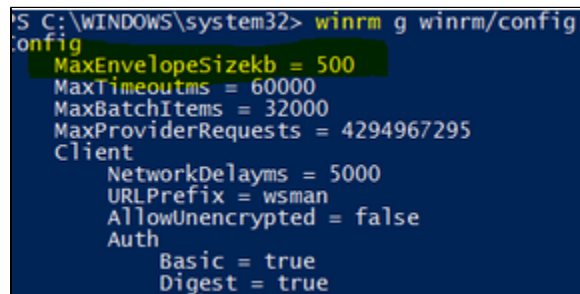
- If the script uses a parameter which is the target server, it must be defined as "server" in order to be resolved automatically from the "Targets" list. Following the example above the "Parameters" field will contain:

*doStuff -param1 parameterValue -server*

The value for the parameter "server" will be set automatically from the "Targets" list for each selected target.

- MaxEnvelopeSizekb parameter on the server gives the size of Soap message that can be sent. Scripts or commands are sent within Soap messages. The config for a server:

*winrm g winrm/config*



```
'S C:\WINDOWS\system32> winrm g winrm/config  
config  
MaxEnvelopeSizekb = 500  
MaxTimeoutms = 60000  
MaxBatchItems = 32000  
MaxProviderRequests = 4294967295  
Client  
NetworkDelays = 5000  
URLPrefix = wsman  
AllowUnencrypted = false  
Auth  
    Basic = true  
    Digest = true
```

- Likely that you have to increase the MaxMemory level on the remote host

what are the current values ?

*winrm get winrm/config/winrs*

set new max memory value (e.g. 1024MB)

*winrm set winrm/config/winrs '@{MaxMemoryPerShellMB="1024"}'*

## Cmndlet (Standard Powershell, Exchange, Sharepoint)

- Files containing cmdlets must exist: ps\_commands.txt, exchange\_ps\_commands.txt, sharepoint\_ps\_commands.txt.
- The field "Commandlet Name" is autocomplete field shows **only** cmdlets of the relevant context (Standard Powershell, Exchange, Sharepoint).  
Cmndlets not in the files are not allowed.

- The field "Parameters" can contain arguments, flags and piped commands. The following must be observed:

Each argument or flag starts with "-"

Each piped Cmndlet must start with "|"

Each argument, flag or piped cmdlet must in a new line. E.g.

-startDate 12/10/2014

Commandlet Name *	Get-Mailbox
Parameters	<div>-Identity r[redacted]@panagenda GmbH.onmicrosoft.com   Get-MailboxStatistics</div>
Only one parameter or parameter-value pair per line	

## Office365

Presently only cmdlets can be executed. Files containing cmdlets must exist in files: o365\_exchange\_ps\_commands.txt, o365\_sec\_and\_compliance\_ps\_commands.txt. The following cmdlets types can be executed:

- Exchange
- Security and Compliance for Exchange