PowerShell Sensor - Exchange

Introduction

There are dozens/hundreds of usecases what you can do with Exchange powershell cmdlets.
This kbase shows you a simple configuration how you can utilize the Test-Mailflow cmdlet with the GL MS Powershell Sensor for an on-premises Exchange Server .

Configuration

Requirements

Before you start the configuration, please make sure that you cover the following requirements on the Exchange Server Level:

- **Activate remote Powershell settings on the target host (issue the following commands in the powershell console of a target)**

  Enable-PSRemoting –force

  set-item -force WSMan:\localhost\Service\Auth\Basic $true

  set-item -force WSMan:\localhost\Client\AllowUnencrypted $true

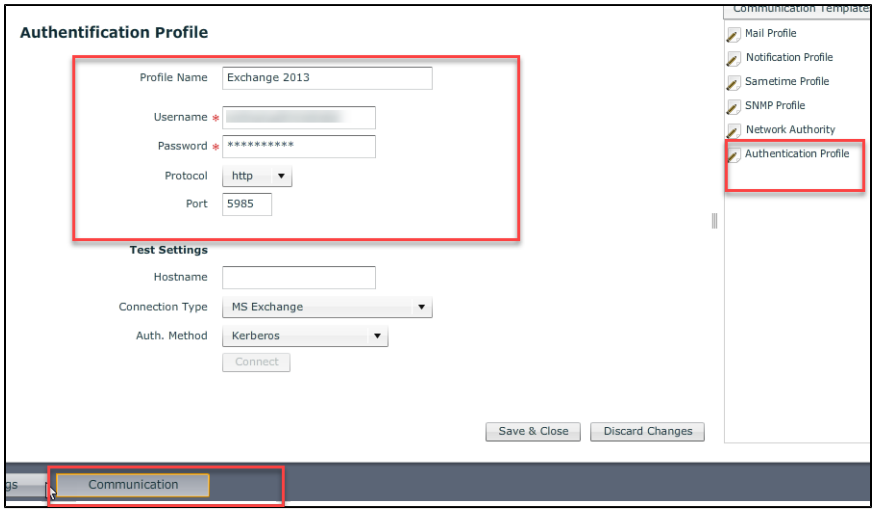
  set-item -force WSMan:\localhost\Service\AllowUnencrypted $true

- Make sure that you have an **Account** which is member of the local Administrator Group of the Target-Host (no need to be a Domain Admin!)
- **TCP Port 5985** (and 5986) needs to be opened between GreenLight and Target-Host

Depending on your requirements you could configure encrypted powershell communication as well (a bit more to configure) : Using SSL for Remote PowerShell in GreenLight

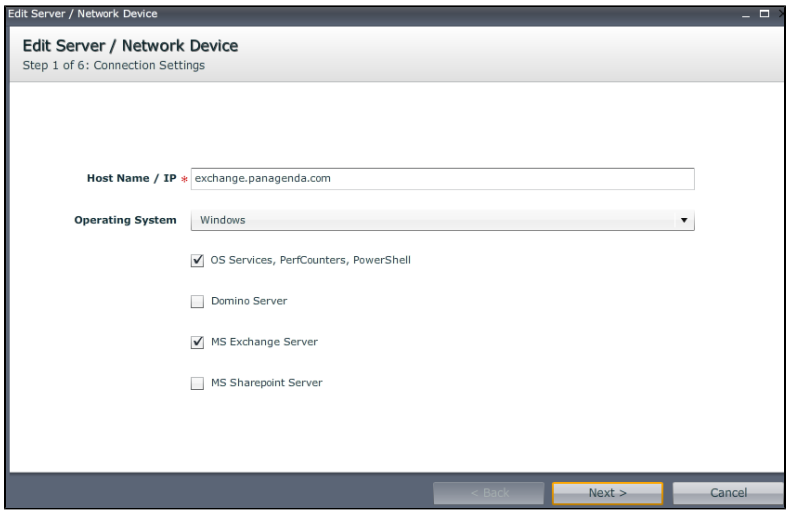
Create an Authentication Profile

- Give it a Profile Name
- Enter Username/Password
- select http
- Port: 5985



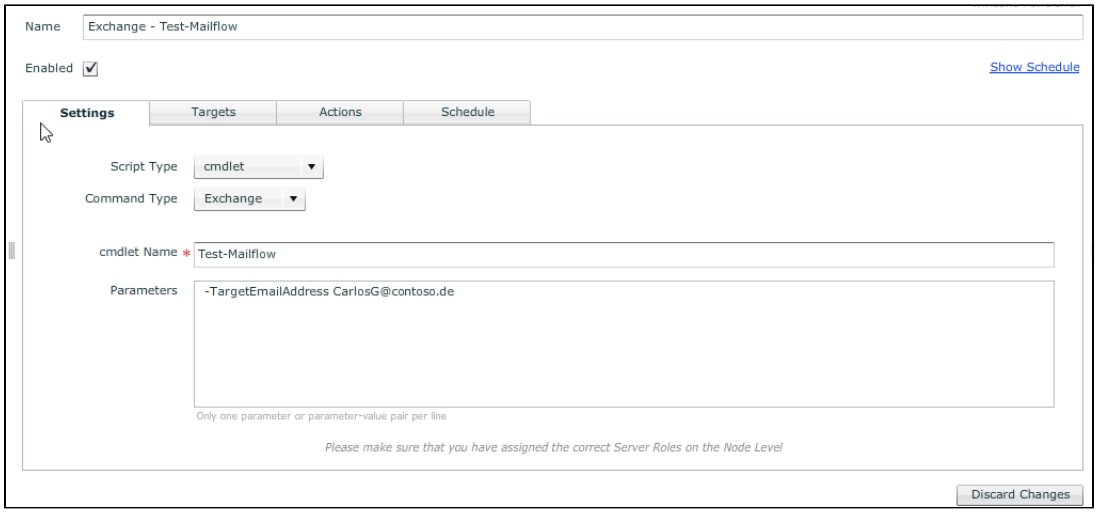
Add Server

Add your on-premises Exchange server to the GreenLight Server list and select "OS Services,PerfCounters, Powershell" and "MS Exchange"



Configure MS PowerShell Sensor

- Script Type: cmdlet
- Command Type: Exchange
- cmdlet Name: Test-Mailflow
- Parameters: -TargetEmailAddress <mailaddress>



- Assign the previously created server as a Target

Output:

greenlight.powershell.exchange.1.Identity		
greenlight.powershell.exchange.1.IsRemoteTest	1	
greenlight.powershell.exchange.1.IsValid	1	
greenlight.powershell.exchange.1.MessageLatencyTime	00:00:19.2055841	
greenlight.powershell.exchange.1.ObjectState	New	
greenlight.powershell.exchange.1.PSComputerName	srv-2	
greenlight.powershell.exchange.1.PSShowComputerName	0	
greenlight.powershell.exchange.1.RunspaceId	2da5d9db-311b-4cfb-...	
greenlight.powershell.exchange.1.TestMailflowResult	Success	
greenlight.powershell.exchange.1.ToString	Microsoft.Exchange.M...	

I assume the important output line is, if the Result shows "Success" or "Failed"