Advanced Threat Analytics (ATA) Version 1.6 introduced a new deployment option, the ATA Lightweight Gateway, to allow customers to deploy the ATA Gateway directly on a domain controller, without the necessity of a dedicated ATA Gateway server and the added complexity of port mirroring from the domain controller to the ATA Center.

As customers have embraced this new paradigm, some of our engagements have asked us to deploy the ATA Lightweight Gateway to dozens, if not hundreds, of domain controllers. This scenario is common when there are multiple branch sites and IaaS deployments. The current deployment model does not support scaling to this level.

In an effort to help my customer deploy to multiple branches, I wrote a PowerShell script to read a list of servers from a file and deploy the ATA Gateway to each server. This allows us to strategically roll out and deploy across the enterprise. We can select the appropriate groups of servers to deploy to maintain availability across the enterprise.

This script has been tested with standalone ATA Gateway servers as well as Lightweight Gateways. These servers are Windows Server 2012 R2. The script copies the Microsoft ATA Gateway Setup.zip file to each server and unzips the contents. A new PSSession is created and runs the Microsoft ATA Gateway Setup.exe on the host with the quiet options (see <https://docs.microsoft.com/en-us/advanced-threat-analytics/deploy-use/ata-silent-installation> for detailed command line information). This requires that PowerShell remoting must be enabled, either through Group Policy, or on the host, via PowerShell’s Enable-PSRemoting cmdlet. The script was written and run from PowerShell ISE version 5.0.

Because the installation command runs in quiet mode (“/quiet”) it is not currently possible to capture any error messages that may be the result of installation failure. As a workaround, I have used the ATA Center console to determine if Gateways have not installed correctly. This is an area for future enhancement.

Another enhancement will be to run the deployments asynchronously, to scale to an even larger deployment. I decided to write this synchronously initially, to avoid flooding the Center with new gateways.

I hope our customers will find this useful in their large scale deployments. The code is available at my github site,

https://github.com/csmithk/ataGatewayDeploy/blob/master/RunATAGatewayInstallation.ps1

Cathy Smith

Senior Consultant

Cybersecurity Group