TPM Verifier – Policy Flow

Installation Instructions for Forescout eyeSight

By David Clapp

Date: 10/26/2022

# Requirements:

* Forescout eyeSight 8.4.x
* Remote Inspection and/or SecureConnector configured/deployed
* Forescout Console Admin role/level permissions

# Installation Steps

1. Extract the file TPMPolicyPack.zip to its own folder: TPMPolicyPack -note its location on your computer
2. Open and log into the Forescout Console with an account that has administrator role capabilities
3. Navigate to dropdown menu: Tools > Group Manager
4. Within the group tree navigate to a folder where you want to store the TPM groups (which will also be in their own folder) and then click the import button:  
   
5. Navigate to the TPMPolicyPack folder that was created when you extracted the TPMPolicyPack.zip file.
   1. Select “TPM Policy Groups.xml”
   2. Click Import
   3. Click OK and then OK
   4. Verify you have the following groups before proceeding:  
      Graphical user interface, application

      Description automatically generated
6. Go to the Policy Tab in the Forescout console:
7. Right click on a policy folder where you would like to import the TPM policies (these will be contained in their own folder)  
   Graphical user interface, application

   Description automatically generated
8. A window will appear, click on the  to select the policy file: TPM\_Policies.xml, click Select, Click OK
9. You should now see the following folders and policies:

Table

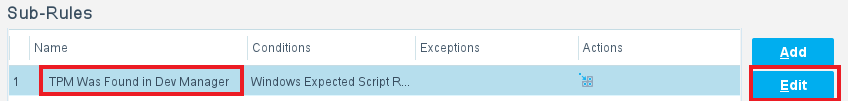
Description automatically generated with medium confidence

1. The scopes for “A. Verify: TPM – Capable” needs to be changed. Currently, it is set to broadly.
   1. Therefore, re-scope it by right clicking on the policy and selecting Edit…  
      Graphical user interface, application

      Description automatically generated
   2. Click on the Edit next to scope so we can constrain this policy to a test group:  
      A picture containing shape

      Description automatically generated
   3. A window will appear, click on the “wrench with a gear” button and then click the Add button  
      Graphical user interface, application

      Description automatically generated
   4. Add a small test group to start with and then click ok and ok.
2. Go back to the policy main page and right click on the policy (A. Verify: TPM – Capable) and select Edit…  
   Graphical user interface, application

   Description automatically generated
3. Click on the “TPM Was Found in Dev Manager” subrule and select Edit:  
   
4. Click on the “Windows Expected Script Result…” and select Edit  
   Graphical user interface, text, application

   Description automatically generated
5. Next, click on the blue box with … next to Command or Script File  
   
6. In the next window, click on the Add button:  
   Graphical user interface, application

   Description automatically generated
7. Next, click on the blue box … to select the file. Navigate to the scripts folder inside TPMPolicyPack and select CheckDMforTPM2.vbs  
   Graphical user interface, application

   Description automatically generated
8. Click Open, Set Title to: Checks Device Manager for TPM, click OK
9. Perform steps 13 – 15 one more time, but select the file CheckTPMEnabled.vbs and Title: Checks if TPM Enabled in Windows, Click OK three more times and then click:

 in the main policy screen.

1. Start Policies in order: A. Verify: TPM – Capable, B. Verify: TPM – Enable State, C. Verify: TPM -Version