How do I configure EPA for Windows Update Check?

Use Case

Scan the user device for Windows update and take a decision to allow or deny access to internal network.

Introduction to EPA

On NetScaler Gateway, End Point Analysis (EPA) can be configured to check if a user device meets certain security requirements and accordingly allow access of internal resources to the user.

This can be configured by using preauthentication policy. If the user device fails the preauthentication scan, users are not allowed to log on.

If additional security is needed, a session policy can be configured and bound to a AAA user or group or VPN vserver or VPN global level. This type of policy is called a post-authentication policy, which runs during the user session to ensure the required software, such as antivirus is running. If the policy fails, the connection to NetScaler Gateway ends.

The Endpoint Analysis Plug-in downloads and installs on the user device when users log on to NetScaler Gateway for the first time. If a user does not install the Endpoint Analysis Plug-in on the user device or chooses to skip the scan, the user cannot log on with the NetScaler Gateway Plug-in. Optionally, user can be put in a quarantine group where (s)he gets limited access to internal network resources.

Configuration Steps

Step 1: Create Preauthentication profile

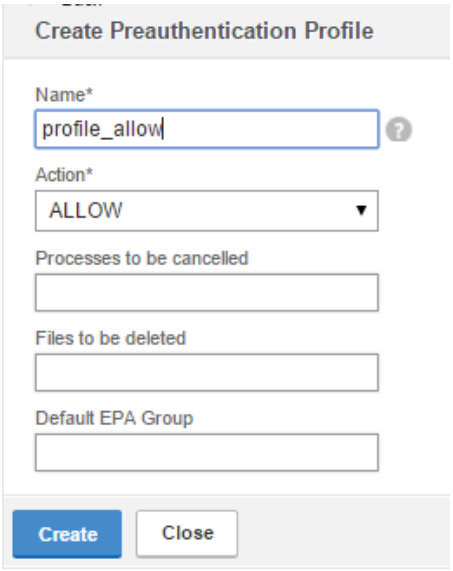
Create preauthentication profile which contains the action to allow or deny logon after preauthentication policy check. Optionally admin can also configure process to be cancelled and files to be deleted by EPA tool and also the default group that is chosen when the EPA check succeeds.

CLI:

> add preauthenticationaction <action name> ALLOW

GUI:

Go to NetScaler Gateway -> Policies -> Preauthentication Profiles -> Add



Step 2: Create Preauthentication Policy

Create preauthentication policy with a profile and an expression to check for windows update on user device.

CLI:

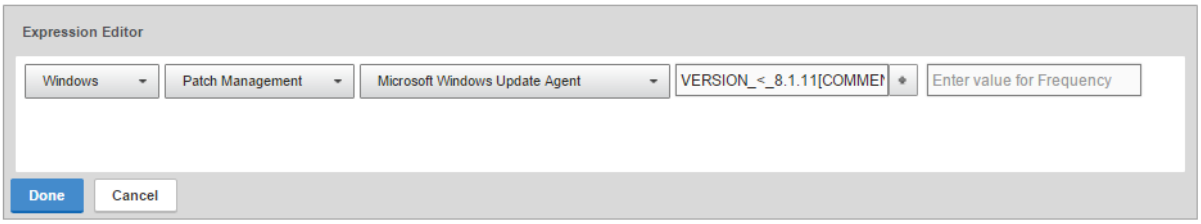
add aaa preauthenticationpolicy <policy name> "CLIENT.APPLICATION(\'PATCH_80400_VERSION_<_8.1.11[COMMENT: Microsoft Windows Update Agent]\') EXISTS" <preauthentication profile name>

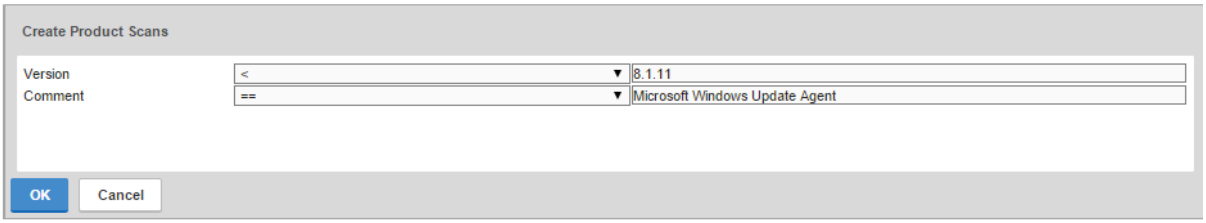
In this example, expression PATCH_80400 corresponds to Microsoft Windows Update on user device. In this expression, it checks in the client device if Windows update version is less than 8.1.11. Also, comment is added to add reference information about the scan.

GUI:

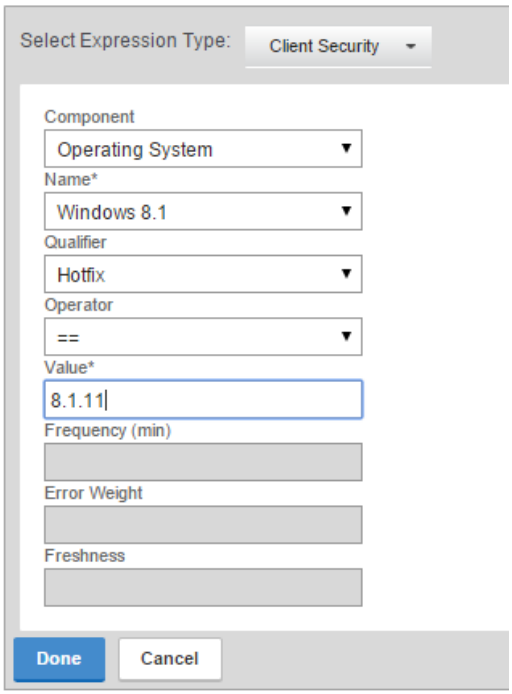
To create policy go to NetScaler Gateway -> Policies -> Preauthentication Policies -> Add. You can use OPSWAT EPA editor to create custom EPA expression.

Selecting Microsoft Windows Update Agent will give expression to check for the presence of the Windows update agent in client device. Additional parameters can be added to the expression by clicking on the + button and filling the required values about the Windows update.





If classic expression editor is used, then the following are the fields to be selected.



Step 3: Binding Preauthentication Policy

CLI:

For global binding use the following command.

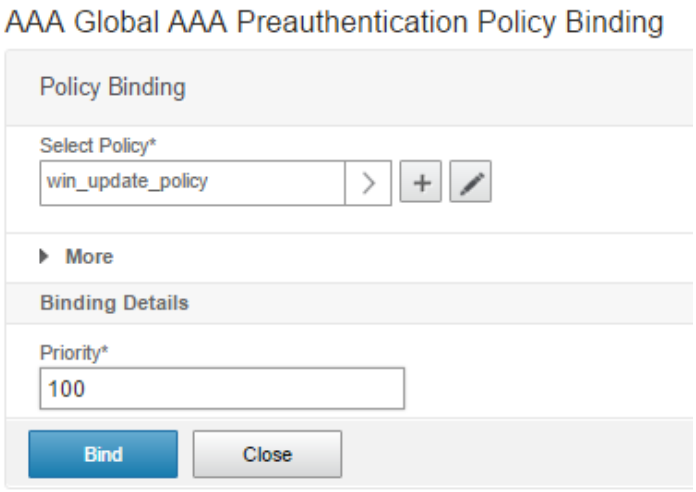
> bind aaa global -policy <preauthentication policy name>

To bind the policy at vserver level, then use the following command.

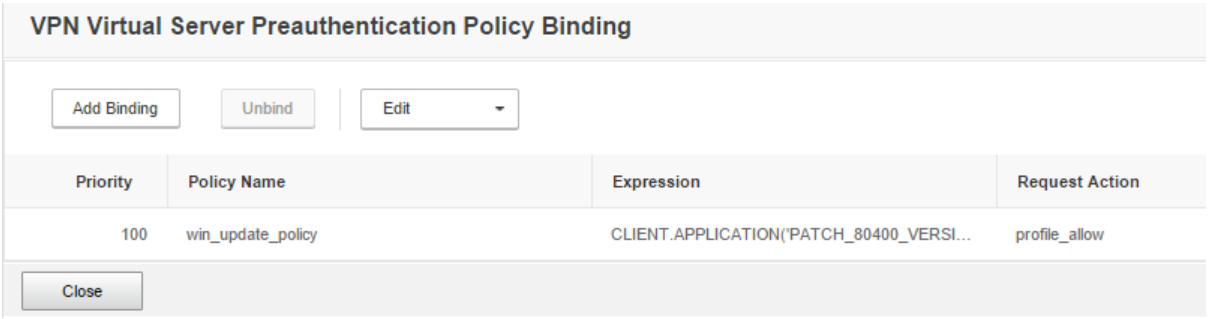
> bind vpn vserver <Gateway virtual server name> -policy <preauthentication policy name>

GUI:

To bind the preauthentication policy globally, select the policy and go to Action -> Global Bindings and do the binding.



To bind the policy at vserver level, go to NetScaler Gateway -> Virtual Servers -> select the virtual server and click edit. In policies section, add preauthentication policy and bind the preauthentication policy created earlier.



For more information about EPA, please see http://docs.citrix.com/en-us/netscaler-gateway/11/vpn-user-config/endpoint-policies.html