How to push a self−signed root certificate with Group Policy or GPO?

Document ID: 118001

Contributed by Khoa Nguyen and Siddharth Rajpathak, Cisco TAC Engineers.

Jul 17, 2014

Contents

Question:

How to push a self−signed root certificate with Group Policy or GPO?

Note: This Knowledge Base article references software which is not maintained or supported by Cisco. The information is provided as a courtesy for your convenience. For further assistance, please contact the software vendor.

With AsyncOS version 5.5.x and above, Cisco Web Security appliance provides the ability to decrypt HTTPS traffic by enabling HTTPS proxy under GUI > Security Services > HTTPS proxy. With HTTPS decryption enabled, clients would need to trust the certificate uploaded or generated under the HTTPS proxy section in order to avoid seeing certificate errors on client machines.

Self−signed or generated certificates on WSA would not be inherently trusted by the client machines & if not trusted, then clients would have to manually accept the certificate warning. If we do not want all users to go through the steps of accepting the untrusted self−signed certificate from the Cisco WSA manually, then we can push the certificate to client machines via Group Policy (GPO).

Please refer to the below articles which provide details on how to accomplish this:

Link: http://www.unixwiz.net/techtips/deploy−webcert−gp.html

Link: http://technet.microsoft.com/en−us/library/cc738131(v=ws.10).aspx

Link: http://technet.microsoft.com/en−us/library/cc770315(v=ws.10).aspx