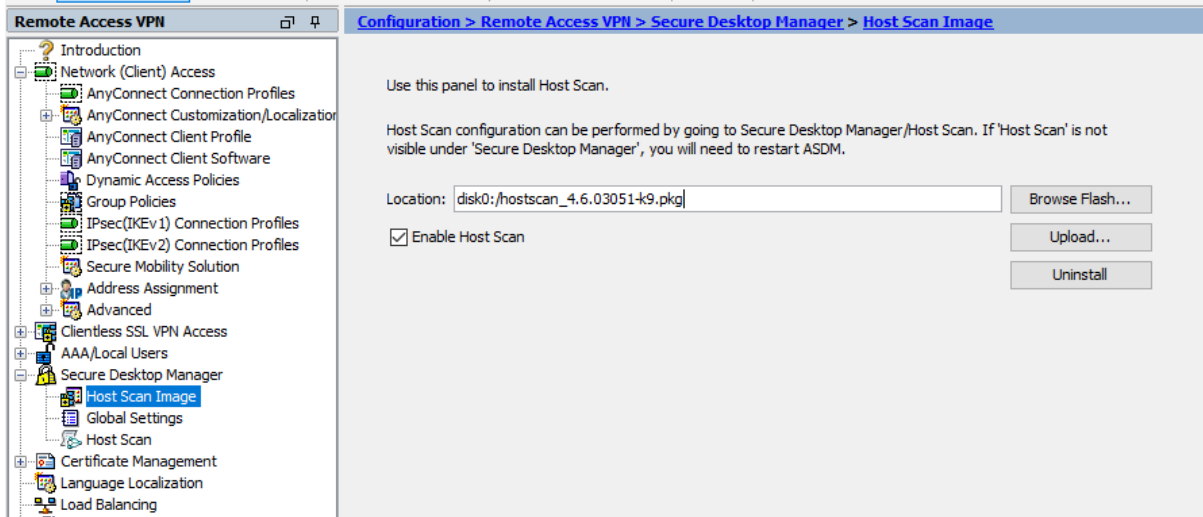


Enforce DAP Based on CSD Host Scan for Domain Registry Key:

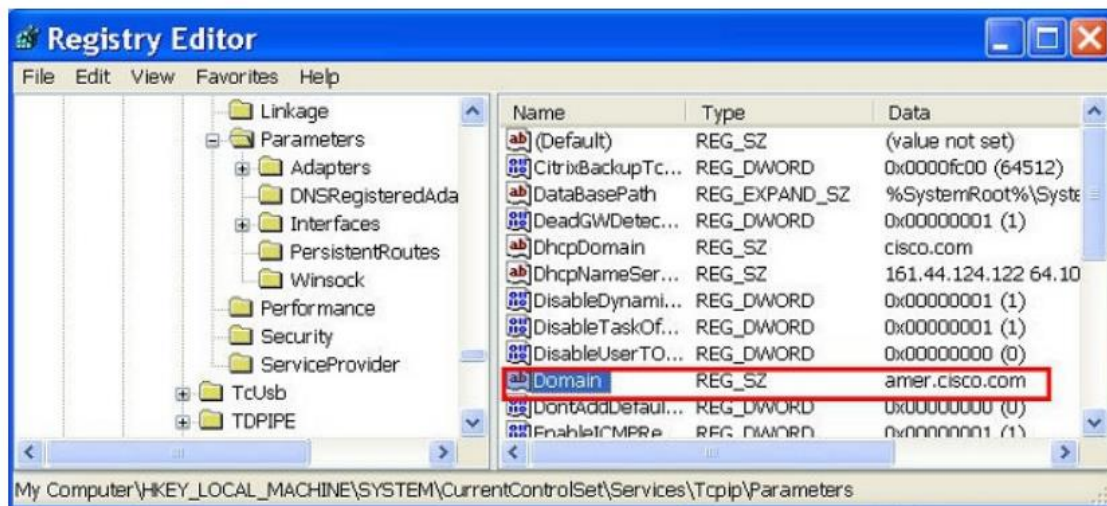
1. Upload and install the Host Scan package:



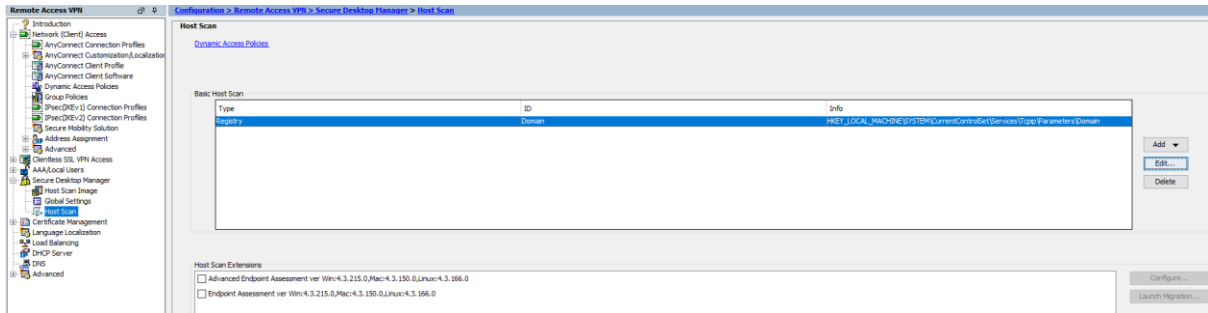
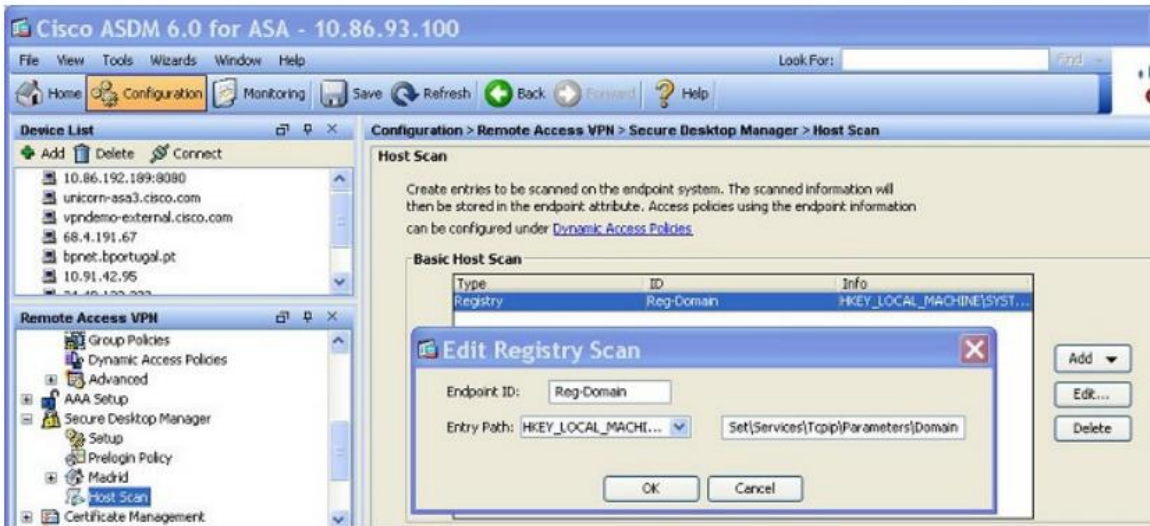
Enforce DAP Based on CSD Host Scan for Domain Registry Key

This procedure provides an example of a configuration procedure with ASDM.

1. Locate the registry key that holds the domain at
\\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Domain.

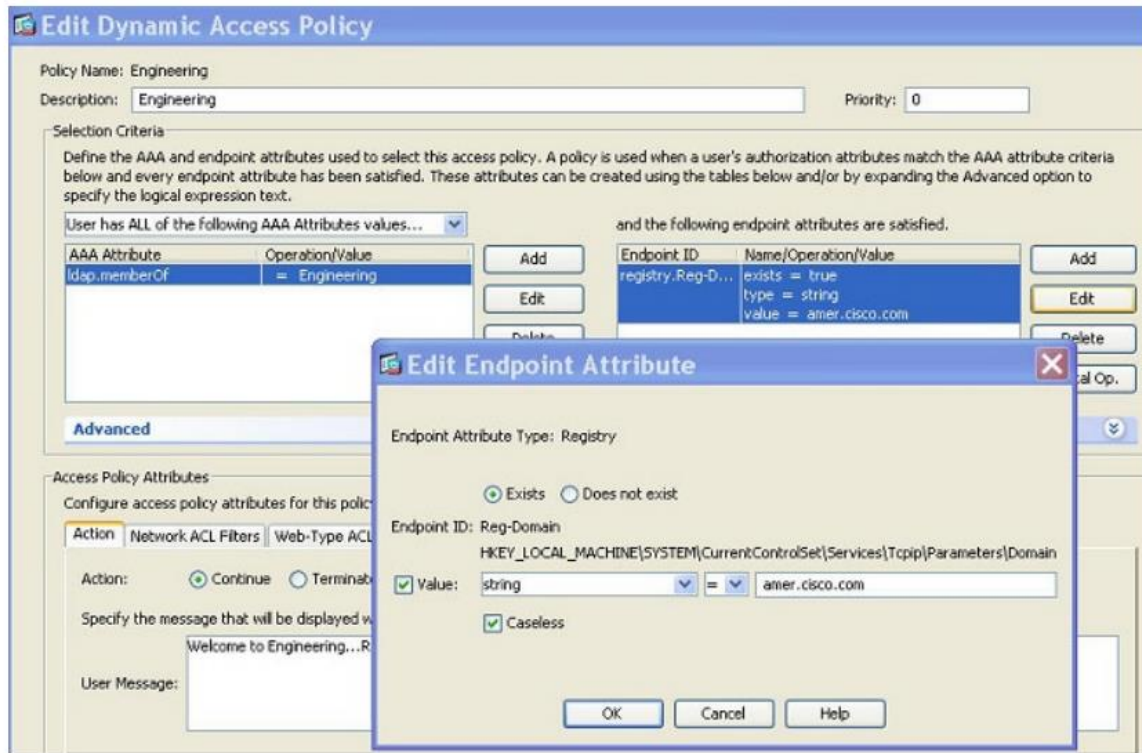


2. Define the host scan parameter for the registry setting.



ID	Info
Domain	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Domain

3. Apply the registry endpoint attribute to the DAP policy.




[Configuration > Remote Access VPN > Network \(Client\) Access > Dynamic Access Policies](#)

Configure Dynamic Access Policies

For IPsec, AnyConnect Client, Clientless SSL VPN, and Cut-Through-Proxy sessions, you can configure dynamic access policies (DAP) that define which network resources a user is authorized to access matched, the ASA will enforce the DftAccessPolicy.

To use certain Endpoint attributes AV/AS/FW , Enable Host Scan Image with valid package.

ACL Priority	Name	Network ACL List	Webtype ACL List	Description
1	AnyconnectDAPBlock			
0	AnyconnectDAP			
-	DftAccessPolicy			

 Edit Dynamic Access Policy

Policy Name:

Description: ACL Priority:


Selection Criteria
 Define the AAA and endpoint attributes used to select this access policy. A policy is used when a user's authorization attributes match the AAA attribute criteria below and every endpoint attribute has been satisfied. These attributes can be created using the tables below and/or by expanding the Advanced option to specify the logical expression text.

User has ALL of the following AAA Attributes values... and the following endpoint attributes are satisfied.

AAA Attribute	Operation/Value	Endpoint ID	Name/Operation/Value
cisco.tunnelgroup	= Test	registry.Domain	exists = true type = string value = exchange.local

Access/Authorization Policy Attributes
 Configure access/authorization attributes for this policy. Attribute values specified here will override those values obtained from the AAA system and the group-policy hierarchy. The resulting VPN authorization policy is an aggregation of DAP attributes, AAA attributes, and group-policy hierarchy attributes (those that are not specified in DAP).

Port Forwarding Lists	Bookmarks	Access Method	AnyConnect	AnyConnect Custom Attributes
Action	Network ACL Filters (client)		Webtype ACL Filters (clientless)	Functions
Action: <input checked="" type="radio"/> Continue <input type="radio"/> Quarantine <input type="radio"/> Terminate <input type="button" value="i"/>				
Specify the message that will be displayed when this record is selected.				
User Message: <input type="text"/>				

 Edit Dynamic Access Policy

Policy Name:

Description: ACL Priority:

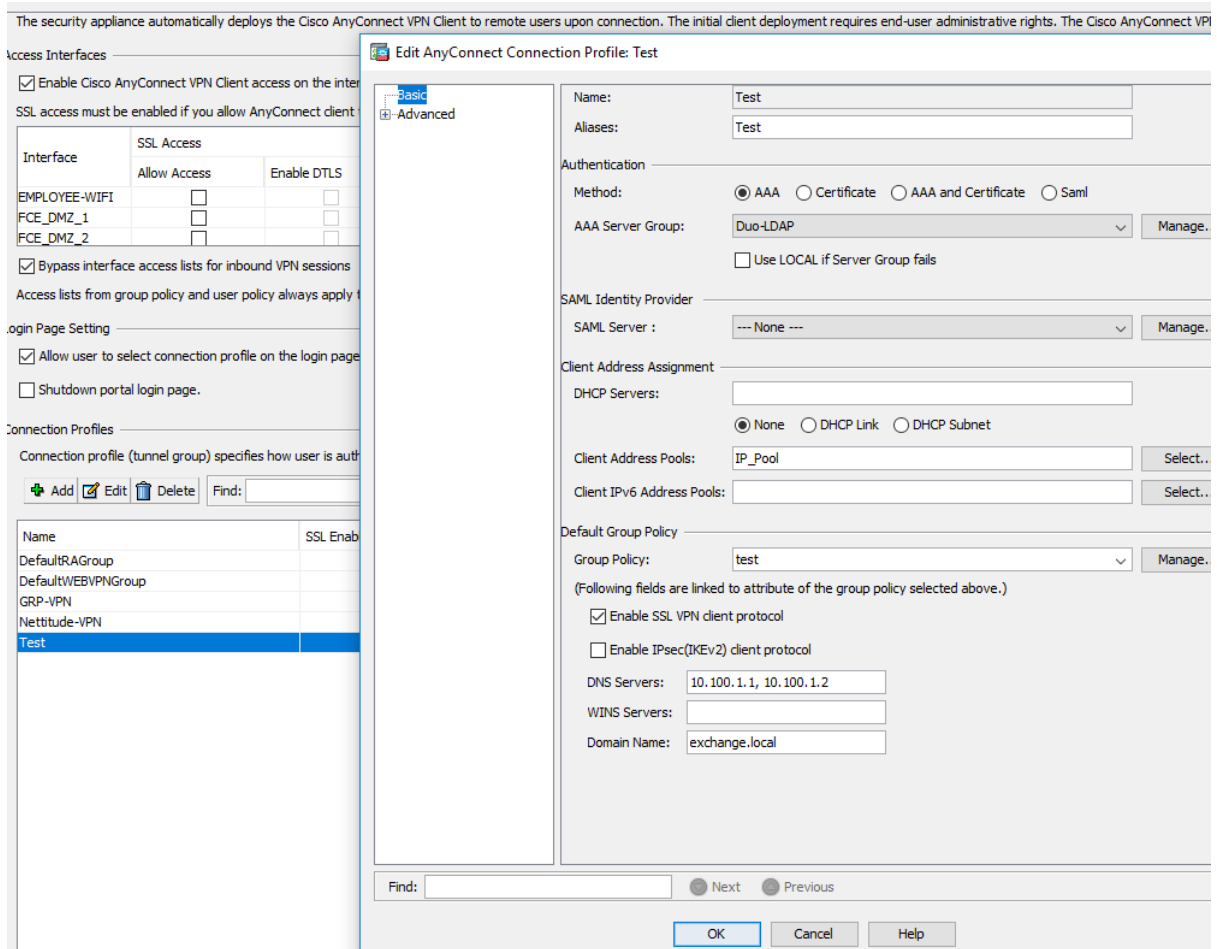
Selection Criteria
 Define the AAA and endpoint attributes used to select this access policy. A policy is used when a user's authorization attributes match the AAA attribute criteria below and every endpoint attribute has been satisfied. These attributes can be created using the tables below and/or by expanding the Advanced option to specify the logical expression text.

User has ALL of the following AAA Attributes values... and the following endpoint attributes are satisfied.

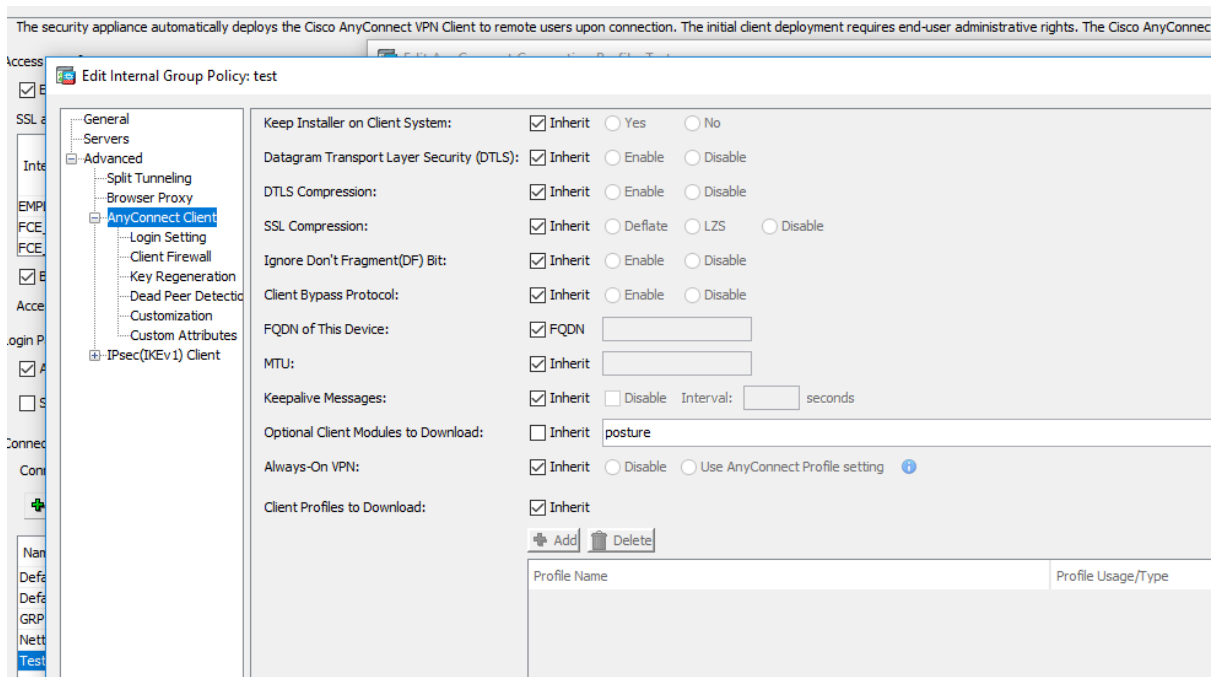
AAA Attribute	Operation/Value	Endpoint ID	Name/Operation/Value
cisco.tunnelgroup	= Test	registry.Domain	exists = true type = string value != exchange.local

Access/Authorization Policy Attributes
 Configure access/authorization attributes for this policy. Attribute values specified here will override those values obtained from the AAA system and the group-policy hierarchy. The resulting VPN authorization policy is an aggregation of DAP attributes, AAA attributes, and group-policy hierarchy attributes (those that are not specified in DAP).

Port Forwarding Lists	Bookmarks	Access Method	AnyConnect	AnyConnect Custom Attributes
Action	Network ACL Filters (client)		Webtype ACL Filters (clientless)	Functions
Action: <input type="radio"/> Continue <input type="radio"/> Quarantine <input checked="" type="radio"/> Terminate <input type="button" value="i"/>				
Specify the message that will be displayed when this record is selected.				
User Message: <input type="text"/>				



Allow posture module to be downloaded onto the client under the Group-policy attached to the profile:



Check the ASDM logs using the username you are testing it with