DAP: Enforcing CSD vault operation via process checks

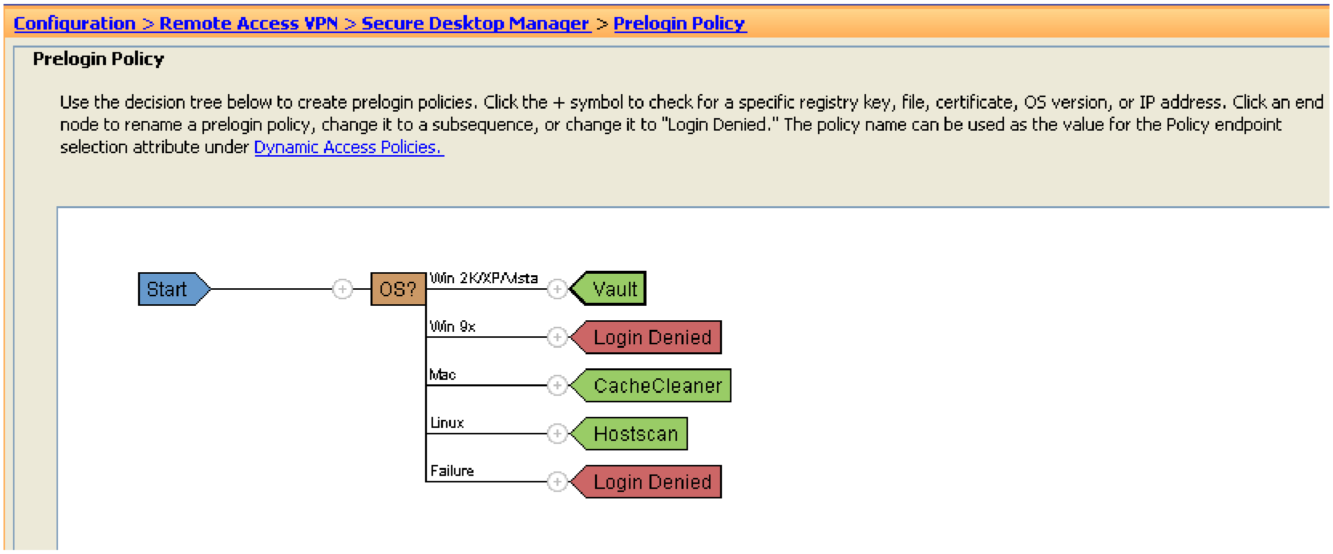
From ASApedia

This simple example shows how to enforce process checks via Dynamic Access Policy (DAP) that specifies that Vista machines must be running CSD Vault to allow the Clientless SSL VPN session to be established.

Configuration steps

1) In ASDM, under Configuration-Remote Access VPN-Secure Desktop Manager-Prelogin Policy, define Prelogin check(s) .

We chose an OS check for Vista and a policy name called Vault. Other types of checks or nested checks can be performed depending on the granularity of the posture assessment desired.

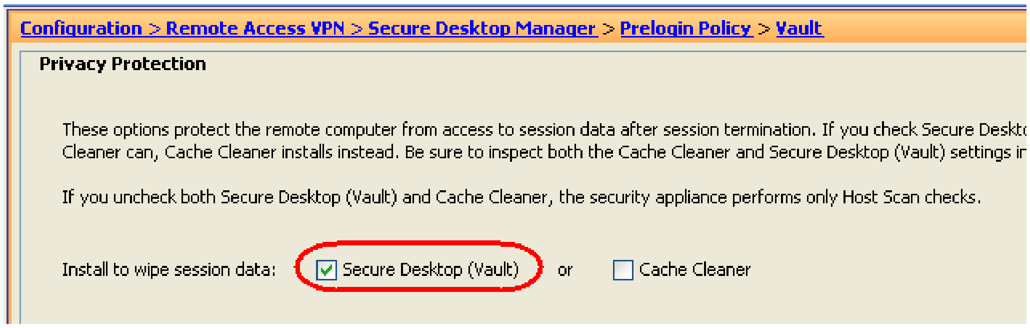


Configuration > Remote Access VPN > Secure Desktop Manager > Prelogin Policy

Prelogin Policy

Use the decision tree below to create prelogin policies. Click the + symbol to check for a specific registry key, file, certificate, OS version, or IP address. Click an end node to rename a prelogin policy, change it to a subsequence, or change it to "Login Denied." The policy name can be used as the value for the Policy endpoint selection attribute under Dynamic Access Policies.

2)In ASDM, under Configuration-Remote Access VPN-Secure Desktop Manager-Prelogin Policy-Vault, select what functionality the Vault policy will carry out. Select Secure Desktop (Vault) option.



Configuration > Remote Access VPN > Secure Desktop Manager > Prelogin Policy > Vault

Privacy Protection

These options protect the remote computer from access to session data after session termination. If you check Secure Deskt
Cleaner can, Cache Cleaner installs instead. Be sure to inspect both the Cache Cleaner and Secure Desktop (Vault) settings ir

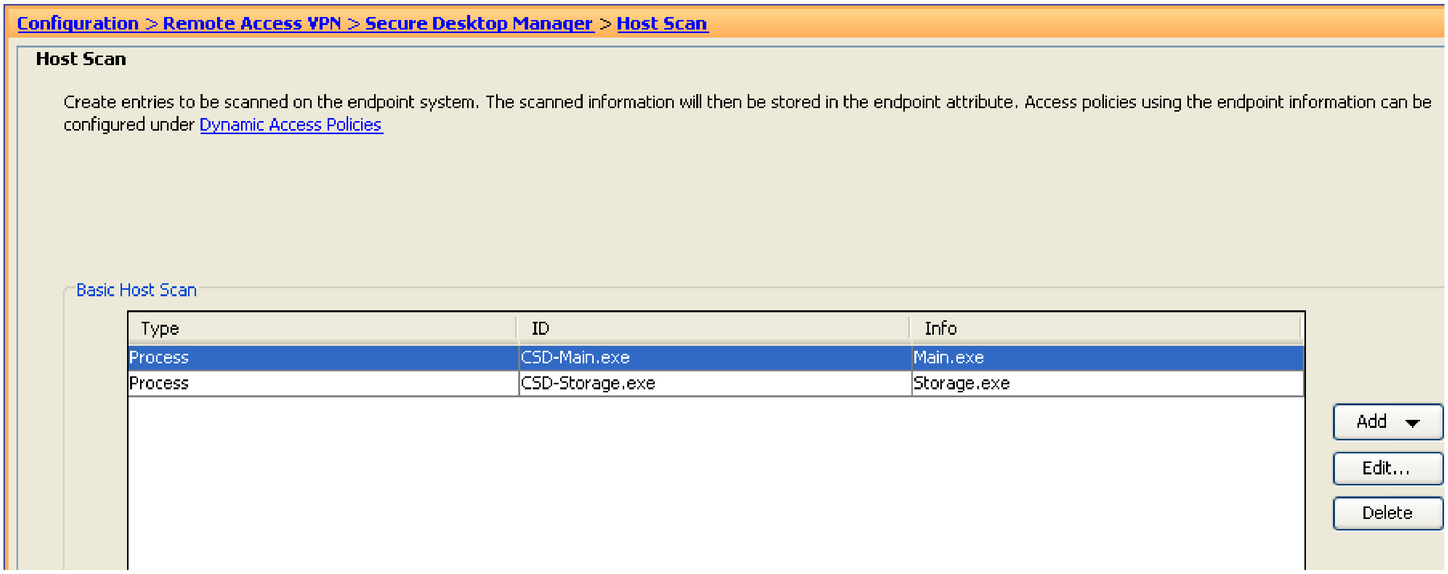
If you uncheck both Secure Desktop (Vault) and Cache Cleaner, the security appliance performs only Host Scan checks.

Install to wipe session data: ☑ Secure Desktop (Vault) or □ Cache Cleaner

3)In ASDM, under Configuration-Remote Access VPN-Secure Desktop Manager-Host Scan,define the process(es) that represent the Vault.

CSD Vault spawns 2 processes: Main.exe and Storage.exe. Hostcan spawns Host.exe and Cache Cleaner spawns Cleaner.exe.

We chose 2 process IDs(names) for the 2 Vault processes.



Configuration > Remote Access VPN > Secure Desktop Manager > Host Scan

Host Scan

Create entries to be scanned on the endpoint system. The scanned information will then be stored in the endpoint attribute. Access policies using the endpoint information can be configured under Dynamic Access Policies

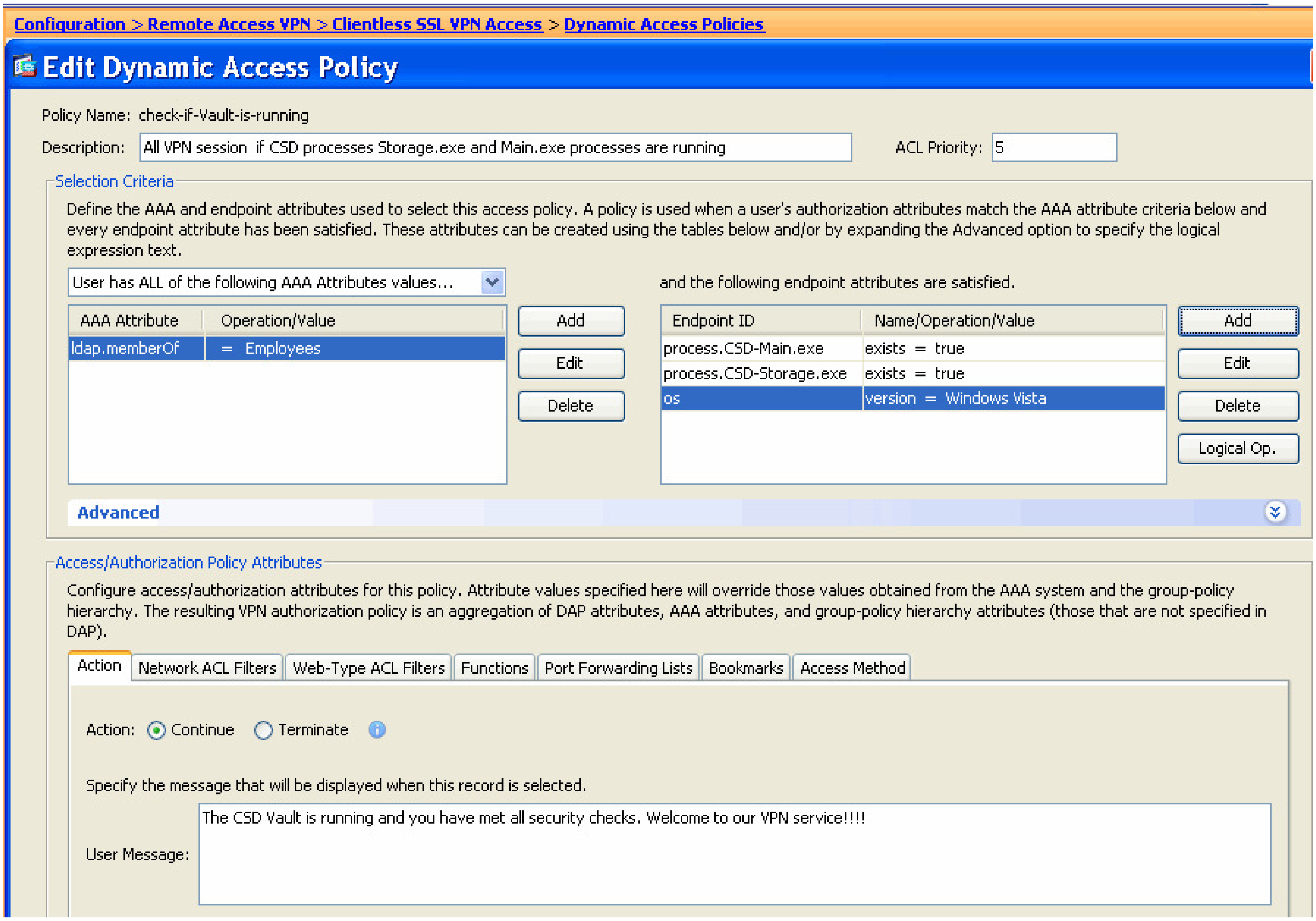
Basic Host Scan

Type	ID	Info
Process	CSD-Main.exe	Main.exe
Process	CSD-Storage.exe	Storage.exe

4) Define a DAP policy with the required checks

In our example we assume the VPN remote access will use Active Directory for authentication.

- The AAA attribute verifies the user is part of the AD's Employees group
- The endpoint.process attributes verifies that CSD is running
- The endpoint.os check attribute verifies tha t only Vista machines meet this DAP policy



Configuration > Remote Access VPN > Clientless SSL VPN Access > Dynamic Access Policies

Edit Dynamic Access Policy

Policy Name: check-if-Vault-is-running

Description: All VPN session if CSD processes Storage.exe and Main.exe processes are running

ACL Priority: 5

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...

AAA Attribute	Operation/Value
ldap.memberOf	= Employees

and the following endpoint attributes are satisfied.

Endpoint ID	Name/Operation/Value
process.CSD-Main.exe	exists = true
process.CSD-Storage.exe	exists = true
os	version = Windows Vista

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).

Action: ● Continue ○ Terminate

Specify the message that will be displayed when this record is selected.

User Message: The CSD Vault is running and you have met all security checks. Welcome to our VPN service!!!!

5) The DAP policy checks represented in LUA are as follows:

```
5540-1(config)# debug menu dap 2


DAP record [    check-if-Vault-is-running       ]:
(EVAL(aaa.ldap.memberOf,"EQ","Employees","caseless")) and ((EVAL(endpoint.os.version,"EQ","Windows Vista","string"))) and ((EVAL(end
point.process["CSD-Main.exe"].exists,"EQ","true","string")) and (EVAL(endpoint.process["CSD-Storage.exe"].exists,"EQ","true","string
")))
```

Alternatively, instead of configuring the Selection Criteria AAA and endpoint attribute boxes, you could paste the string in the DAP Advanced box. Remove the 1st (an last) characters:

```
EVAL(aaa.ldap.memberOf,"EQ","Employees","caseless")) and ((EVAL(endpoint.os.version,"EQ","Windows Vista","string"))) and ((EVAL(end
point.process["CSD-Main.exe"].exists,"EQ","true","string")) and (EVAL(endpoint.process["CSD-Storage.exe"].exists,"EQ","true","string
"))
```

Retrieved from "http://asapedia/index.php/DAP:_Enforcing_CSD_vault_operation_via_process_checks"
Categories: CSD | DAP

- This page was last modified on 17 December 2009, at 10:04.