Posture Conditions:

Posture Conditions form is the check we want to perform against the endpoint to ensure our security policy is being met. Posture conditions are the set of rules in our security policy that define a compliant endpoint. Some of these items include the installation of a firewall, anti-virus software, anti-malware, hotfixes, disk encryption and more. Posture conditions are used to check specific attributes on the client system. There are several categories for assessment options. These conditions can be used alone or in combination with other conditions:

1. File Conditions:

File Conditions checks existence of a file, the date of a file and versions of file on the client.

2. Registry Conditions:

Registry condition checks for existence of registry key or value of the registry key on client.

3. Application Conditions:

A condition that checks if an application (process) is running or not running on the client.

4. Service Conditions:

A condition that checks if a service is running or not running on the client computer.

5. Dictionary Conditions:

A condition that checks a dictionary attribute with a value is called Dictionary Conditions.

6. Firewall Conditions:

The Firewall condition checks if a specific Firewall product is enabled on an endpoint.

1. Compound Conditions:

Contains one or more simple, or compound conditions type File, Registry, Application or Service

2. Antivirus Compound Conditions:

Contains one or more Antivirus conditions, or Antivirus compound conditions.

3. Antispyware Compound Conditions:

Contains one or more Anti-Spyware conditions, or Anti-Spyware compound conditions.

4. Dictionary Compound Conditions:

Contains one or more dictionary simple conditions or dictionary compound conditions.

5. Anti-malware Condition:

The anti-malware condition is a combination of the anti-spyware and antivirus conditions.