Configuring Access Control Service Trustzones

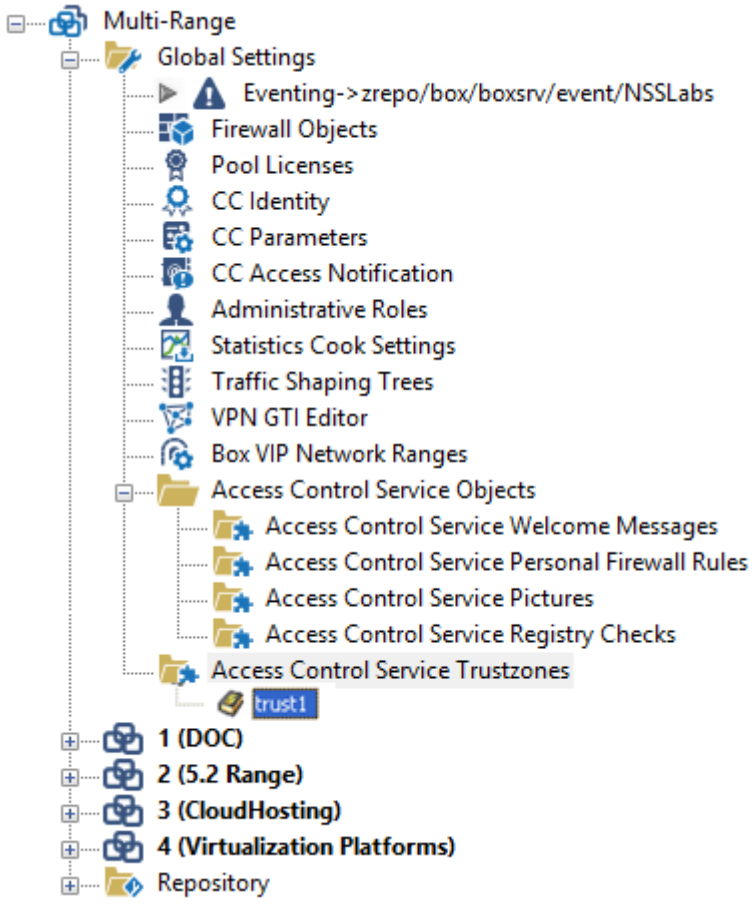
https://campus.barracuda.com/doc/43846874/

Each Access Control Service belongs to a so-called trustzone. To enforce security policies across multiple F-Series Firewalls, the Control Center provides Access Control Service Trustzones as global objects (see also: Configuring Access Control Objects). This advanced feature allows all Access Control services within the same trustzone to share the same set of security policies. In addition, they share a signing key, so that a mutual trust relationship can be established.

In this article:

On stand-alone firewalls, configuration of the trustzone is located in the **CONFIGURATION > Configuration Tree > Box > Virtual Servers > *your virtual server* > Assigned Services > Access Control Service > Access Control Service Trustzones**.

The Control Center provides Access Control Service Trustzones either within the **Global Settings**, **Range Settings** or the **Cluster Settings**.



The predefined Access Control Service Trustzones can be referenced by navigating to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > *your virtual server* > Assigned Services > Access Control Service > Access Control Service Settings > System Health-Validator > Trustzone**.

The NextGen Control Center automatically links the trustzone to the appropriate global / range / cluster object.

Each trustzone contains three policy rulesets. There is a **local machine** policy ruleset that is used to determine a policy for a connecting machine if no user is currently logged in. As soon as user authentication is requested by the connecting client, the **current user** policy ruleset is used for policy matching.

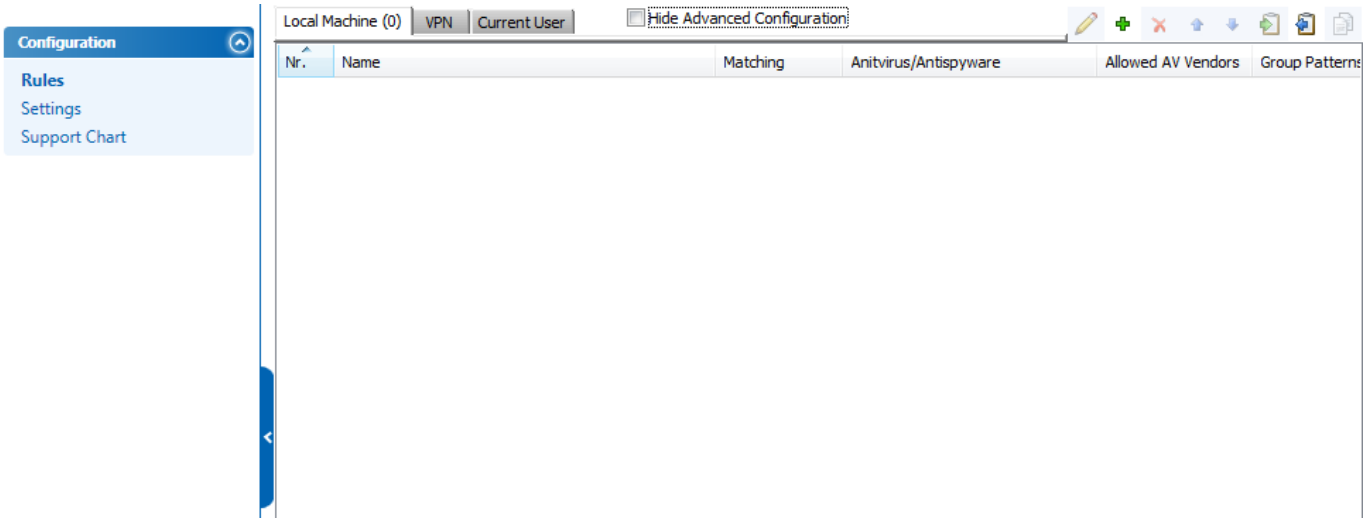
> User authentication can be skipped by setting **Access Control Service Settings > User Authentication > User Authentication Required** to **No**. In addition, local machine rulesets allow user authentication to be skipped for a specific policy rule (**Policy Assignments > Exception > User Authentication Required**).

If the connection attempt is mediated by an intermittent VPN service, the VPN policy ruleset is adopted.

Create an Access Control Server service within **CONFIGURATION > Configuration Tree > Box > Virtual Servers > your virtual server > Assigned Services > Access Control Service**. Click **Access Control Service Trustzone** to open the configuration dialogue.

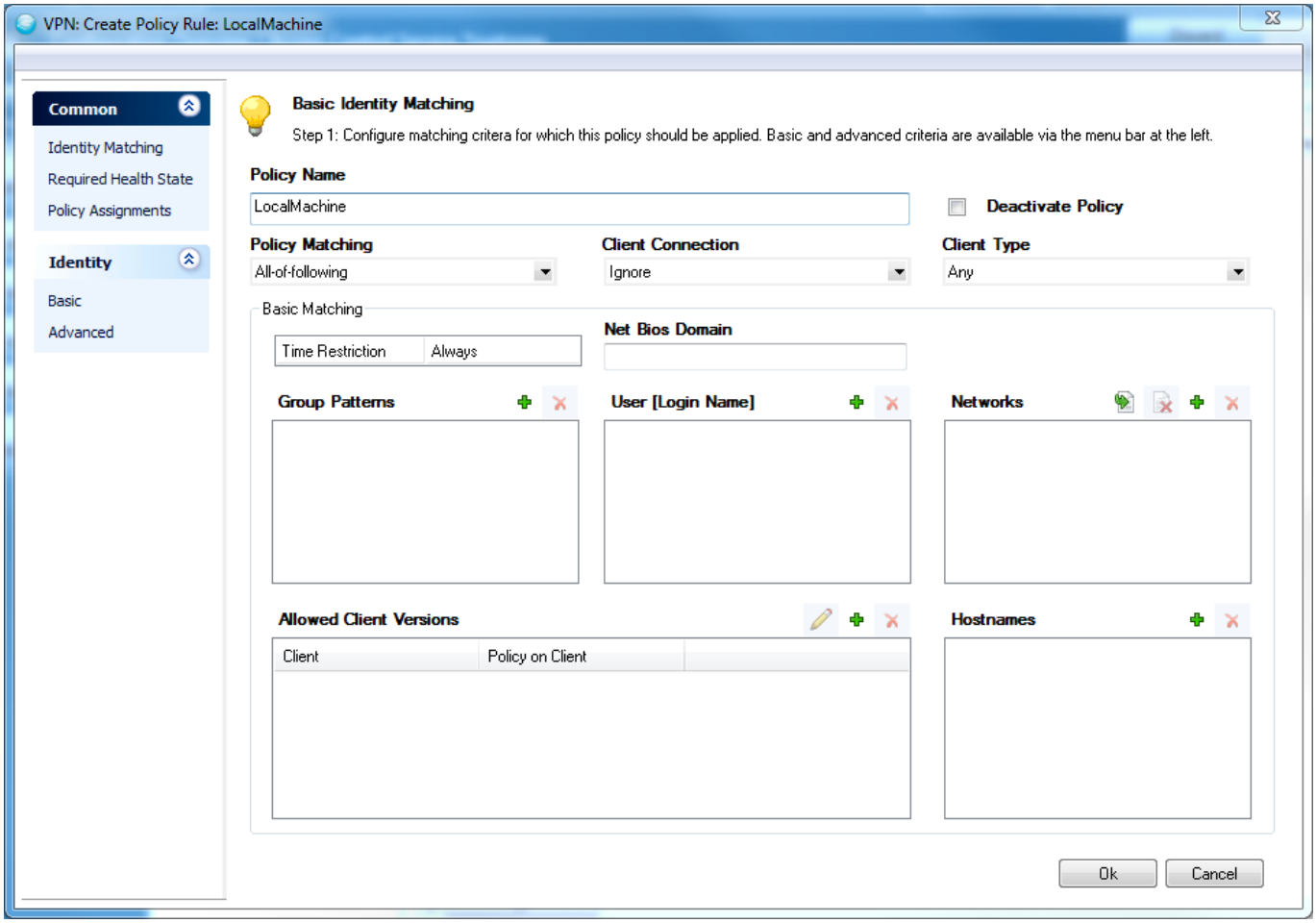
Rules

The main window of an Access Control Service Trustzone is split up into a navigation bar on the left and policy rulesets on the right (if some are already defined).



Identity Matching - Basic

The first step when processing a policy ruleset (either local machine, current user, or VPN) is to determine the client's identity.
Depending on the value of **Basic Matching > Policy Matching**, either all or one of the specified criteria must match to determine the client's identity. If the identity match fails, the next rule is considered.

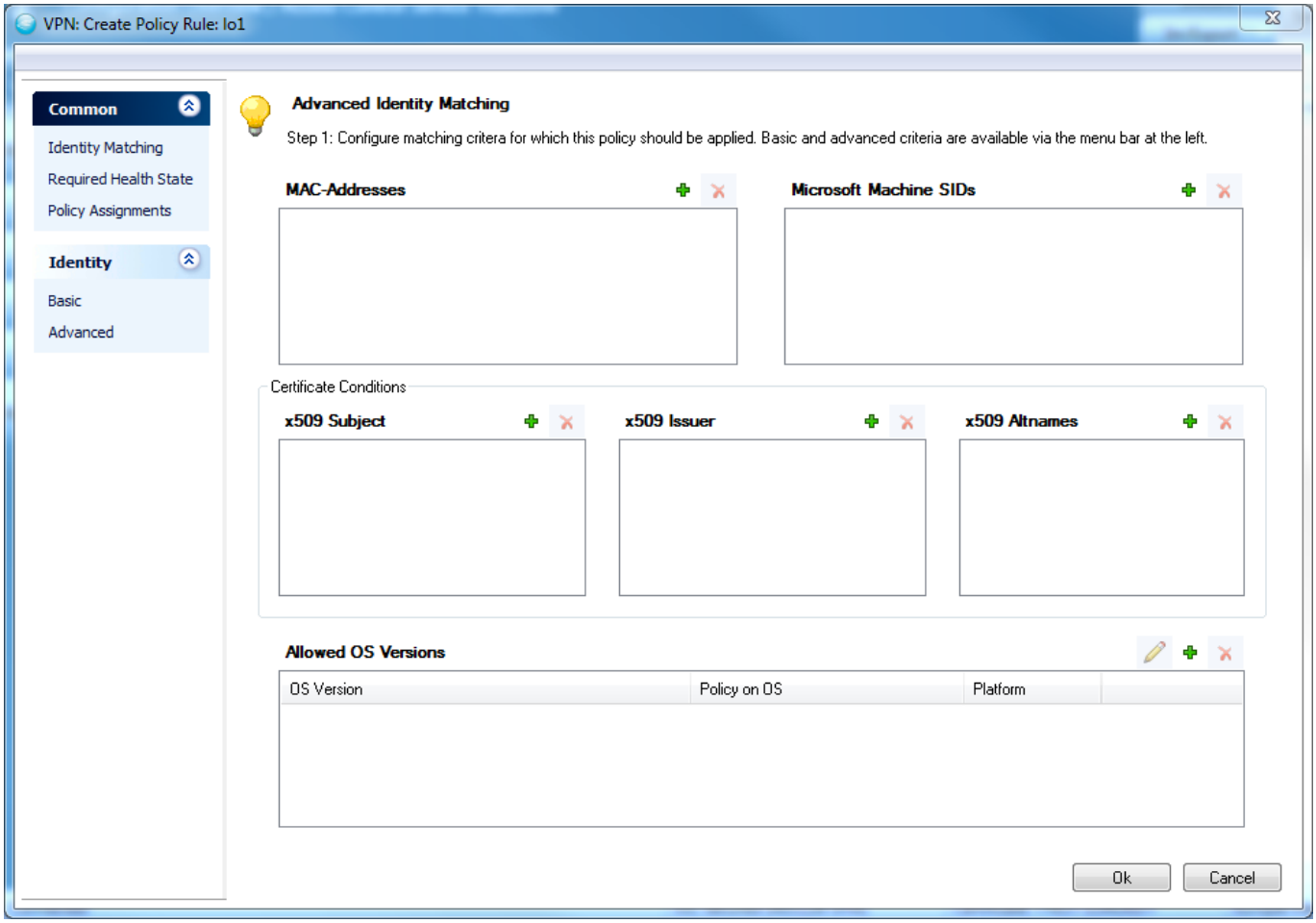


Access Control Service Trustzone > Rules > Identity Matching Basic > Basic Identity Matching	
Policy Name	The name of the policy. This name is visible in the log file and in the access cache.
Deactivate Policy	Disables the configured policy.
Client Connection	• **External** • **Ignore** • **Internal** **External** effects that this policy rule is ignored for internal connection (connections to an IP address not defined in **External IPs**) **Internal** effects that this policy rule is ignored for external connections (connection to an IP address defined in **External IPs**). **Ignore** means that the policy rule is ignored neither for internal nor external connections.

Time Restriction	Each policy rule can be assigned with a date and time restriction. The date restriction consists of a **Start Date** and an **End Date**. Outside that time period, this policy rule will be ignored. The granularity of the time restriction is 1 hour per week? A rule is allowed at all times by default; that is, all check boxes in the **Time Interval** window are cleared. Selecting a check box denies a rule for the given time. Click **the respective icon** to configure allowed and disallowed time intervals simultaneously. Click **the respective icon** to clear selected check boxes. Click **the respective icon** to configure disallowed time intervals. Select **Continue if mismatch** to proceed with the health evaluation process within the policy ruleset of the next rule (default). Select **Block if mismatch** to stop the health evaluation process and set the client to "unhealthy" immediately.
Access Control Service Trustzone > Rules > Identity Matching Basic > Basic Matching	
Policy Matching	• **All-of-following** • **One-of-following** Set this to **All-of-following** if all of the identity matching parameters (basic and advanced), except the empty ones, must match for a successful identity verification. If just one field does not match, the identity is not verified successfully within this policy rule and the health match process will proceed with the next policy rule in the policy ruleset. Set this to **One-of-following** to let the identity verification succeed if just one field matches. Empty fields will be ignored in both cases. String comparison is case insensitive. For the pattern to match, at least one user group must match at least one defined group pattern.
Group Patterns	At least one user group must match at least one of these patterns for successful identity verification. Ensure that you are using the accurate syntax for the group patterns. For example, MSAD groups must be entered as follows: `CN=group-*, OU=my-unit,CD=mycompany,DC=at`
Net Bios Domain	A NetBIOS domain to match only users belonging to a specific domain. This is only available for the **Current User** and **VPN** rulesets.
User [Login Name]	Username patterns consist of the login name (without leading **DOMAIN**).
Networks	The user's peer address must be part of at least one of these networks.

Allowed OS Versions	• **Name** • **OS Versions** • **Service Pack Major Number** • **Service Pack Minor Number** • **Minimum Build Number** • **Policy on OS** Allowed or explicitly denied client OS versions. **OS Versions** must be one of the listed Microsoft Windows Versions. **Service Pack Major Number** and **Service Pack Minor Number** are the service pack numbers of the client OS. **Minimum Build Number** needs to be the OS build number and is checked only if **Policy on OS** is set to **This-One-Or-Newer**. Possible values for **Policy on OS** are: • **Exact-This-One** The client OS must match **OS Versions**, **Service Pack Major Number**, and **Service Pack Minor Number**. • **Explicit-Deny** If the client OS matches **OS Versions**, **Service Pack Major Number**, and **Service Pack Minor Number**, then the current policy rule will be ignored for the current match, and health evaluation processing proceeds with the next policy rule in the policy ruleset. • **This-One-Or-Newer** The client OS must be identically equal to **OS Versions**. The client **Service Pack Major Number** and **Service Pack Minor Number** need to be equal or greater than those defined here.
Hostnames	Enter hostnames here. Patterns may be used.

Identity Matching - Advanced

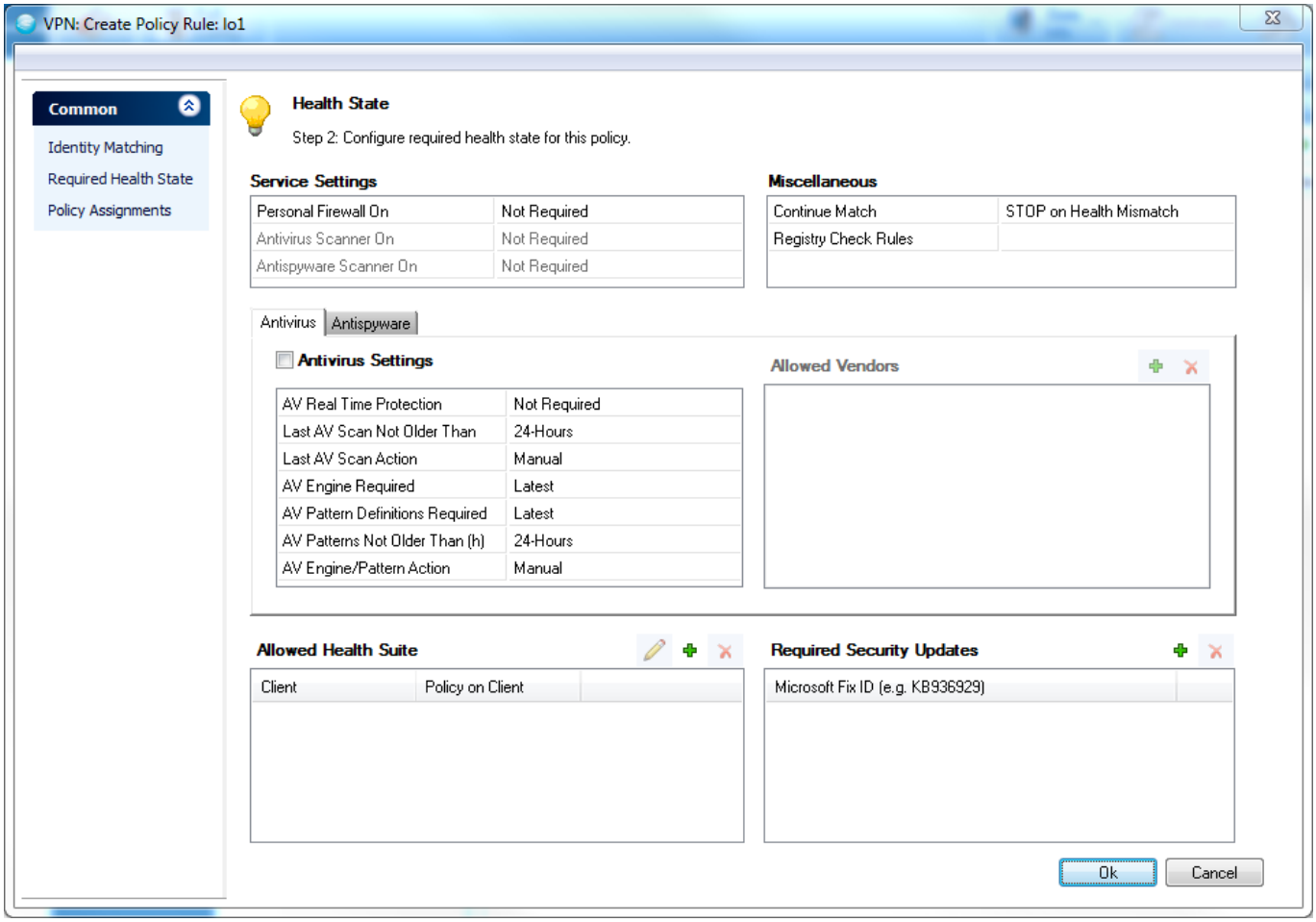


Access Control Service Trustzone > Rules > Identity Matching Advanced > Advanced Identity Matching	
MAC Addresses	Patterns may be used.
Microsoft Machine SIDs	A SID is a globally unique machine identifier generated by Microsoft operating systems. It is visualized in the Access Control Server's access cache. Patterns may be used.

Access Control Service Trustzone > Rules > Identity Matching Advanced > Certificate Conditions	
x509 Subject	The X.509 subject of the client's authentication certificate must match at least one of these patterns. For example: **CN=name-*, O=my-company**. Certificate authentication is only possible in local machine and basic user authentication.
x509 Issuer	The subject of the issuer of the client's certificate must match at least one of these patterns. For example: **CN=name-*, O=my-company**. Certificate authentication is only possible in local machine and basic user authentication.

x509 Altnames	The subject alternative name of the client's authentication certificate must match at least one of these patterns. For example: **IP:10.0.10.***. Certificate authentication is only possible in local machine and basic user authentication. The subject alternative name must be prefixed with its type (for example, **email:** or **IP:**)

Required Health State - Basic



After successful verification of the client's identity, this configuration entity is used for determining the client's health state. Some of the parameters provide the following options:

- **Not required**
  The result of the health evaluation does not depend on this parameter.
- **Required**
  If a **Required** parameter does not match, the user is notified and manual action is required. In addition, the client's health state changes to **Probation**.

Required
Notifies the client as well, but tries to automatically execute the necessary actions to fulfill the health

requirements. During this period, the client's health state changes to **Probation**.

For third-party products (e.g., a Virus Scanner), **Auto-Remediation** may not work with all available engine versions. As a fallback, the client always requests manual action.

Access Control Service Trustzone > Rules > Required Health State Basic > Service Settings	
Personal Firewall On	• **Required** • **Required** • **Not Required** (default) Set to **Required** if a client must have the Personal Firewall up and running to be healthy. If the client does not meet this requirement, the user will be advised to turn on the firewall.
Antivirus Scanner On	• **Required** • **Required** • **Not Required** (default) Set to **Required** if a client must have the Virus Scanner up and running to be healthy. If the client does not meet this requirement, the user will be advised to turn on the Virus Scanner. The **Required** option only takes effect as long as the **Antivirus** check box is activated (see the figure above).
Antispyware Scanner On	• **Required** • **Required** • **Not Required** (default) Set to **Required** if a client must have the Spyware Scanner up and running to be healthy. If the client does not meet this requirement, the user will be advised to turn on the Spyware Scanner. The **Required** option only takes effect as long as the **Antispyware** check box is activated (see the figure above).
Access Control Service Trustzone > Rules > Required Health State Basic > Miscellaneous	
Continue Match	• **STOP on Health Mismatch** (default) • **Continue on Health Mismatch** Set this to **Continue on Health Mismatch** if the health validation should continue with the next policy rule in the policy ruleset in cases where the health evaluation in the current rule stated that the client is **not healthy**. Set this to **STOP on Health Mismatch** if health validation should not continue with the next policy rule in the policy ruleset if the client is **not healthy**. In this case, the policy attributes of the current rule are assigned to the client and the client is advised to heal itself.
Registry Check Rules	Select a registry check object. To be healthy, the client's registry entries must match those of the selected registry check object.
Access Control Service Trustzone > Rules > Required Health State Basic	

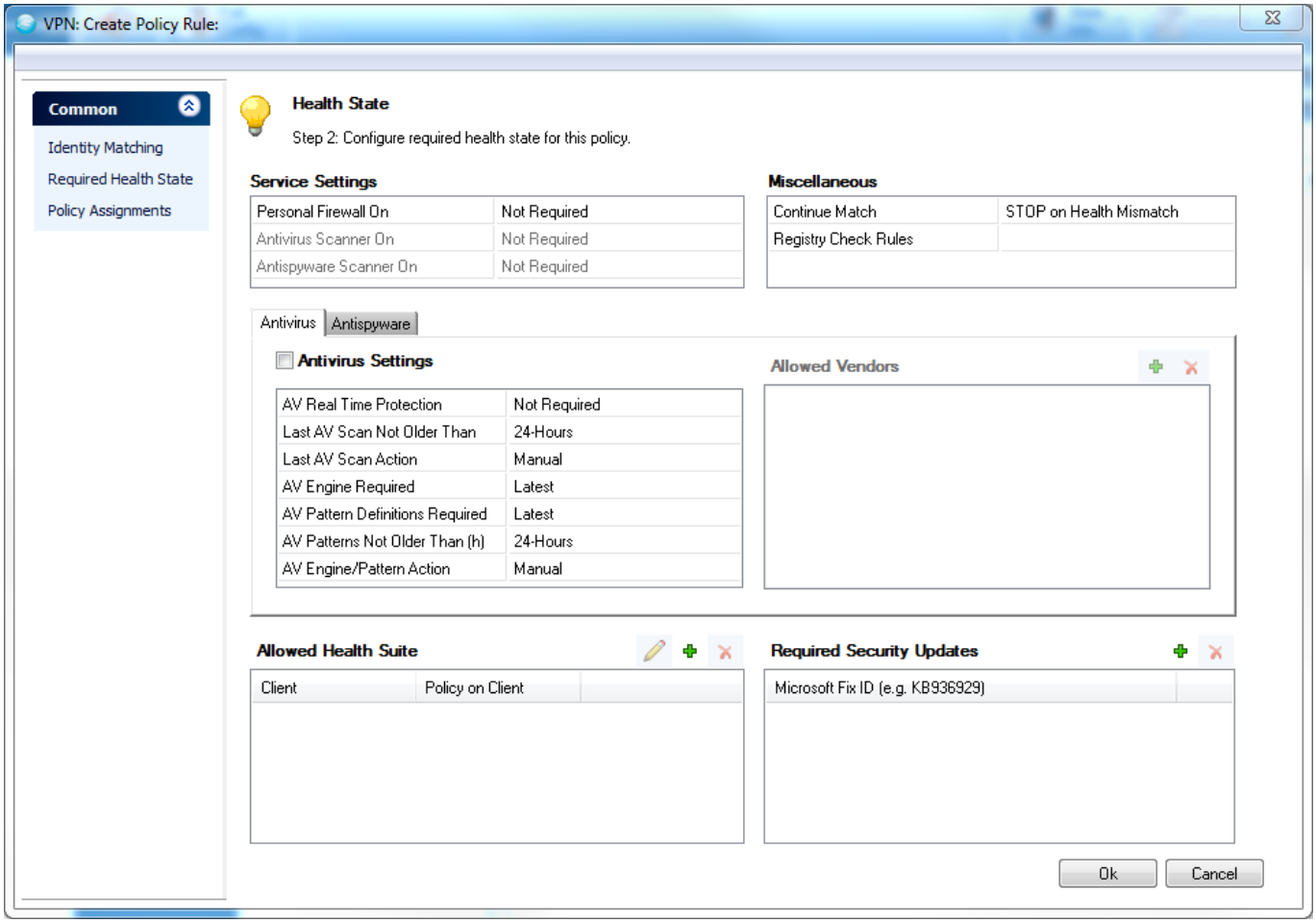
Antivirus	Enable or disable the **Antivirus** settings parameters. For the parameter description, see the next list. Default**: not selected**.
Antispyware	Enable or disable the **Antispyware** settings parameters. For the parameter description, see the next list. Default: **not selected**.

Access Control Service Trustzone > Rules > Required Health State Basic > Antivirus	
AV Real Time Protection	• **Required** • **Required** • **Not Required** (default) Set to **Required** if a client must have enabled the real-time protection of the Virus Scanner to be healthy. If the client does not meet this requirement, it will be advised to turn on the real-time protection of the Virus Scanner.
Last AV Scan Not Older Than	• **Ignore** • **6-Hours > 1-Month** • **24-Hours** (default) Set to a value other than **Ignore** to ensure that the client's last full virus scan is not older than to be healthy. If the client does not meet this requirement, it will be advised to perform a full virus scan.
Last AV Scan Action	• **Manual** • **Auto Remediation** Depending on this parameter, either the user gets informed to manually perform a full virus scan, or the client tries to execute a full system scan automatically.
AV Engine Required	• **Ignore** • **Latest** (default) • **Previous** • **Last-2** Set to **Ignore** if the client's Virus Scanner version should not be checked. Set to **Latest** if the client must not have an older version of the Virus Scanner to return a **healthy** state. Set to **Previous** if the latest and the previous version of the Virus Scanner are accepted to return a **healthy** state. Set to **Last-2** if the latest, the previous, and the second-to-last Virus Scanner versions are accepted to return **a healthy** state. If the client does not meet the chosen requirement, it will be advised to perform a Virus Scanner engine update.
AV Patterns Not Older Than (h)	• **Ignore** • **6-Hours > 1-Month** • **24-Hours** (default) Set this to a value other than **Ignore** to require Virus Scanner patterns to be not older than to be healthy. This value will be ignored if the latest Virus Scanner pattern is older than . For example, if this option is set to **6-Hours** but the latest pattern was released 8 hours ago, the client will be set to **unhealthy** state due to this option. Release cycles of Virus Scanner patterns depend on the Virus Scanner vendor.

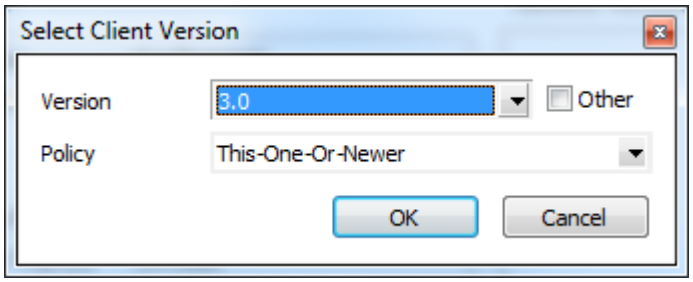
AV Engine/Pattern Action	• **Manual** • **Auto Remediation** Depending on this parameter, either the user gets informed to manually update the AV system, or the client tries to trigger AV updates automatically.
Allowed Vendors	Choose one or more out of this list of Virus Scanner vendors in order to enforce a specific Virus Scanner product to be installed on the client. Virus Scanner products not listed here are ignored in the health validation process. This option is helpful especially to exclude certain Virus Scanner products from the health validation process. The list of available Virus Scanner vendors is created dynamically.
Access Control Service Trustzone > Rules > Required Health State Basic > Antispyware	
AS Real Time Protection	• **Required** • **Required** • **Not Required** (default) Set to **Required** if a client must have enabled the real-time protection of the Spyware Scanner to be healthy. If the client does not meet this requirement, it will be advised to turn on the real-time protection of the Spyware Scanner.
Last AS Scan Action	• **Manual** • **Auto Remediation** Depending on this, the user either gets informed to manually perform a full spyware scan, or the client tries to execute a full system scan automatically.
Last AS Scan Not Older Than	• **Ignore** • **6-Hours > 1-Month** • **24-Hours** (default) Set to a value other than **Ignore** to ensure that the client's last full spyware scan is not older than for validly returning the **healthy** state. If the client does not meet this requirement, it will be advised to perform a full spyware scan.
AS Engine Required	• **Ignore** • Latest (default) • **Previous** • **Last-2** Set to **Ignore** if the client's anti-spyware engine version should not be checked. Set to **Latest** if the client must not have an older version of the Spyware Scanner engine to validly return the **healthy** state. Set to **Previous** if the latest and the previous version of the Spyware Scanner engine can validly return the **healthy** state. Set to **Last-2** if the latest, the previous, and the second-to-last Spyware Scanner engine versions are allowed to validly return the **healthy** state. If the client does not meet the chosen requirement, it will be advised to perform a Spyware Scanner engine update.

AS Pattern Definitions Required	• **Ignore** • **Latest** (default) • **Previous** • **Last-2** Set to **Ignore** if the client's spyware pattern definitions should not be verified. Be aware that, in this case, the client may be healthy without having any spyware patterns installed. Set to **Latest** if the client's spyware patterns must be up-to-date to validly return the **healthy** state. Set to **Previous** if the client's spyware patterns must either be up-to-date or of the previous version to validly return the **healthy** state. Set to **Last-2** if the client's spyware patterns must either be up-to-date or of the previous or the second-to-last versions to validly return the **healthy** state. If the client does not meet the chosen requirement, it will be advised to perform a spyware patterns update.
AS Patterns Not Older Than (h)	• **Ignore** • **6-Hours > 1-Month** • **24-Hours** (default) Set this to a value other than **Ignore** to require spyware patterns to be not older than to validly return the **healthy** state. The setting will be ignored if the latest spyware pattern is older than . For instance, if the value is set to **6-Hours** but the latest spyware pattern was released 8 hours ago, the client will be set to the **unhealthy** state due to this setting. Release cycles of spyware patterns depend on the Spyware Scanner product vendor.
AV Engine/Pattern Action	• **Manual** • **Auto Remediation** Depending on this setting, the user either gets informed to manually update the Spyware Scanner, or the client tries to trigger such an update automatically.
Allowed Vendors	Choose one or multiple entries from the list of Spyware Scanner vendors in order to enforce specific Spyware Scanner vendor products to be installed on the client. Spyware Scanner products not listed here are ignored during the health validation process. This setting is helpful especially for excluding certain Spyware Scanner products from the health validation process. The list of available Spyware Scanner vendors is dynamically created.

Required Health State > Advanced Health State



Select **New** from the context menu to create a new entry. The configuration dialog provides the following entries:



Access Control Service Trustzone > Rules > Required Health State > Advanced > Allowed Health Suite Versions	
Name	Specify a name.
Major Release	The client's health suite major release version number must match **Major Release**.
Minor Release	The client's health suite minor release version number must match **Minor Release**.

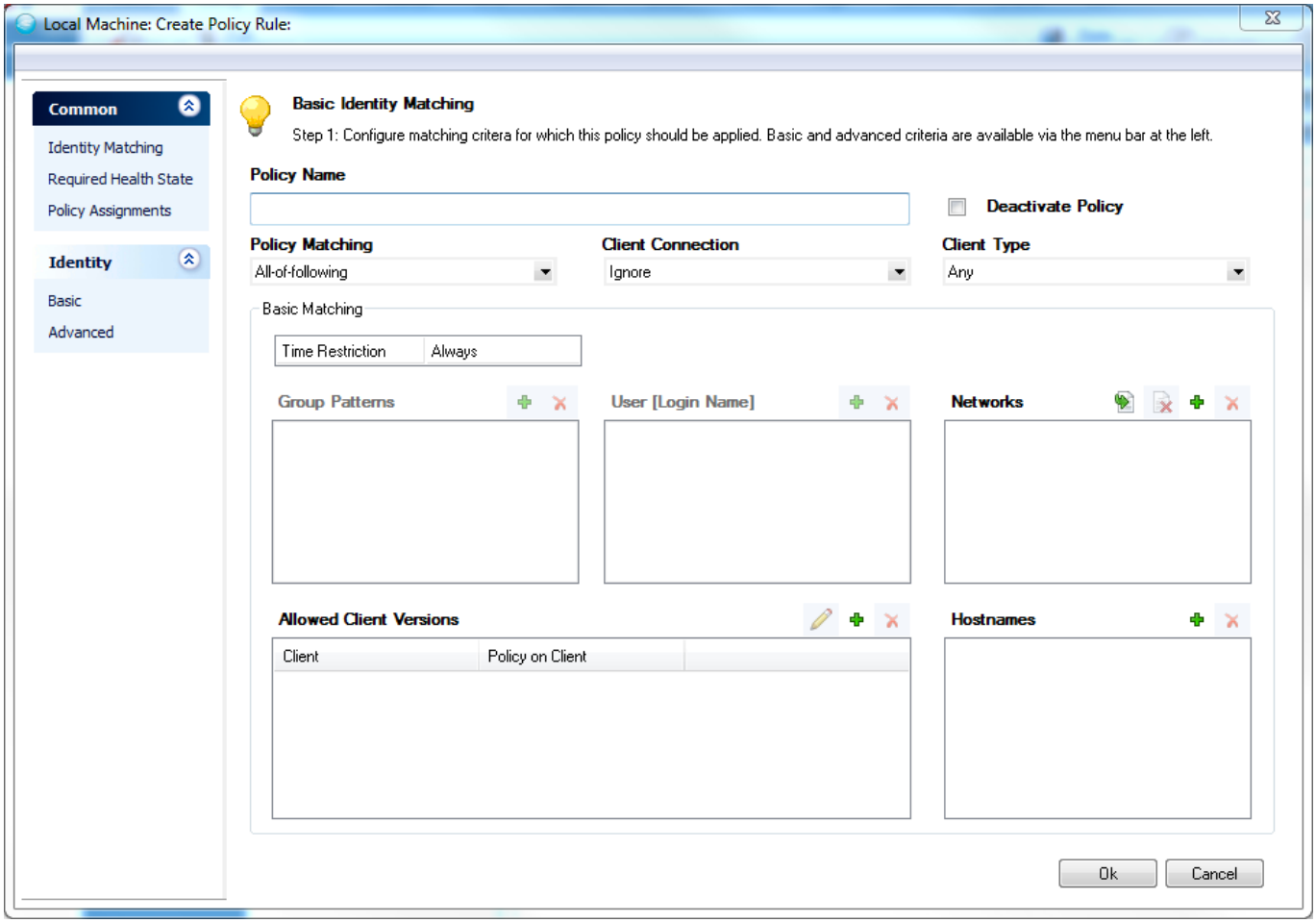
Service Pack Number	The **Service Pack Number** must match the service pack number of the client's health suite.
Policy on OS	• **Exact-This-On** The client's health suite version must match all three number values. • **Explicit-Deny** If the client's health suite version matches all three number values, the health state will be set to a value different than **healthy** and the clients will be advised to update the health suite. • **This-One-Or-Newer** The client's health suite major version must equal **Major Version**. The minor release version number and the service pack number need to be equal or greater than those defined here.

Health suite updates are always performed on an equal major release version number. For instance, a client's health suite version 4.0.2 can be updated to 4.1.0 but not to 5.0.0.

It is also possible to include a validation of the currently installed Microsoft hotfixes on the client computer:

1. Right-click into the **Required Security Updates** field
2. Click **New...**, then enter the ID of the Microsoft hotfix. For example: **KB936929.**

Policy Assignments

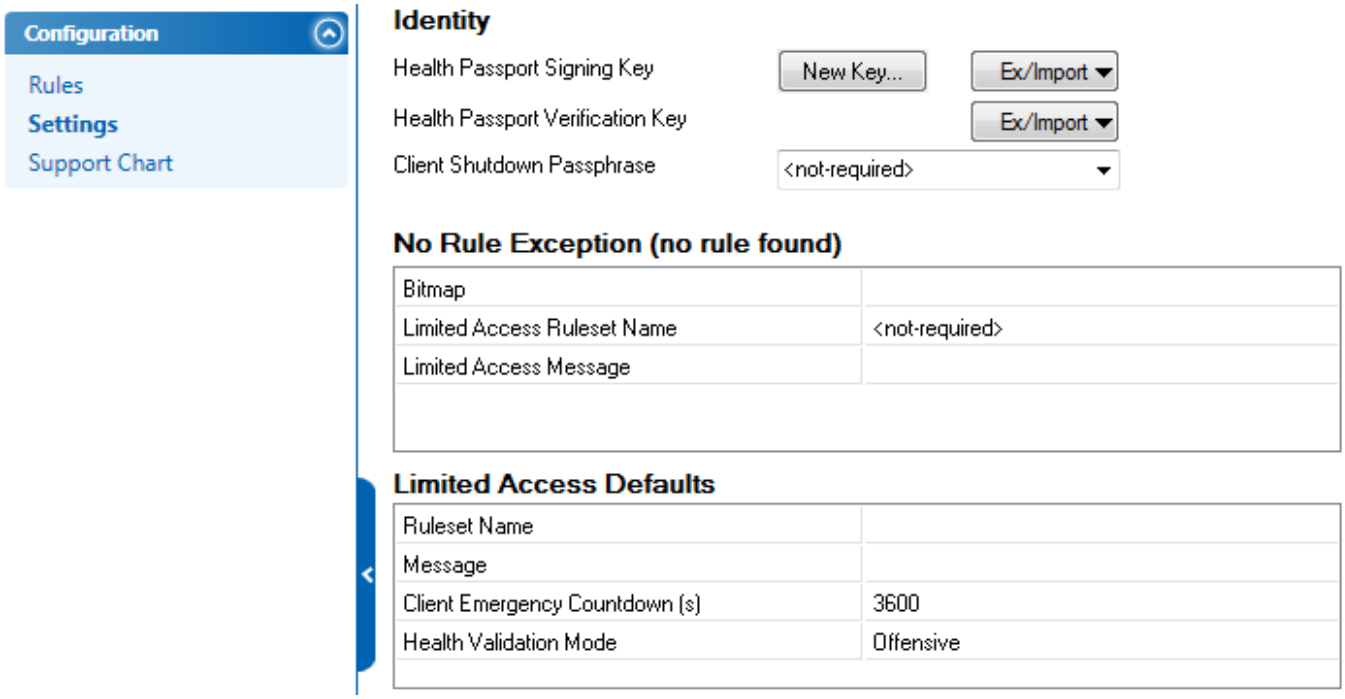


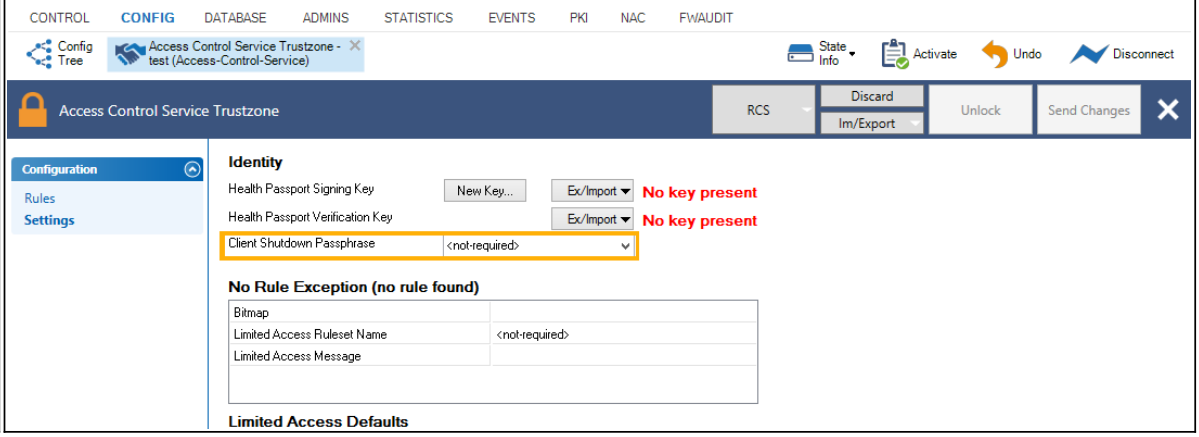
Access Control Service Trustzone > Rules > Policy Assignments > Attributes	
Personal Firewall Settings	• **Ruleset Name** Select one of the created **Personal Firewall Rule** objects. If the client does not already have this ruleset installed, the health state will be set to a value other than **healthy** and the client will be advised to update the personal firewall rule set from the remediation server.
Message of the Day	Select one of the created **Welcome Message** objects. If the client does not already have this message, it will be advised to get the message from the remediation server.
Limit Access	• **Ruleset Name** • **Message** • **Client Emerg. Quarantine Time (s)** Configure the quarantine ruleset. Assignment of **Limited Access** rulesets and messages is only available for the **Local Machine** ruleset. The quarantine ruleset (**Limited Access**) is stored on the local machine. This means that the quarantine ruleset can only be updated if the current user logs off or the client is rebooted. If a client changes its state to **unhealthy,** the local machine quarantine ruleset is activated.
Access Control Service Trustzone > Rules > Policy Assignments > Exceptions	

Software Update Required	• **Yes** • **No** (default) • **Yes-Even-Major** Change this to **Yes** for the client to automatically perform software updates if a new software minor version is available on the CC. **Yes-Even-Major** will cause the client to also perform major version updates.
User Authentication Required	• **Yes** • **No** • **Like Service Settings** (default) Only available for the local machine ruleset. If this is set to **No**, user authentication is not performed even if a user logs in.
Access Control Service Trustzone > Rules > Policy Assignments > Radius Attributes	
Healthy Attribute Assignments	RADIUS attribute assignments passed to a RADIUS server as key-and-value pairs if the client meets the health requirements.
Unhealthy Attribute Assignments	RADIUS attribute assignments passed to a RADIUS server as key-and-value pairs if the client does not meet the health requirements.

Settings

If no policy rule matched the identity for a client, or at least one matched but the **Continue Match** parameter was set on that/those policy rule(s), the client's state will be **untrusted** and it will be assigned the **No Rule Exception** attributes.



Access Control Service Trustzone > Settings > Identity	
Health Passport Signing Key	The RSA key for digital passport signing. The Health Validator returns a digital passport to the client as result of the health validation. The passport contains all information required for the remediation server. To ensure authenticity, the passport is digitally signed. Since all Access Control services of the same trustzone share the same credentials, the remediation server instances can verify whether a passport was issued by a health validator of the same trustzone.
Health Passport Verification Key	The RSA public key for verifying a digital passport signature. If one Access Control Server instance acts exclusively as a remediation server, it is not necessary to set the **Health Passport Signing Key.** However, the **Health Passport Verification Key** must be set.
Client Shutdown Passphrase	If a passphrase is set here, the Access Control service will lock the **Advanced Settings** locally on the clients unless the local user enters the correct passphrase. In addition, the client can only be terminated on the workstation after the passphrase has been entered. The default setting disables these restrictions and enables the local user to administer and terminate the client. 
Access Control Service Trustzone > Settings > No Rule Exception	

Bitmap	Select one of the **Picture** objects. The client will then be advised to get the respective bitmap from the remediation server.
Limited Access Ruleset Name	For more information on these two parameters, see Limit Access.
Limited Access Message	
Access Control Service Trustzone > Settings > Limited Access Defaults	
Client Emergency Quarantine Time (s)	If the Access Control Server is not reachable anymore for the client, it switches automatically to the **Unhealthy r**estricted state. Entering a value of **0** disables this. For more information, see Limit Access. If no Access Control Server IP address is available, this parameter does not have any effect. For more information, see The Barracuda Access Monitor, **Access Control Server IPs from Registry** and **Access Control Server IPs from DHCP** sections.
Quarantine Ruleset Name	Select one of the **Personal Firewall Rules** objects. The client will be advised to get the respective bitmap from the remediation server.
Quarantine Message	Select one of the **Welcome Messages** objects. The client will be advised to get the respective bitmap from the remediation server.
Health Validation Mode	• **Moderate** Health checks are executed after connection establishment. • **Offensive** Health checks are executed during connection establishment.

The **Health Validation Mode** parameter can also be configured on the client via the following registry key:

Path	`.DEFAULT\Software\Phion\phionha\settings\`
Key	SpeedVPNValidation
Value	• Moderate • Offensive

The **Client Emergency Quarantine Time (s)** parameter can also be configured on the client using the following registry key:

Path	`.DEFAULT\Software\Phion\phionha\settings\`
Key	QuarantineCountDown
Value	[Default: **3600000** (= 1 hour in milliseconds)]

Access Control Service Trustzone > Settings > Radius Attribute Assignments	
With this feature, it is possible to send additional attributes to the switch, depending on the health state of the client. **VLAN Change** attributes are already hardcoded.	
Healthy	For a description of these two parameters, see the radatt.
Unhealthy	

Support Chart

This view provides information concerning the supported Virus Scanner and Spyware Scanner vendors and versions.

The **Support Chart** is automatically downloaded from the Barracuda Networks update service and distributed to Barracuda NextGen Admin upon connecting. Thus, the **Support Chart** reflects the current capabilities of the Access Control service.

The following restrictions appear on Microsoft Windows Vista and Windows 7 64-bit:

The supported features listed in the support chart may differ from the technically executed actions. For example, regarding automatic updating of Windows Defender 1.x, the chart states **Implemented** although it may not work on the 64-bit client. The reason is that the released version of the 64-bit client contains a 32-bit compatible COM+ server for integrated OPSWAT modules (health check). Therefore, this component is not yet implemented as native 64-bit.

This leads to some restrictions regarding auto-remediation features of the health agent system:

- Enabling and disabling of Virus and Spyware Scanner functionality cannot be done automatically for some vendors (see support charts).
- Auto-remediation for Virus Scanner and Spyware Scanner engine and pattern updates is disabled in the 64-bit client.

Figures

1. ac1.png
2. image2012-11-13 15-46-26.png
3. image2012-11-13 15-44-0.png
4. image2012-11-13 15-42-13.png
5. image2012-11-13 15-41-32.png
6. image2012-11-13 15-37-11.png
7. image2012-11-13 15-39-22.png
8. image2012-11-13 15-35-2.png
9. image2012-11-13 15-29-15.png
10. ac2.png