How to Configure the Access Control Service

https://campus.barracuda.com/doc/98220204/

The Access Control service defines security policies for network users (e.g., VPN clients) and enables the CloudGen Firewall to perform identity and health checks on clients. For this feature, the Barracuda CloudGen Firewall includes an automatic software downloader which periodically connects to the Barracuda Networks website. To reduce the need for permanent Internet connection for Barracuda CloudGen Firewalls, the Barracuda Networks update service behaves differently on stand-alone boxes than on CC administered boxes. Internet access using an HTTP/HTTPS proxy server is possible.

- Stand-alone boxes running an Access Control Service require Internet access.
- CC-administered boxes running an Access Control Service get the required files uploaded from the Barracuda Firewall Control Center. The CC itself requires Internet access to **secure.phion.com:443**.

Configure the Access Control Service

1. Create an Access Control Service. For more information, see How to Assign Services.
2. Go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > Access Control Service**.
3. Configure the Access Control Service settings as described in the following sections.
4. Click **Send Changes** and **Activate**.

Access Control Service Settings

This section defines the general parameters of the Access Control Service.

System Health Validator

Trust Zone / General	
Name	On a Barracuda Firewall Control Center, this parameter allows referencing to global trustzone objects. An empty value indicates that the local trustzone configuration (for example, only this Access Control Service should use the configured trustzone) should be used. For more information, see Configuring Access Control Service Trustzones.
Start System Health-Validator	Setting to **yes** will cause starting of the Access Control Server module for authentication before VPN health validation occurs.
Start VPN Health-Validator	Setting to **yes** will cause starting of the Access Control Service module for VPN health state evaluation.

External IPs	This option defines service IP addresses as external IP addresses. This information may be used in policy rules for health evaluation to distinguish between external and internal requests.
Health State Validation Cycle	
Healthy (min.)	This value restricts validity time of authentication. If the client does not re-evaluate its health state within that period, all assigned **network access rights** will be dropped.
Probation/Limited Access (min.)	This value defines the probation interval of a health validation. If a client does not satisfy the health requirements in an initial health validation step, the client will be set into probation. It will get the special network access right **probation**, additionally to the rights as it was healthy. If the client doesn't become healthy within the probation time it will be set to health state "unhealthy" automatically after the probation time was elapsed.

The **Health Validation Mode** parameter, to be configured in Barracuda Firewall Admin within the **Access Control Server Trustzones (VPN only)** settings screen, may also be modified on the client using the following registry key:

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

User Authentication	
User Authentication Required	If this option is set to **no**, the client will not re-evaluate its health state when a user logs on. For example, no **current user** health evaluation will take place.
Authentication Scheme	The used phibs scheme for basic authentication.
Fallback Authentication Scheme	This option is only available if **Authentication Scheme** was set to **MSCHAP**. In this case, this scheme is used for authentication if the MS-CHAP authentication fails. The client will display a pop-up requesting username and password.
Local Machine Authentication	
Certificate Required	If set to **yes**, a local machine authentication requires a certificate for a successful local machine authentication. Do not forget to set an accurate search string for box certificates since there is no default box certificate that could be used for authentication. The client needs to know which certificate from the local certificate store should be used for health evaluation.
Search String Type	May be set to either **Issuer** or **Subject**. This setting defines how the search string for box certificates is interpreted.
Search String for Box Certificates	Either a X.509 issuer string or a X.509 subject string (e.g. **C=AT, O=Barracuda, OU=*,CN=***). Pattern matching is allowed.

General Authentication	
Authentication Root Certificate / Explicit Authentication Root Certificate	The root certificate is used to verify the validity of certificates provided by clients within a local computer health validation process.
Root Cert. Revocation Settings	This section provides configuration settings for certificate revocation. Certificate revocation can be done by using either CRL (LDAP) or OCSP. Click **Set/Edit** to configure the settings.

Referrals	
Remediation Server Location	This defines where the remediation server can be reached. Select **This**, if the remediation server is running on the same system as the Access Control Server. In this case, **Start Remediation Server** must be set to **yes**. Select **Other** in case it is running on a different system, and specify the remediation server IP addresses in the fields below.
Internal Remediation Server IPs	IP address(es) of the remediation servers accessible by clients within the secure network.
External Remediation Server IPs	IP address(es) of the remediation servers accessible by clients within the restricted network.
VPN Remediation Service IPs	The IP address(es) for the Access Control Service remediation service module for VPN clients. This IP address must not be identical with the internal or external remediation service's IP address. **Example:** For the internal clients, the Access Control Service listening socket is on **10.0.8.108** and you also want to have a remediation service for clients connected via VPN: • Introduce an additional IP address, for example **10.0.8.150** on the virtual server layer, and insert these two bind IP addresses (**10.0.8.108** and **10.0.8.150**) in the Access Control Service configuration. • Now open the Access Control Service settings, scroll down to the VPN Remediation Service IP addresses and select the IP Address **10.0.8.150** from the dropdown menu.
Sync authentication to Trustzone	Using a Barracuda Firewall Control Center, multiple Access Control Services can reference to the same trustzone. Already validated clients can be propagated to all Access Control Services sharing the same trustzone configuration. This also affects gateway firewall authentication. This parameter is only available on a CC.

Remediation Service

Access Control Server > Access Control Server Settings > Remediation Server > General	
Start Remediation Service	Setting this to **yes** starts the Access Control Server remediation service module.

TLS required	Setting this to **yes** will allow unencrypted downloads from the remediation server. This will increase download velocity, however, it will also decrease the security because Personal Firewall rule sets are transmitted unencrypted over the network.

Trustzone-Border

General	
Start Border Health-Validator	Starts the Access Control Service module responsible for trustzone border health state evaluation.
Trustzone Border IP	IP address the health validator uses for listening for trustzone border health validations.
Foreign Health Passp. Verification	Add all foreign health passport verification keys here of which health passports should be trusted for this border trustzone. The health state of clients with a signed and trusted health passport is revalidated for this trustzone, however, their authentication credentials are accepted from the signed cookie.
Allowed Peer Networks	Only peers from listed networks are allowed to perform trustzone border health validations.

Advanced

General	
Log Level	This option defines the verbosity of log file output. Usually it should be set to **0** (that is **no debug output**). Higher values provide more detailed log information.
Number of used Threads	Number of used worker threads for health validation and remediation. The default value is **5**. This should meet the requirements in most cases. Increasing this value leads to a more reactive server, but also increases the load on the system.
Keep Access Cache Entries (d)	Amount of days for which access cache entries generated by activities traversing the Access Control Server should be deleted.
Keep Max. Access Cache Entries	Maximum number of access cache entries to keep.
Sync Access Cache to CC	By enabling this, the access cache entries of this Access Control Service are synced to the Barracuda Firewall Control Center. Thus, a consolidated health status of multiple Access Control Services will be available. Additionally, the appropriate Barracuda Network Access Client service must be introduced on the CC. Use with care in case of limited bandwidth as the synchronisation consumes additional bandwidth. The parameter is only available in conjunction with a Barracuda Firewall Control Center.
Sync to HA	Enable / disable HA synchronization.
Resource Cleanup Policy	Enforce a strict resource cleanup policy in case of an overload on the service.

TLS/SSL	
TLS/SSL Private Key	Corresponding RSA private key to be used with TLS.
Explicit TLS/SSL Certificate	The X.509 certificate to be used with TLS.