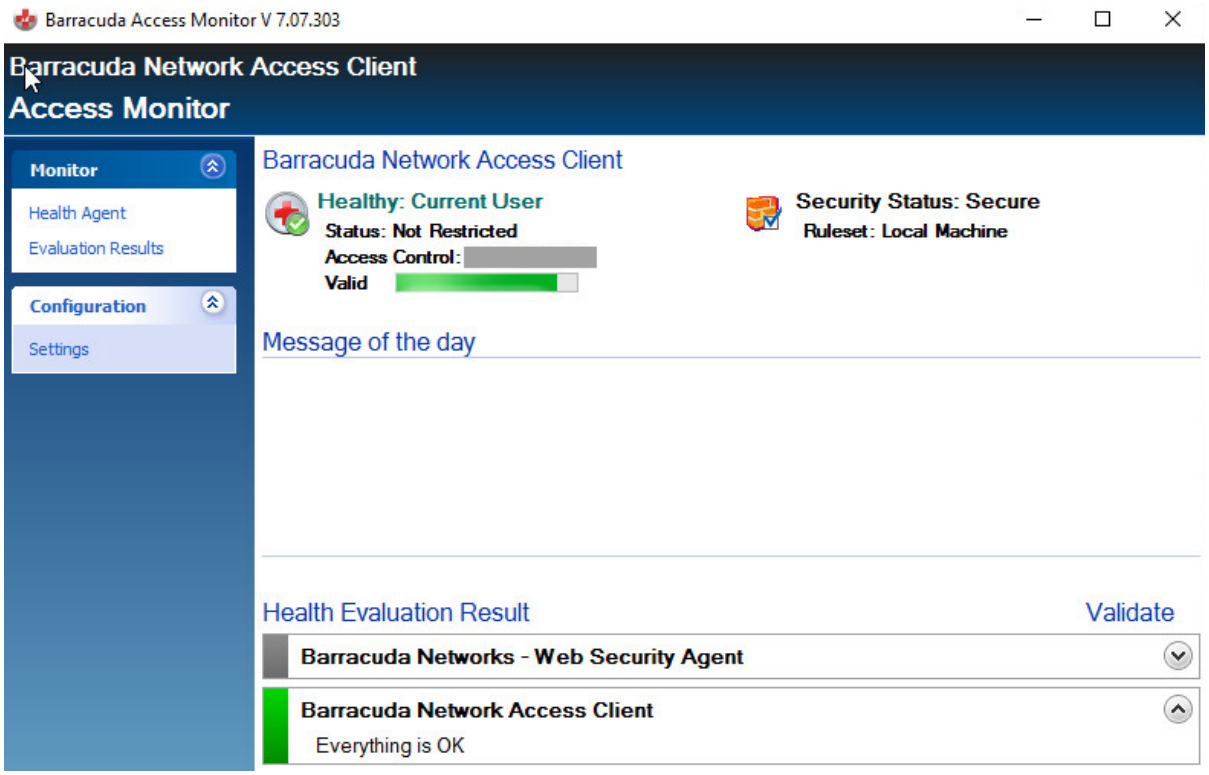
# How to Use the Barracuda Access Monitor

https://campus.barracuda.com/doc/46206577/

The Barracuda Access Monitor communicates with the Access Control Server and provides all necessary information regarding the client computer's health state and network restrictions. The Access Monitor collects information from the client, including workstation identity, operating system, and patch-level antivirus and anti-spyware, and takes security measures depending on the health evaluation result returned by the Access Control Server. Such sescurity measures include downloading and installing necessary updates, restricting network access, executing antivirus or anti-spyware updates, and starting scans or updates.

## The Health Agent Window

Launch the Barracuda Access Monitor by left-clicking the red cross icon in the system tray. The Access Monitor opens in the **Health Agent** view:




Whenever the Barracuda Access Monitor is working, a status message is displayed in the **Message of the Day** section. If either the Client service or the Barracuda Access Monitor Agent service (both of which are vital for normal operation) are not running, red warning messages will be shown for either of them. No message indicates that both services are operating normally.

## Communication Status

The following communication states exist for the Barracuda Access Monitor:

- **Initializing** – The Barracuda Access Monitor is initializing before entering operational state.
- **Termination** – The Barracuda Access Monitor service is shutting down and freeing all resources.
- **Pending communication, validating** – A health evaluation has been started; now, the client is waiting for the result from the Access Control Server.
- **Pending communication, downloading** – Files such as rulesets, patches, and other data necessary to comply with the matching policy are being downloaded.
- **Waiting for user input** – The Barracuda Access Monitor requires user credentials for user-specific authentication and health evaluation. Whenever this message is shown, a dialog is visible to enter the user credentials.

While the Barracuda Access Monitor is communicating, it is not possible to start a health evaluation.

If, for any reason, the Access Control Server cannot be reached at the IP addresses configured for health evaluation, a connection error will be shown. See the **ICMP Connectivity Checking** section in How to Configure the Barracuda Access Monitor for more details on this specific connection error. For more information, see Troubleshooting.

## Health Monitoring

The **Health Agent** window provides the following information:

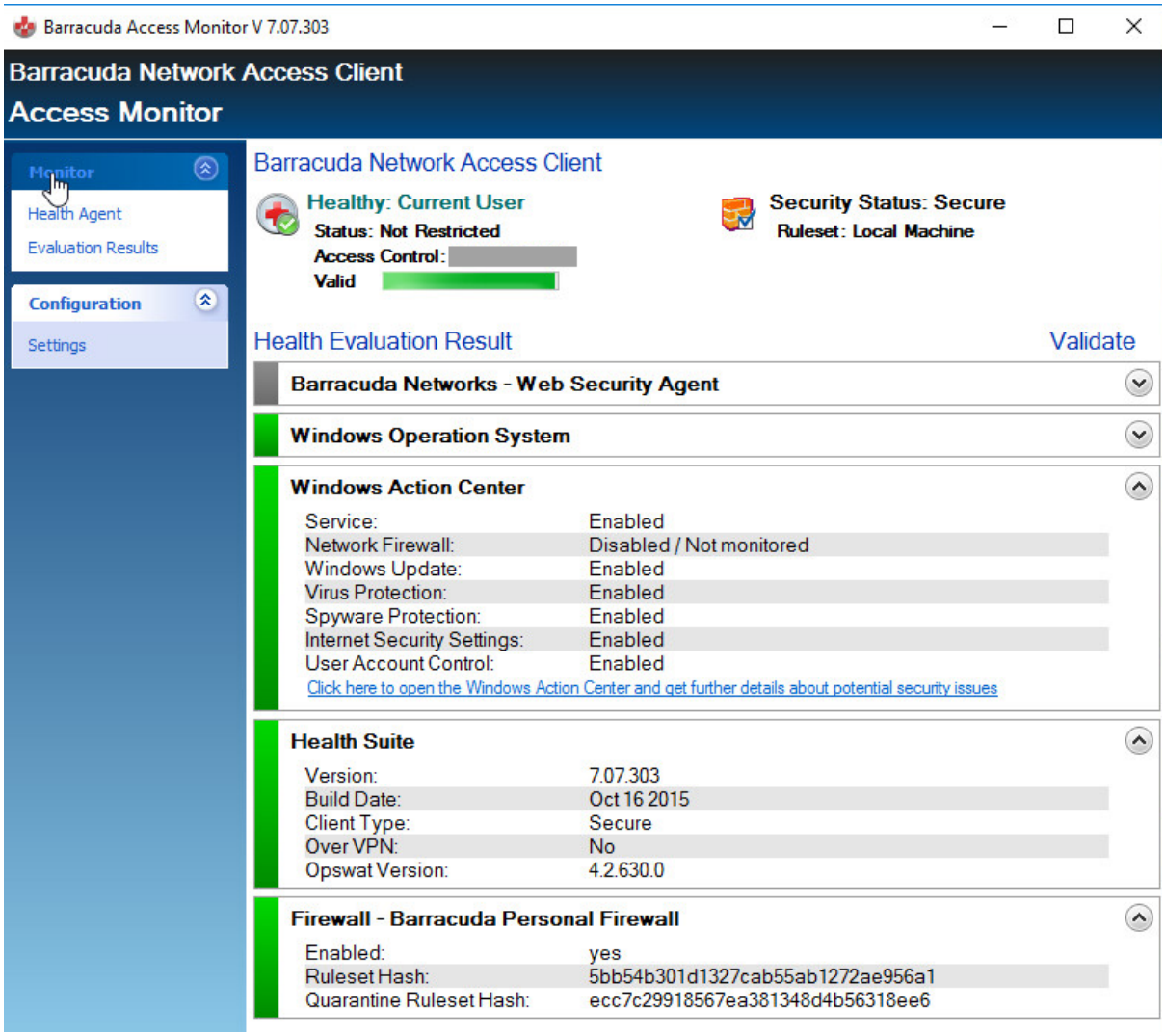
- **Health Condition** – There are 3 different health states:
  - **Healthy** – The client computer complies with the policy configured on the Access Control Server.
  - **Unhealthy** – The client computer does not comply with the policy; actions need to be taken to meet the health requirements.
  - **Untrusted** – There is no rule defined for the client computer, so the client has only restricted network access.
- **Client Origin** – Indicates the orgin of the client sytem:
  - **Local Computer** – Health evaluation for the client computer is mandatory. If the health evaluation for the client computer is not successful, an evaluation based on user credentials is not possible.
  - **Current User** – When multiple users use the same computer, it is possible to start health evaluation based on user credentials, matching each user with the user's individual policy depending on their role in the network.

    - **VPN** – The client is connected to the Access Control Server using a VPN connection.
- **Security Status** – Displays the status of the Barracuda Personal Firewall and the ruleset.
- **Quarantine Status** – The quarantine status depends on the health condition of the client computer. The following three states are provided for policy-based network access:
    - **Not Restricted** – Full network access is granted if the health evaluation result returns a health state of **Healthy**.
    - **Probation** – If the client computer does not meet the configured health requirements, it will enter probation state. In this state, the client is not restricted, so it can contact network resources necessary to meet all health requirements. If the subsequent health evaluation does not return a **Healthy** state, the client will enter restricted network access mode.
    - **Restricted** – If restricted network access is active, the client will activate the quarantine ruleset assigned by the Access Control Server. You can configure two quarantine rulesets, one for when the client computer does not meet the health requirements and is unhealthy, the other for when the client computer is untrusted because no rule is defined for it.
- **Access Control Server** – IP address or hostname of the Access Control Server to be contacted for health evaluation.
- **Message of the day** – Custom welcome message supporting Unicode, configurable on the Access Control Server for following states:
    - **Local Computer** – healthy, limited access
    - **Current User** – healthy
    - **VPN** – healthy, limited access
- **Health Evaluation Result** – Shows the actual health evaluation result. If a criterion does not meet the requirements, a description of necessary actions in order to comply with the policy is shown.

To start a health evaluation manually, click **Validate**.

## The Evaluation Results Window

To view detailed information on health evaluation results, select **Evaluation Results** in the **Monitor** menu on the left.




Depending on configuration and policies, the following details are displayed:

- **Barracuda Web Security Agent** – If installed and configured, this section provides information about the Barracuda Web Security Agent. For more information, see Overview.
- **Windows Operating System** – Shows the Windows version of the client and provides collected information about user, host, and domain.
- **Windows Action Center** – Provides information about Windows updates, security, and virus protection as required in the Access Control Service policy.
- **Health Suite** – Shows the version and type of the health suite that applies to the client.
- **Firewall - Barracuda Personal Firewall** – Shows if the Personal Firewall is enabled and displays the ruleset hash key.

## Advanced Settings

To configure advanced Barracuda Access Monitor settings, open the **Configuration > Settings** menu. For more information, see How to Configure the Barracuda Access Monitor. The **Log Files** section displays log files created by the Barracuda Network Access Client. For information on available logging options, see How to Configure the Barracuda Access Monitor and Network Access Client Logging.

## Figures

1. access_monitor_launch.png
2. access_monitor.png