

AppGate Client Check feature

Using the AppGate Client Check feature

For a system administrator a connecting PC is always a potential threat to the security of the network. It is therefore important to secure the integrity of the PC. The AppGate server asks the PC to run a certain command, which is first downloaded from the AppGate server, to scan the system. Usually this function is used to check antivirus versions or in other ways check that the PC is a corporate PC. Of course the results of these scans can be a part of the access rule set.

When it's useful

The Client Check should be viewed as a feature that can help the user in keeping the client computer in line with the security policy.

Example of usage:

- Verification of correct Anti Virus software and updates.
- Verification of OS updates and patch levels.
- Differentiating between corporate PCs, e.g company Lap tops, and private PCs, e.g. home users.

How it works

Technically it is a framework that allows the AppGate Security Server to verify the state of the client and as such it has to be adapted fit each specific security policy.

The Client Check verification is done after authentication but before the authorization. The result of this verification can then be a factor in the subsequent authorization decision.

The log-on process is done in three steps:

1. User authentication
2. Client Check
3. Authorization

As an example, it may be possible to verify that the client is a corporate lap top of a certain kind, perhaps by checking the Ethernet mac addresses, and that it also has the latest anti virus software version properly installed. A positive result of such a verification can then be used to grant the user access to certain sensitive application servers.

If the verification fails it may still be possible to allow access to other less sensitive servers.

Implementation

In practice the Client Check feature is using a program stored on the AppGate Security Server. This program is downloaded to the client during the log-on process and is launched by the AppGate Client. The resulting output of the execution is passed back to the AppGate Security Server and is fed as input to the authorization mechanism.

The program is a binary or any natively executable for the client platform in question. AppGate provides a contributed example binary for the Windows platform that can be used to check a few common but simple things on the client. This program can do the following:

- Check that a certain file exists
- Check that a registry entry exists or has a specific value.
- Check that a specific process runs.

Conclusion

The client machine is a piece of hardware of which we have no physical control. It is by nature outside our data center and in the hand of a user.

In large we have to put trust in the user to keep the client in a secure state. However even if we trust the intentions of the user there is always the risk of the human factor - the risk that the user unintentionally is compromising the security.

Checking the state on the client computer can help the users maintain the the desired security level. All in all, this can lead to an improvement of the total security level for the whole infrastructure.