



McAfee Application Control for PCs ("ACD")

ACD-5.x

Quickstart Scope Definition Guidelines

McAfee Application Control ("ACD") gives enterprises an effective way to block unauthorized applications on servers and endpoints. Unlike simple whitelisting, Application Control uses a dynamic trust model, which eliminates the need for tedious manual updates to approved lists. As enterprises face an avalanche of unknown software from the web, this centrally managed solution adds a timely control to any systems security strategy, one attuned to the operational needs of enterprises. Get the appropriate service type below to ensure it is implemented and configured fast, cost-effectively and securely.

New Installation: 1 X MD-QS-SMB-4HR*

A McAfee Subject Matter Expert ("SME") will remotely configure and deploy ACD based on McAfee's Best Practices.

- o Review server and software requirements
- o Install and Configure ACD from the ePO Server:
 - Install the ACD Extension
 - Install License
 - Add the ACD deployment package to the ePO Repository
 - Deploy and enable the ACD Agent to endpoints (up to 5)*
 - Create ACD policies based on your environment (up to 5)*
- o Test the ACD policies to verify they are working properly.

Upgrading: 1 X MD-QS-SMB-4HR*

McAfee's SME will perform the following tasks:

- o Review server and software requirements
- o Upgrade and Configure ACD from the ePO Server:
 - Export current ACD policies
 - Install the latest ACD extension
 - Update the ACD license
 - Add the latest ACD deployment package to the ePO Repository
 - Install and enable the new ACD Agent on endpoints (up to 5)*
 - Import and Modify ACD policies (up to 5)*
- o Test the ACD policies to verify proper operation.

Optimization: 1 X MD-QS-SMB-4HR*

McAfee's SME will perform the following tasks:

- o Verify the ACD software functions as expected.
- o ACD Features:
 - Block unwanted applications and their risk
 - Dynamic whitelisting
 - Code Protection
- o ACD Framework:

- Application Code Protection
- Memory Protection
- o ACD Categories:
 - Binary
 - Trusted Publisher
 - Trusted Installer
 - Trusted Directories
 - Trusted Program
 - Trusted User
 - Trusted Time Window
- o Review current ACD policies for compliance with McAfee Best Practices (up to 5)*
- o Validate ACD Policy Assignment functionality.
- o Confirm availability of ACD queries and dashboards.

Knowledge Transfer: 1 X MD-QS-SMB-4HR*

McAfee's SME will perform the following tasks:

- o Explain the ACD features:
 - Block unwanted applications and their risk
 - Dynamic whitelisting
 - Code Protection
- o Explain the two principal mechanisms that enable ACD:
 - Application Code Protection
 - Memory Protection
- o Explain the uses to allow or disallow membership into the whitelist: (will explain all 7)*
 - Binary
 - Trusted Directory and Trusted Publisher
 - Trusted Installer and Trusted Program
 - Trusted User
 - Trusted Time Window
- o Explain policy creation and assignment based on the previous uses mentioned (up to 5)*.
- o Review the available ACD queries and dashboards (up to 5)*.

Session Requirements - before getting started: Client's responsibility...

- o Functional ePO environment based on McAfee's recommended requirements
- o McAfee Agent installed on the servers to be managed by ACD
- o Identify the names of the targeted clients
- o List applications to be whitelisted (allow)
- o Validate that all endpoints, databases and servers meet McAfee's hardware and software requirements (See Product Guide)
- o Validate that all applicable McAfee software licenses have been installed via Client's valid grant number
- o Perform necessary backups
- o Indicate if there are any outstanding Service Requests/Trouble Tickets opened with McAfee Technical Support

* Configurations and deployments exceeding these numbers will require additional sessions. Each remote session lasts up to 4.0 hours