NetMan Desktop Manager
Take the next step in server based computing

Program control
Nothing Launches without Approval
NetMan Desktop Manager
Take the next step in server based computing

Effective program control
NetMan Desktop Manager 5 gives you wide-reaching control over programs and processes on Windows clients. It closes a perilous gap between the security functions integrated in Windows and those provided by virus scanners and firewalls and the like. After all, the worst threats to network security do not always come from outside – the company’s own employees may unintentionally introduce malware, for example if they are able to install unlicensed or unsafe applications.

Locally and in Sessions
With NDM, you can block programs and other processes from executing on a client machine if they do not have administrator approval. This effectively prevents malware or potentially dangerous scripts from running, and basically makes it impossible to install or launch unlicensed and undesirable software.

The Program Control utility can restrict user access – both locally and in remote desktop sessions – so that only permitted programs, i.e. programs launched through NetMan Desktop Manager, can execute. And you can grant launch permission based on any of a number of factors, including drives, folders, programs, and program certificates. Even if the NetMan Client has not been started in the system – in that case, the NetMan Service can perform the filtering as a basic protection function.

Moreover, the Program Control feature in NDM 5 can prevent the launch of programs on the terminal server without authorization, even if the attempt is made using a roundabout method such as starting from the file explorer.

Comprehensive Data Logging
You can also have NDM 5 log each application call to maintain records of application use. This function also plays an important role in license management, for example in regulating the access and usage of Microsoft Office products to reduce your overall licensing costs.

Time-dependent Access control
In addition to the familiar access control functions that operate based on user name, group or station identity, or access method, you can also use NetMan Desktop Manager to define time-dependent permission for the launch of applications and resources.

Client drive filter
NetMan Desktop Manager also closes security gaps that result from uncontrolled access to the workstations’ locally connected client drives and removable USB storage media. The administrator can specify which folders are accessible on locally connected drives. This effectively prevents the introduction of undesired data and applications during the session.

Internet filter
The Internet Filter integrated in NDM 5 can block any URLs to which you have not explicitly authorized access for the requesting user or computer. This cuts down on the distraction of web browsing and helps prevent users from inadvertently downloading Trojan horses or other malware. When the NetMan Desktop client is installed, the filter works both for local browser sessions and within terminal server sessions. With this filter in place, web access is controlled by means of blacklists and whitelists that can easily be edited by the administrator. The filtering mechanisms can optionally be applied to processes, in addition to URLs. For example, even when users are completely blocked from Internet access, you can let their programs open online help sites and the like. The NDM 5 Internet filter supports all common browsers and proxy servers.