

What is Access Management?

The Access Management console, utilizing Microsoft®* Active Directory®, simplifies and streamlines logon control for networked HMIs and devices covered under the *DisPatch* system. It provides consolidated administration of user and group access permission as well as network policies.

Access Management enables:

- ▶ Better security through a single set of administrators.
- ▶ Stronger user accountability.
- ▶ Consistent enforcement of policies.
- ▶ Reduced administrative overhead.



Key features include:



User Groups

An Access Management system provides centralized management of group policies. This enables administrators to set up group level permissions and then create unique logins for every user within that group. Group members inherit the permissions of the group, eliminating the need for shared accounts.



Access Log Management

By centrally logging all attempted and successful logins, administrators can improve authorization control of the entire network.



Password Authentication

This feature allows an administrator to set password rules for the entire network using parameters like:

- ▶ Minimum length
- ▶ Required combination of alphanumeric and special characters
- ▶ Forced change after a specified timeframe



Security Policies

Centralized management of additional security policies on all connected devices

- ▶ Default account lock-down
- ▶ Domain configuration change management
- ▶ Session lock
- ▶ Banner management

Redundancy Best Practice

Utilizing dual Access Management servers is one way to ensure the system redundancy needed to reliably monitor network logons in the event of a hardware failure. A simplex solution is supported, however uptime cannot be guaranteed in this configuration.

Warranty

Five Year Service and Support Agreement with Next Day On-site.

*Microsoft and Active Directory are registered trademarks of Microsoft Corporation.