



Milestone XProtect - How to optimize AD user logins

Support Team - 2018-08-11 - Comments (0) - IP Surveillance

For XProtect versions 2017 R1 or older, for very large or complicated AD environments, it may be beneficial to limit the depth of AD group enumeration.

1. Ensure that all Smart Client users are added to a single AD group, and they are added as Milestone users via this group only (alternatively, add them as individual users, not as one or more groups)
2. Copy the file "<C:\Program Files (x86)\Milestone\Milestone Surveillance\x64\rename_to_LoginOptimizationParameters.xml>" to a location where you can work with it, and edit it to match what is relevant for your AD Server (default value is to look up in all subgroups, which can cause long AD lookup times). The comments in the XML file explains what you should set it to. If all the Milestone users are in a single group with no subgroups, I'd suggest changing recursiveLevel to 0 (default is -1)
3. Rename the file from step 2 to LoginOptimizationParameters.xml
4. Copy the LoginOptimizationParameters.xml file from step 3 to C:\ProgramData\Milestone\Milestone Surveillance
5. Restart Milestone Image Server Service

The purpose of this file is to limit the number of nested AD groups we will index or enumerate.

The default is 0, which means all AD groups will be indexed. In a very large AD environment or in the event there are recursive groups (Group A is a member of Group B and Group B is also a member of Group A), this can be problematic.

Using LoginOptimizationParameters, you can set the depth of AD user/group enumeration to a fixed number like 1-2.

Does not apply to versions 2017 R2 or newer.

Tags

Milestone

XProtect