

Accessing Applications for Monitoring / Password Encryption

One of the most frequent problems associated implementing any monitoring system is that the applications doing the monitoring (in this case the GeoSystems Monitor) must be able to access the service (or application) that is being monitored. Understanding the security and access requirements of your services and applications is fundamental to making any monitoring point check effective.

All user IDs and passwords are encrypted before they are stored in the GeoSystems SQLite monitoring database.

When working with the ArcGIS Server you can use either Windows or ArcGIS Server security. If you are using Windows security, the server and the GeoMonitor is running on must be in the domain and all userIDs must include the domain (e.g. mydomain\user1).

Article ID: 411

Last updated: 18 Aug, 2020

Revision: 2

GeoSystems Monitor Enterprise -> Product Guide v4.1 - 4.2.1 -> Administrating the GeoSystems Monitor -> Accessing Applications for Monitoring / Password Encryption

<http://www.vestra-docs.com/index.php?View=entry&EntryID=411>