

**Technical Note**

# **Using SQLMagic with XYPRO XYGATE/AC**

**Document Version 1.00**

**Copyright ©2003 Merlon Software Corp.**

## Trademark Acknowledgments

The following are trademarks or service marks of

### Hewlett Packard Company

Guardian Non-Stop Kernel (NSK)  
SafeGuard

The following are trademarks of

### XYPRO Technology Corporation:

XYGATE/AC

## Introduction

This document explains how to modify the configuration of Merlon's SQLMagic product to utilize the facilities of the XYGATE/AC product from XYPRO Technology Corporation. XYGATE/AC is a general purpose access security and control product from:

*XYPRO Technology Corporation  
3325 Cochran Street, Suite 200  
Simi Valley, California 93063-2528 U.S.A.  
Email: support@xypro.com  
Telephone: + 1 805-583-2874 FAX: + 1 805-583-0124*

## Background

SQLMagic is a client-server application. The client runs on a PC workstation and sends commands to a server program which runs on the NSK system. In order to use any client facilities, the user must enter a valid logon name and password, which is encrypted and sent to the SQLMagic server, which in turn logs on to the NSK system. Thereafter, functions performed by the server are subject to standard Guardian and Safeguard security settings.

Some installations however, may have in place a security scheme in which database development and maintenance functions are performed under a single "shared" or "functional" id. Accountability for these functions is ensured through the use of an access control product such as XYGATE. XYGATE allows users to log on using their own unique id, but to perform specific functions (such as database maintenance) using the shared id. The XYGATE product ensures that these operations are audited in such a way that individual activities can be traced to the unique id used to log on.

You must have SQLMagic version 3.23 or greater to implement this feature. Before attempting to configure SQLMagic to use XYGATE/AC, you should perform a standard installation of SQLMagic and ensure that it is working properly under a single userid.

## Configuration Procedure

1. Use the XYGATE EDIT-XAC-ACL procedure to add at least one command for the SQLMagic server. Each entry should look something like:

```
COMMAND SQLMAGIC-DBA
  USER 240,1
  OBJECT $SYSTEM.MERLON.SQLMS
  STARTUP "-S"
  ACL $EVERYONE
  OPENSBYOBJECTS \*.$*.*.*
```

The STARTUP and OPENSBYOBJECTS settings are essential for proper functioning of SQLMagic. You can create entries with different user id specifications as appropriate for your installation.

2. Stop any running SQLMagic processes.
3. After a standard SQLMagic installation the SQLMagic server process (SQLMS) is configured to be started in one of two ways: either
  - The full guardian filename for the SQLMS program file is entered into the TCP/IP portconf file, or
  - The SMSTART macro in the SQLMagic subvolume contains commands to run a specific number of SQLMS servers.

In either case, these entries must be replaced with the name of the SQLMagic Logon Agent program (SLA). This program file should be present in the SQLMagic subvolume. Ensure that the output file is appropriate. The XYGATEAC process will inherit the in and out file settings of the SLA program. To change the PORTCONF file, you need to stop and restart any LISTENER processes.

4. Ensure that there are no SQLMagic processes running. Edit the SQLMagic INI file (SQTINI). Add the following lines to the end of the file:
 

```
[ACCESSCONTROL]
ACTIMEOUT=30
ACPROGRAM=$SYSTEM.XYGATE.XYGATEAC
ACCOMMAND=-N%NAME %CLASS
```
5. Create an EDIT file called ACMAP in the SQLMagic subvolume. Add as many lines as are appropriate for your installation. Each line contains a username pattern followed by a space and the XYPRO command which is used to start the SQLMS server for these users; for example:
 

```
DBA.* SQLMAGIC-DBA
```

 would cause the XYGATE/AC command SQLMAGIC-DBA to be invoked when a user in the DBA group logged on. If, when a user logs on, there is no matching entry in the ACMAP file, the SQLMS server will be run under the user's own id and will be subject to any of the inherent security restrictions for that id.
6. If necessary, restart the SQLMagic servers using SMSTART
7. Attempt to connect to the system using the SQLMagic client.

## Audit

You can audit the SQLMagic session using the XYGATE audit facilities by causing the SQLMagic server to log status messages to its output file. To do this, modify the STARTUP setting in the XYGATEAC ACL to read:

```
STARTUP "-S -L>XAC_AUDIT_OUTPUT"
```

Whenever SQLMagic executes an SQL operation, information (including the text of the SQL statement) is written to the XYGATEAC process. This information will be written to the XYGATEAC audit trail if detail logging has been configured.

## SQLMagic User Profiles

SQLMagic profiles can be used to restrict or control activity performed by a user or group of users. When SQLMagic is run using XYGATEAC, it is started with the functional userid defined in the XYGATE ACACL file. As such, the SQLMagic session is subject to profile settings which apply to the functional id.