Milestone XProtect Corporate 3.1
Step-by-Step Guide

How to Back Up and Restore the System Configuration

This document describes backup and restoration on the same XProtect Corporate Management Server. If you need to back up your XProtect Corporate system configuration on one server, move to another physical server, and then restore your configuration on that server, you should read the step-by-step guide How to Back Up, Move and Restore System Configuration, available on the XProtect Corporate software DVD as well as from http://www.milestonesys.com.

Why Back Up?

The Management Server stores your XProtect Corporate system’s configuration in a database. The database contains almost your entire XProtect Corporate system configuration, including recording servers, cameras, inputs, output, users, rules, alerts, patrolling profiles, clients’ views, any XProtect Smart Walls, etc. Only if you use the Map feature is some of your configuration also stored outside the database (read more about that on page 2). The system configuration database can be stored in two different ways:

- **Network SQL Server:** You have chosen to store your XProtect Corporate system’s configuration in a database on an existing SQL Server on your network. When that is the case, XProtect Corporate’s Management Server simply points to the database’s location on the SQL Server.

- **SQL Server Express Edition:** You have chosen to store your XProtect Corporate system’s configuration in a SQL Server Express Edition database on the Management Server itself.

Regularly backing up your XProtect Corporate system configuration database is always recommended: Having a backup gives you the ability to restore your system configuration in a disaster recovery scenario. However, backing up also has the added benefit that it flushes the SQL Server’s transaction log.

What is the SQL Server transaction log, and why does it need to be flushed?

Each time you make a change to your XProtect Corporate configuration, the SQL Server will log the change in its transaction log—regardless whether it is a SQL Server on your network or a SQL Server Express edition. The transaction log is essentially a security feature that makes it possible to roll back and undo changes to the SQL Server database. The SQL Server by default stores its transaction log indefinitely, and therefore the transaction log will over time build up more and more entries.

The SQL Server’s transaction log is by default located on the system drive, and if the transaction log just grows and grows, it may in the end prevent Windows® from running properly. Flushing the SQL Server’s transaction log from time to time is thus a good idea; flushing it does not in itself make the transaction log file smaller, but it prevents it from growing out of control. XProtect Corporate does not, however, automatically flush the SQL Server’s transaction log at specific intervals. This is because users have different needs. Some want to be able to undo changes for a very long time, others do not care; what would suit one organization’s needs could be problematic for others.

You can do several things on the SQL Server itself to keep the size of the transaction log down, including truncating and/or shrinking the transaction log (for numerous articles on this topic, go to support.microsoft.com and search for SQL Server transaction log). However, backing up XProtect Corporate’s system configuration database is generally a better option since it flushes the SQL Server’s transaction log and gives you the security of being able to restore your XProtect Corporate system in case something unexpected happens.
**Prerequisites**

You will need:

- **Microsoft® SQL Server Management Studio Express**, a tool downloadable for free from [www.microsoft.com/downloads](http://www.microsoft.com/downloads). Among its many features for managing SQL Server databases are some easy-to-use backup and restoration features. Download and install the tool on your existing Management Server. Other backup tools than SQL Server Management Studio Express will also work, but this document describes use of SQL Server Management Studio Express.

**Are You Using the XProtect Smart Wall Add-on Product?**

Smart Wall configuration is stored in the system configuration database, and will consequently also be covered when you follow the instructions in the following.

**Are You Using XProtect Corporate’s Map Feature?**

If using XProtect Corporate’s Map feature (for using maps, floor plans, etc. for navigation and status visualization in clients), virtually all configuration of the Map server is done through a Smart Client. The Map Server configuration, however, is stored server-side, but typically not on the Management Server itself, although that may also happen in some organizations.

The Map Server configuration is stored in a regular Windows folder, not in the SQL Server-based system configuration database. It is therefore not included when you back up the system configuration database, so you must back up and restore the Map Server configuration separately. The separate backup and restoration processes for the Map Server are described on page 4 and 7 respectively.
**Backing Up the System Configuration**

1. Stop the Management Server service to prevent configuration changes being made. This is important since any changes made to the XProtect Corporate configuration between the time you create a backup and the time you restore it on your new Management Server will be lost. If changes are made after the backup, you will have to make a new backup. Note that certain conditions apply while the Management Server service is stopped:

   - **Recording servers will still be able to record:** Any currently working recording servers will have received a copy of their configuration from the Management Server, so they will be able to work and store recordings on their own while the Management Server service is stopped. Scheduled and motion-triggered recording will therefore work, and event-triggered recording will also work as long as it is based on events from the recording server itself.

   - **Recording servers will store log data locally:** They will automatically send log data to the Management Server when the Management Server service is started again.

   - **Clients will not be able to log in:** Smart Client and Remote Client access is authorized through the Management Server. When the Management Server service is stopped, clients will not be able to log in. See the following, however.

   - **Already logged in clients can remain logged in for up to an hour:** When clients log in, they are authorized by the Management Server. Technically, the Management Server gives each client a token, which allows the clients to communicate with recording servers for up to one hour. Should the clients need to communicate with recording servers for longer than one hour, the Management Server automatically renews the clients’ tokens. When the Management Server service is stopped, however, tokens cannot be renewed, and the clients will lose their connections to recording servers when their tokens expire. If you start the Management Server service within an hour, there is a good chance that many of your users will not be affected. We definitely recommend that you inform your users about the possibility of losing contact with the surveillance system while the Management Server service is stopped, even though many users might not experience any loss of contact at all.

   - **No ability to configure the system:** While the Management Server service is stopped, you will not be able to change system configuration through the Management Client.

2. Open Microsoft SQL Server Management Studio Express from Windows’ Start menu (typically by selecting All Programs > Microsoft SQL Server 2005 > SQL Server Management Studio Express). When you open the tool, you are prompted to connect to a server. Specify the name of the required SQL Server (in the example illustration in the following, the server is called MM01232), and connect with the user account under which the database was created.

   **Tip:** You do not have to type the name of the SQL server: If you click inside the **Server name** field and select <Browse for more...>, you can select the required SQL Server from a list instead.

3. Once connected, you will see a tree structure in the **Object Explorer** in the left part of the window. Expand the SQL Server item, then the **Databases** item. We are primarily interested in the **Surveillance** database. The **Surveillance** database contains your entire XProtect Corporate system configuration, including recording servers, cameras, inputs, output, users, rules, alerts, patrolling profiles, clients’ views, any XProtect Smart Walls, etc.

   **No database called Surveillance?** **Surveillance** is the default name of the database containing the system configuration. If you can find the database, but it is not called **Surveillance**, it could be because you gave the database another name when you once installed the Management Server. In the following, we will assume that the database uses the default name.
Example: When the Management Server was installed, you had the option of changing the database name from the default name Surveillance to another name. This can be the reason why your database has another name.

4. Right-click the Surveillance database, and select Tasks > Back Up...

5. On the Back Up Database dialog's General page, do the following:
   - Under Source: Verify that the selected database is Surveillance and that the backup type is Full.
   - Under Destination: A destination path for the backup is automatically suggested. Verify that the path is satisfactory. If not, remove the suggested path, and add another path of your choice.

6. On the Back Up Database dialog's Options page, do the following:
   - Under Reliability: Select Verify backup when finished and Perform checksum before writing to media.

7. When ready, click OK to begin the backup. When backup is finished, you will see a confirmation. When finished, exit Microsoft SQL Server Management Studio Express.

   Tip: Also consider backing up the SurveillanceLog database, using the same method. The SurveillanceLog database (name may be different if you renamed the system configuration database) contains all your XProtect Corporate system logs, including errors reported by recording servers and cameras. Backing up this database is not vital since it does not contain any system configuration, but you may later appreciate having access to system logs from before the Management Server move.

8. During the backup process, the Management Server service was stopped to prevent configuration changes being made until you were done. Remember to start the Management Server service again.

**Backing Up the Map Server Configuration**

If using XProtect Corporate’s Map feature (for using maps, floor plans, etc. for navigation and status visualization in clients), virtually all configuration of the Map server is done through a Smart Client. The Map Server configuration,
however, is stored server-side, but typically not on the Management Server itself, although that may also happen in some organizations.

The Map Server configuration is stored in a regular Windows folder, not in the SQL Server-based system configuration database. It is therefore not included when you back up the system configuration database, so you must back and restore the Map Server configuration separately.

On the computer on which the Map Server configuration is stored, make a backup copy of the XProtect Map Server folder, including all of its subfolders and content:

- On a computer running Windows Vista®, Windows 2008 Server or Window 7, you will typically find the folder at C:\ProgramData\Milestone\XProtect Map Server
- On a server running Windows XP or Windows Server 2003, you will typically find the folder at: C:\Documents and Settings\All Users\Application Data\Milestone\XProtect Map Server
Restoring the System Configuration

Luckily, most users never need to restore their backed-up XProtect Corporate system configuration, but if you ever have the need, use the following process:

1. Stop the Management Server service to prevent configuration changes being made until you have restored the system configuration database. Note that certain conditions apply while the Management Server service is stopped:

   • **Recording servers will still be able to record:** Any currently working recording servers will have received a copy of their configuration from the Management Server, so they will be able to work and store recordings on their own while the Management Server service is stopped. Scheduled and motion-triggered recording will therefore work, and event-triggered recording will also work as long as it is based on events from the recording server itself.

   • **Recording servers will store log data locally:** They will automatically send log data to the Management Server when the Management Server service is started again.

   • **Clients will not be able to log in:** Mart Client and Remote Client access is authorized through the Management Server. When the Management Server service is stopped, clients will not be able to log in. See the next item, however.

   • **Already logged in clients can remain logged in for up to an hour:** When clients log in, they are authorized by the Management Server. Technically, the Management Server gives each client a token, which allows the clients to communicate with recording servers for up to one hour. Should the clients need to communicate with recording servers for longer than one hour, the Management Server automatically renews the clients’ tokens. When the Management Server service is stopped, however, tokens cannot be renewed, and the clients will lose their connections to recording servers when their tokens expire. If you start the Management Server service within an hour, there is a good chance that many of your users will not be affected. We definitely recommend that you inform your users about the possibility of losing contact with the surveillance system while the Management Server service is stopped, even though many users might not experience any loss of contact at all.

   • **No ability to configure the system:** While the Management Server service is stopped, you will not be able to change system configuration through the Management Client.

2. Open Microsoft SQL Server Management Studio Express from Windows’ Start menu (typically by selecting All Programs > Microsoft SQL Server 2005 > SQL Server Management Studio Express). When you open the tool, you are prompted to connect to a server. Specify the name of the required SQL Server, and connect with the user account under which the database was created.

   **Tip:** You do not have to type the name of the SQL server: If you click inside the Server name field and select <Browse for more...>, you can select the required SQL Server from a list instead.

2. Once connected, you will see a tree structure in the Object Explorer in the left part of the window. Expand the SQL Server item, then the Databases item.

3. Right-click the Surveillance database, and select Tasks > Restore > Database...

   **No database called Surveillance?** Surveillance is the default name of the database containing the system configuration. If you can find the database, but it is not called Surveillance, it could be because you gave the database another name when you once installed Management Server. In the following, we will assume that the database uses the default name.

4. The Restore Database dialog’s General page, do the following: Under Source for restore, select From device, and click the button to the right of the field.

5. In the Specify Backup dialog’s Backup media list, make sure that File is selected. Then click the Add button.
6. In the **Locate Backup File** dialog, locate and select your backup file `Surveillance.bak`. Then click **OK**.

7. Back in the **Specify Backup** dialog, the path to your backup file is now listed. Click **OK**.

8. Back on the **Restore Database** dialog’s **General** page, your backup is now listed under *Select the backup sets to restore*. Make sure you select the backup by selecting the check box in the **Restore** column.

9. Now go to the **Restore Database** dialog’s **Options** page, and select *Overwrite the existing database*. Leave the other options as they are.

10. When ready, click **OK** to begin the restoration. When the restoration is finished, you will see a confirmation. When finished, exit **Microsoft SQL Server Management Studio Express**.

   **Tip:** If instead you get an error message telling you that the database is in use, try exiting **Microsoft SQL Server Management Studio Express** completely, then repeat steps 1-10.

11. During the restoration process, the Management Server service was stopped to prevent configuration changes being made until you were done. Remember to start the Management Server service again.

If you also backed up the `SurveillanceLog` database from the old Management Server, restore it using the same method.

### Restoring the Map Server Configuration

If using XProtect Corporate’s Map feature (for using maps, floor plans, etc. for navigation and status visualization in clients), virtually all configuration of the Map server is done through a Smart Client. The Map Server configuration, however, is stored server-side, but typically not on the Management Server itself, although that may also happen in some organizations.

The Map Server configuration is stored in a regular Windows folder, not in the SQL Server-based system configuration database. It is therefore not included when you restore the system configuration database, so you must back and restore the Map Server configuration separately.
On the computer on which the Map Server configuration is stored, restore your Map Server configuration by placing your backup copy of the XProtect Map Server folder, including all of its subfolders and content, to the location where your XProtect Corporate system expects to find it:

- On a computer running Windows Vista, Windows 2008 Server or Windows 7, you would typically place the folder at \textit{C:\ProgramData\Milestone\XProtect Map Server}
- On a server running Windows XP or Windows Server 2003, you would typically place the folder at: \textit{C:\Documents and Settings\All Users\Application Data\Milestone\XProtect Map Server}

Restart the Management Server service after placing the XProtect Map Server folder at its required location. Then make sure that the Map Server service is recognized as a trusted service within XProtect Corporate:

1. In XProtect Corporate’s Management Client, click the \textit{Tools} menu, then select \textit{Registered Services}...
2. In the \textit{Add/Remove Registered Services} window, select the \textit{Map Service} in the list, then click \textit{Edit}...
3. In the \textit{Edit Registered Service} window, select \textit{Trusted}, then click \textit{OK}.
4. The Map Server is now restored with its previous configuration. In the \textit{Add/Remove Registered Services} window, click \textit{Close}.
Trademarks

XProtect is a registered trademark of Milestone Systems A/S.

Microsoft® and Windows® are registered trademarks of Microsoft Corporation.

All other trademarks mentioned in this document are trademarks of their respective owners.

Disclaimer

This document is intended for general information purposes only, and due care has been taken in its preparation.

Any risk arising from the use of this information rests with the recipient, and nothing herein should be construed as constituting any kind of warranty.

Milestone Systems A/S reserve the right to make adjustments without prior notification.

All names of people and organizations used in this document's examples are fictitious. Any resemblance to any actual organization or person, living or dead, is purely coincidental and unintended.

Want More?

The XProtect Corporate Administrator’s Manual, and many other useful guides and manuals, are available for download in PDF format from www.milestone.dk/support/documentation.