

1. MonitorMagic connection basics

In MonitorMagic, the following connection types can be distinguished:

Client - Service:

Windows authenticated RPC communication, embedded in TCP/IP, over port 48155.

Used when:

- Monitor window is open
- Global alarm window is open
- Service configuration
- Control center connections
- Report generation
- Central policies

Service – Monitored host:

Windows authenticated RPC communication, embedded in TCP/IP, over port 48155. For ping hosts, the ICMP protocol is used. For SNMP hosts, the SNMP Get v1 protocol specification is used.

- All Windows monitor types
- SNMP get monitor
- Ping monitor

Service – Database:

ODBC connection, native Windows or SQL authentication.

Used when:

- Monitor has database storage enabled
- Accessing the graph feature in the MonitorMagic client
- Report generation

Service – Internet Browser:

HTTP or HTTPS using certificates uses native Windows authentication. The ports are configurable.

Used when:

- Show MonitorMagic results in the event browser
- Manage event logs, services, computers and more

2. Using SQL authentication when service is running in DMZ

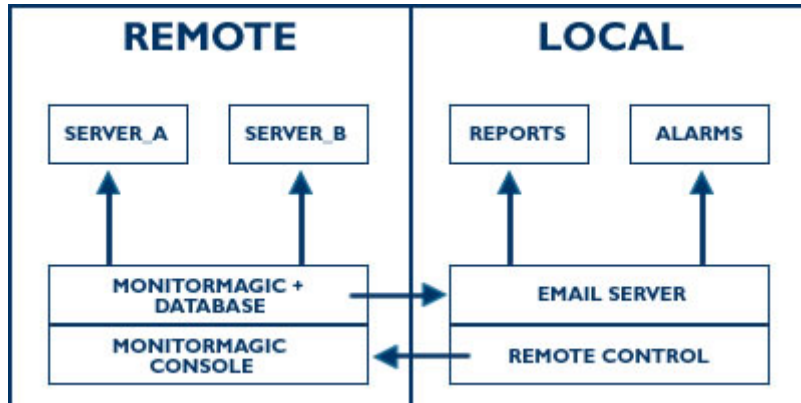
- Configure the SQL Server to support both Windows and SQL authentication, be sure to restart the SQLServer services afterwards. Note that modifying this setting can take a while; please be patient for the operation to complete.
- Modify the data source, switch from Windows authentication to SQL authentication, and make sure that the MonitorMagic database is the default database for the data source.
- In MonitorMagic, go to the service configuration, and then the advanced -> database configuration. Use the Configure button and select the existing data source which was preset to use Windows authentication. Make sure the data source is selected and the radio button is enabled. In the lower portion of the screen, make sure that you include the username and password for the SQL account:
`DSN=MonitorMagicSql;UID=<sqlaccountname>;PWD=*****`
- The existing database will now be used and the status will be shown as 'Ok' in the MonitorMagic Control Center.

3. Connection scenarios when working with remote sites

When working with MonitorMagic deployments at remote sites, you will want to connect to these sites from time to time to perform maintenance. There are several scenarios to do this:

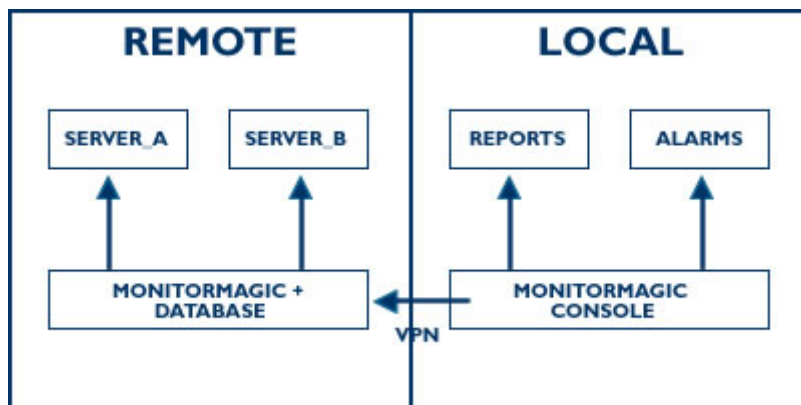
1. Client and service both on remote site:

In this scenario, the complete MonitorMagic application runs on a remote site. Using third party tools such as pcAnywhere or DameWare, you can connect to the remote site and use the MonitorMagic client to connect to the service.



2. Client on local site, service on remote site:

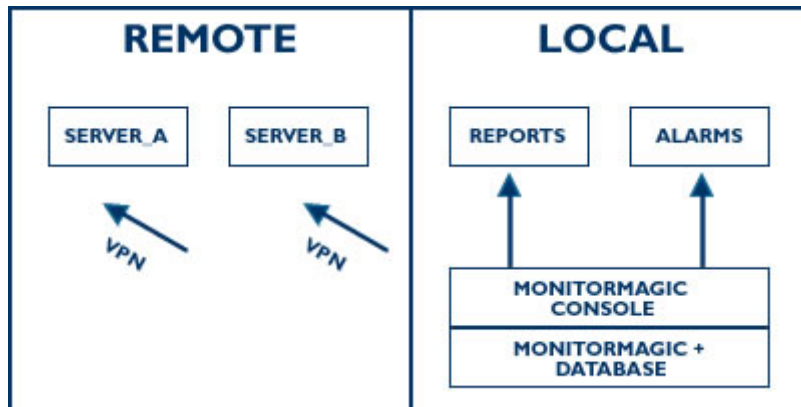
In this scenario, the client runs on your local network, while the MonitorMagic service runs on a remote site. To connect to the MonitorMagic service, the user account you are using to run the client must have sufficient permissions to connect to the service. This means that a VPN including a trust is required for security reasons. This is essentially the same as when you use computer management, and connect yourself to another computer. If you can connect to the computer running the MonitorMagic service, then the security should be fine.



You can use the global alarm window, while the MonitorMagic client has connections open to all remote sites. This means that you would need to have permanent VPN connections with trusts to provide the required security. Tools4ever recommends using e-mail notification in combination with automatic report e-mail distribution instead of this setup.

3. Client on local site, service on local site:

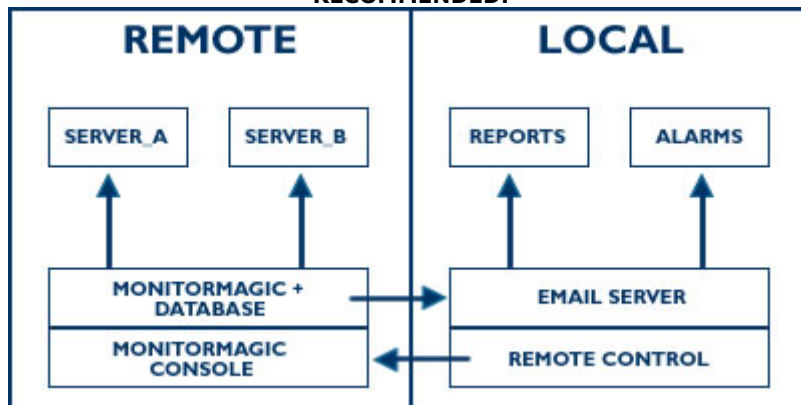
In this scenario, the client runs on your local network and connects to the MonitorMagic service running also on your local network. The MonitorMagic service monitors remote sites using a permanent VPN connection. This setup can easily use a central database running at the local network, but has limited scalability due to network traffic restrictions. When using monitoring, network traffic will be minimal, but when using event archiving you have to make sure to schedule this outside office hours.



4. Distributed databases at remote site:

Tools4ever recommends installing a SQL Server or MSDE instance on each remote site. This means that on every site, a single agent will monitor multiple servers and store the results in a local database. You can then enable automatic report e-mail distribution to receive weekly or daily updates from this site to automate regular maintenance. This minimizes the occurrences where you have to manually connect yourself to a remote site to perform maintenance. Installing a central database on the local network which also receives its data from a local service, as described above has limited scalability due to network traffic restrictions.

RECOMMENDED:



5. Central database at local site:

The other scenario is to place a central database on the local side which will then receive data from either distributed MonitorMagic services at remote sites, or from one central MonitorMagic agent. Both scenarios will cause significant network traffic and require a permanent VPN connection.

Note: when the MonitorMagic service accesses a database over a VPN connection, the VPN connection has to be open at all times. The MonitorMagic service cannot handle a disconnected VPN; this will result in unexpected behavior. When the VPN is reconnected, the MonitorMagic service will not automatically resume database storage. Tools4ever strongly recommends not using a database connection over a VPN.

