

SCS-VR™

VIRTUAL RECEIVER

INSTALLATION SETUP GUIDE

SCS-VR™ VIRTUAL RECEIVER

DIGITAL MONITORING PRODUCTS, INC.

© 2023

TABLE OF CONTENTS

SYSTEM OVERVIEW 1

- What is SCS-VR?.....1
- Benefits.....1
- Recommended Server Specifications1
 - SCS-VR Application Server (Each Primary and Backup Server)1
 - SQL Server (Each Primary and Backup Database)1
- General Requirements2
 - California State Fire Marshall Listing2
 - 256-bit AES Encryption2
- UL Listed Compliance Specifications3
 - Hardware Installation Requirements3
 - SQL Local Database Configuration Requirements.....3
 - SQL Remote Database Configuration Requirements.....3
 - Minimum Hardware Requirements3
- UL Listed Hardware Setup 4

INSTALLING SCS-VR 6

- SCS-VR Configuration using Database Configurator Utility 6
 - Test Connection7
- Distinguishing Primary and Backup Servers..... 8
- Communication Settings 8
 - Container Format 8
 - Expected ACK..... 8
 - Outgoing ACK..... 8
 - Message Expiration Delay (Hours) 8
- Test Panel Communication to SCS-VR..... 9
- Configure Windows Authentication Login..... 9
 - Launch the Service 9
 - Setup Console.....10
 - User Login Management.....10
 - Login Permissions 11
- SCS-VR Viewer12
- Updating SCS-VR13
- Upgrade Process for Recommended Configuration15
- Upgrade Process for Non-Existing Backup Database17
- Upgrade Process for SCS-VR with Full Disaster Recovery18

SYSTEM OVERVIEW

What is SCS-VR?

The SCS-VR is a UL Classified software solution that runs on a server as a virtual receiver for network, IP, and cellular communications. SCS-VR manages alarm signals and supervision messages without the maintenance, space, or power requirements of a rack-mounted hardware receiver.

The SCS-VR communicates with panels and central stations using DMP network alarm messaging. The SCS-VR works with Microsoft® SQL Server® and can run on more than one server from the same database. The SCS-VR software accepts alarms from network, Internet, or cellular communicators.

Benefits

The SCS-VR offers a wide range of benefits for alarm dealers and central station operators, including:

- Scalability: SCS-VR can support small network monitoring organizations to central stations monitoring thousands of accounts.
- Wide Area Network (WAN) support: WAN inputs monitor the status and condition of one another and back each input up, enhancing the panels' ability to reach the receiver. This supports redundant communications service providers on a single receiver.
- Dispersed server support: Software can be deployed on multiple servers to support a geographically distributed approach with path protection and minimize nuisance supervision failure messages for high-security applications.
- Advanced diagnostics: Full data logging for reliable service and fast troubleshooting.
- Unique server programming: Group capability enables a single receiver to function as multiple separate receivers equipped with their own unique programming.
- Power and space savings.
- Supports 128-bit and 256-bit AES encryption.

Recommended Server Specifications

You will need to meet the following requirements to successfully use the SCS-VR:

SCS-VR Application Server (Each Primary and Backup Server)

- Intel® Core™ iSeries Processor or better (Dual Core)
- Dedicated 12 GB RAM
- Gigabit Ethernet adapter or better
- Dedicated 20 GB HDD or greater
- Microsoft Windows Server 2016 or newer
- Java 8

If using encryption, Java Cryptography Extension (JCE) is required.

SQL Server (Each Primary and Backup Database)

- Intel Core iSeries Processor or better (Quad Core)
- Dedicated 16 GB RAM
- Gigabit Ethernet adapter or better
- Microsoft Windows Server 2016 or newer
- Dedicated 160 GB HDD or SSD: RAID 1 for Redundancy (recommended, not required)

General Requirements

- All servers must be operating at all times including monitors.
- Do not use screen savers on any SCS-VR server.
- All servers must be connected to an uninterruptible power supply suitable for use with security systems.
- All servers must have a keyboard, mouse, monitor, and network connected. Refer to the manufacturer's instructions.
- The installation must provide supply line transient protection complying with the Standard for Transient Voltage Surge Suppressors, UL 1449, with a maximum marked rating of 330 V.
- The source of power for the equipment shall be within the rated voltage range of the signal processing equipment.
- The installation must provide supply line transient protection complying with the Standard for Protectors for Data Communications and Fire Alarm Circuits, UL 497B, with a maximum marked rating of 50 V.
- The communication circuits and network components connected to the telecommunications network must be protected by secondary protectors for communication circuits. These protectors must comply with the Standard for Secondary Protectors for Communications Circuits, UL 497A, with a marked rating of 150 V or less. These protectors must be used only in the protected side of the telecommunications network.
- All equipment must be installed in a temperature-controlled environment that can be maintained between 13 - 35°C (55 - 95°F) by the HVAC system. The environment shall also be maintained within the humidity range rating of the equipment. Twenty-four hours of standby power must be provided for the HVAC system. The standby power system for the HVAC system may be supplied by an engine driven generator alone. A standby battery is not required to be used. A maintenance contract that provides for restoring operation of the HVAC system within 24 hours, 7 days a week shall be in place.
- In addition to the 110/240 VAC, 50/60 Hz main and secondary power supplies that are required to be provided at the central supervisory station, the system must also be provided with an uninterruptible power supply (UPS) with sufficient capacity to operate the server equipment for a minimum of 15 minutes. If more than 15 minutes is required for the secondary power supply to supply the UPS input power, the UPS must be capable of providing input power for at least that amount of time.
- UPS systems must comply with the Standard for Uninterruptible Power Supply Equipment, UL 1778, or the Standard for Fire Protective Signaling Devices, UL 1481.
- In order to perform maintenance and repair service, a means for disconnecting the input to the UPS while maintaining continuity of power to the automation system shall be provided.
- A polling error "non check-in message" alarm must be responded to as a compromise attempt by proper authorities.
- The central station's primary power supply is monitored for AC loss. A tamper switch is also provided to monitor the control unit's front cover removal. For either condition, a change of status display occurs at the central station.
- Equipment must be installed within a locked room or a locked rack provided with a tamper switch.
- A power conditioner used with the system shall comply with the applicable requirements in the Standard for Power Units Other Than Class 2, UL 1012.
- All equipment connected to the signal processing equipment must be located in the same room as the signal processing equipment.
- All equipment must be self-contained in a rack with means for connection to the branch circuit supply which includes installing the supply conductors in conduit.
- The self-contained rack with the SCS-VR servers shall also have speakers for audible annunciation for local operation and must be located in proximity of the supervising station for operator interface.
- All interconnected equipment used in conjunction with the SCS-VR or SQL servers such as monitor, keyboard, and mouse must not have cabling exceeding 8 feet in length.

California State Fire Marshall Listing

SCS-VR is approved by the California State Fire Marshall (CSFM) for fire installations. Refer to Listing No. 7168-1157:0133.

256-bit AES Encryption

The SCS-VR virtual receiver, version 1.4.0 or higher, supports the 256-bit AES encryption option for XR550E control panels using version 104 or higher software. SCS-VR supports both the new 256-bit option and 128-bit to maintain compatibility with existing control panels. Either 128-bit or 256-bit encryption can be enabled in panel programming for NET or CELL communication paths. Once enabled in the panel, SCS-VR automatically communicates with that panel using the appropriate encryption. Refer to Listing NIST AES Algorithm Certificate #3027 256-bit.

To support AES Encryption, Java Cryptography Extension (JCE) must be deployed.

UL Listed Compliance Specifications

The UL Classified Compliance Specifications are for SCS-VR software version 1.4.0 or higher used in conjunction with UL listed ITE Equipment.

Hardware Installation Requirements

- The UL 864, UL 1076, and UL 1610 installations must consist of at least two completely duplicated servers running SCS-VR version 1.4.0 or higher. The SCS-VR backup must be programmed to accept alarm communication as if it was the SCS-VR primary.
- No software unrelated to the processing of alarm signals other than the operating system software and anti-virus/security protection shall be installed on the primary and backup servers.
- Configurations employing virtual servers are permitted where applicable requirements for supervision and redundancy are met. These configurations must include at least two physical servers.

SQL Local Database Configuration Requirements

- All SCS-VR servers must share a primary SQL Server database located on the SCS-VR primary server. A duplicate SQL Server database must be available on the SCS-VR backup server.
- The databases of both SQL servers must be structured to communicate with either SCS-VR primary or SCS-VR backup including database name and password.
- If the SQL primary fails, both SCS-VR servers will produce a pop-up window indicating that SCS-VR cannot communicate with the SQL database. SCS-VR automatically switches to the backup SQL database.
- For an example setup of the local database configuration, see Figure 1

SQL Remote Database Configuration Requirements

- All SCS-VR servers must share a primary SQL Server database located on a third server. A fourth server with a duplicate backup SQL Server database must be available. At the installer's choice, one SQL server is to be designated as the SQL primary and the second SQL server is to be designated as the SQL backup.
- The databases of both SQL servers must be structured to communicate with either SCS-VR primary or SCS-VR backup including database name and password.
- The local operator monitoring the systems must know the IP addresses of each SQL server.
- If the SQL primary fails, both SCS-VR servers will produce a pop-up window indicating that SCS-VR cannot communicate with the SQL database. SCS-VR automatically switches to the backup SQL database.
- For an example setup of the remote database configuration, see Figure 2.

Minimum Hardware Requirements

SCS-VR was evaluated by UL with the following minimum configuration:

General Requirements

- 160 GB storage
- 2 GB RAM
- CD drive
- 10/100 network (NIC) card
- Video card

SCS-VR Application Server

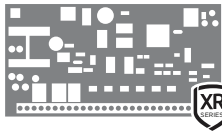
- Intel® Core™ i3-540, 3.06 GHz processor
- Windows Server 2012 Standard R2 or newer
- SCS-VR version 1.4.0 or higher (version number is displayed on the SCS-VR console **Configuration** tab).

SQL Server

- Intel® Core™ 2 Duo E6300, 2.80 GHz processor
- Windows Server 2012 Standard R2 or newer
- Microsoft SQL Server 2012 or newer
- .NET Framework 3.5 or higher
- Windows PowerShell 1.0 or higher

UL Listed Hardware Setup

XR150/XR550 Series



Network or Cell



* All computers are UL listed for ITE equipment

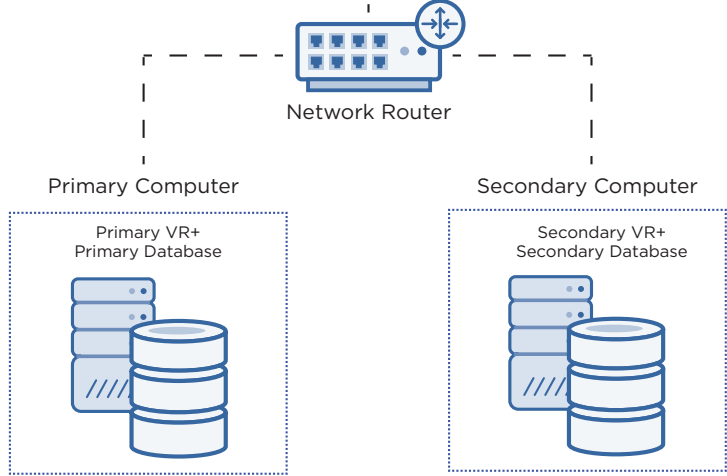
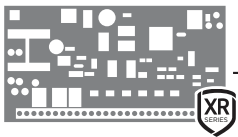


Figure 1: UL Listed Local Database Setup Diagram

XR150/XR550 Series



Network or Cell



* All computers are UL listed for ITE equipment

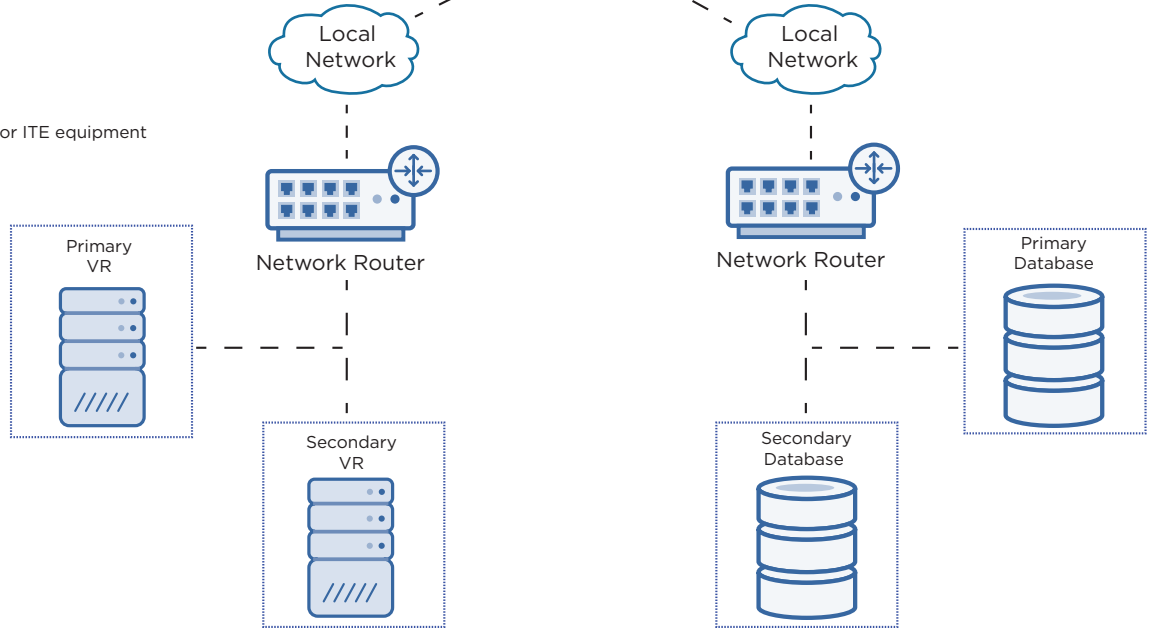


Figure 2: UL Listed Dual Environment Setup Diagram

Microsoft SQL Server Best Practices

For optimal SCS-VR performance, do the following processes regularly to maintain the Microsoft SQL database:

Rebuild and reorganize indexes (daily/weekly)

As data is added, indexes become inaccurate because data is added to the end instead of in order. It is a maintenance best practice to reorganize daily and rebuild weekly. Reorganizing is faster and puts less overhead on the system. Rebuilding takes more system resources and automatically updates statistics.

Update statistics (nightly)

Microsoft SQL tries to optimize its performance by making the most used data the most readily available. Updating statistics allows Microsoft SQL to come up with query plans to find popular data the fastest. Those statistics can be set to auto update or run nightly. Always update statistics manually after performing a database reorganization.

Check for free space (weekly)

If auto grow is turned on, set it as close to 10% as possible. Ensure there is enough actual drive space to accommodate growth.

Check disk drive contention (weekly)

Check disk drive contention weekly. Ideally, data files and log files are on different physical disks. Use Windows Performance Monitor to monitor the disks and ensure that the read and write queue lengths are always less than 1. If the queue length is longer than 1, the disk is receiving more requests for data than it can process. This will slow down performance significantly.

Check database integrity (weekly)

Use the DBCC check to verify the health of the database in general. Also, run the DBCC check table and check ALLOC and the DBCC check catalog. These commands verify that the database is not corrupt.

INSTALLING SCS-VR

The SCS-VR must be able to communicate with a SQL database.

- Enable Mixed Mode authentication on your SQL Server Instance.
- Ensure that proper permissions for the login used by the SCS-VR can create a database and fully read, write, and modify all content within. (For example: DB Owner privileges or better)

SCS-VR Configuration using Database Configurator Utility

After installation, SCS-VR Installation Database Configurator Utility should open automatically. If **Database Configurator Utility** does not open, navigate to **Start > All Programs > SCS-VR > Configurator.exe**. Right-click on **Configurator.exe** and select **Run as administrator**.

To configure **Primary Database Configuration**, complete the following fields:

- **Database name**—The name of the primary SCS-VR database.
- **Database server name**—The name of the server where the primary database is installed. (This can also be an IP address if preferred or if DNS issues arise.)
- **Database port number**—Enter the appropriate SQL port here. Default is **1433**.
- **Database username**—The database administrator username for the primary database.
- **Database password**—The database administrator password for the primary database.

Select **Use Secondary Database** to configure the secondary database. Complete the following fields:

- **Database name**—The name of the secondary SCS-VR database.
- **Database server name**—The name of the server where the secondary database is installed. (This can also be an IP address if preferred or if DNS issues arise.)
- **Database port number**—Enter the appropriate SQL port here. Default is **1433**.
- **Database username**—The database administrator username for the secondary database.
- **Database password**—The database administrator password for the secondary database.

 **Note:** If connection to the primary database is lost, SCS-VR will use the secondary database. If you are not creating a secondary database, skip to “Test Connection”.

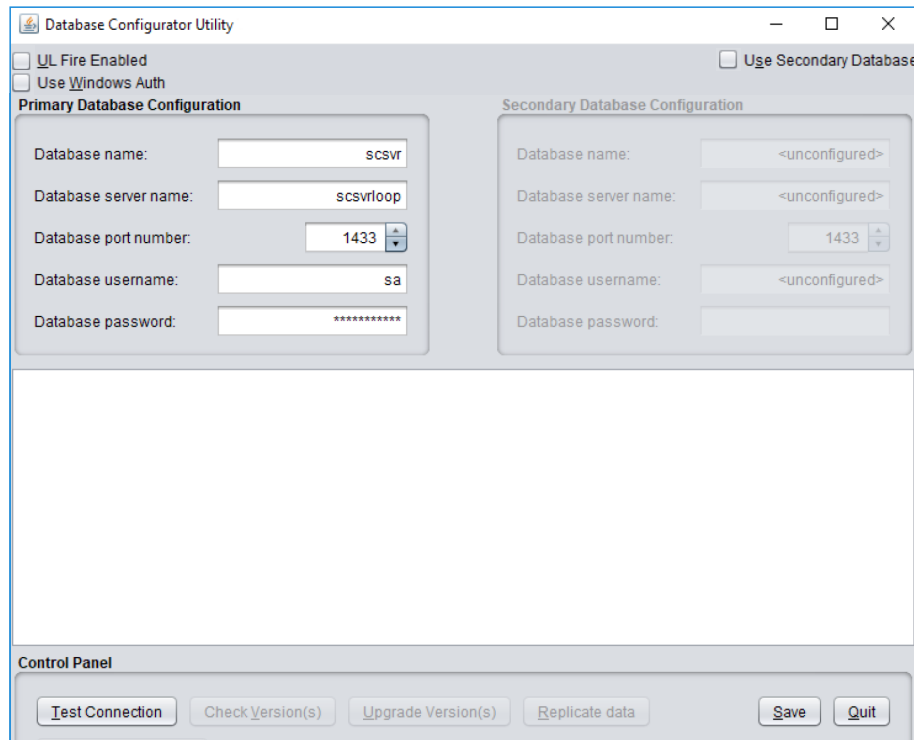


Figure 5: Database Configurator Utility

Test Connection

1. Select **Test Connection**. The **Database Configurator Utility** will test the connection to the primary and secondary databases. A successful test will display **Connection obtained from <database> on <server>**. An error during testing will display **Failed to connect to <database> on <server>**.

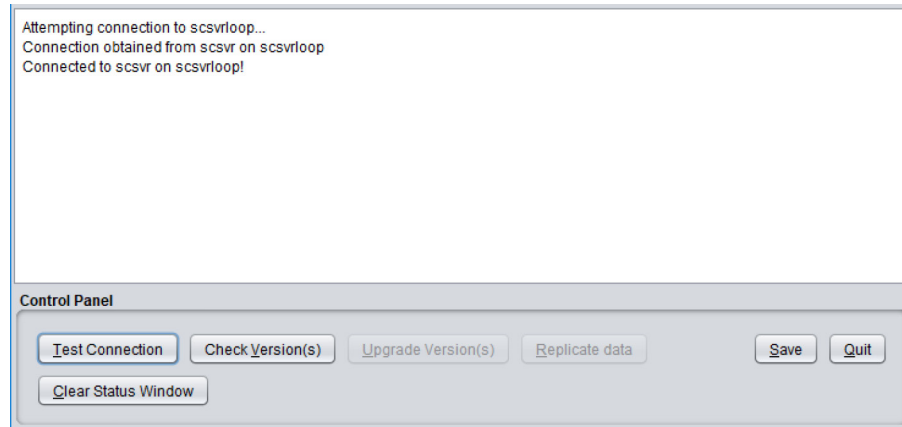



Figure 6: Test Connection

2. If the configured database does not exist or you are creating a new database, a dialog pops up to confirm database creation. Choose **YES** to create the database as configured. Choose **NO** to disregard the configuration information and return you to the Configuration Tool.
3. Select **Check Version(s)** to determine the version level of the database(s) running on the SCS-VR. The database version will be displayed in the **Status Window**.

 **Note:** Newly-created databases should be version 0 (zero).

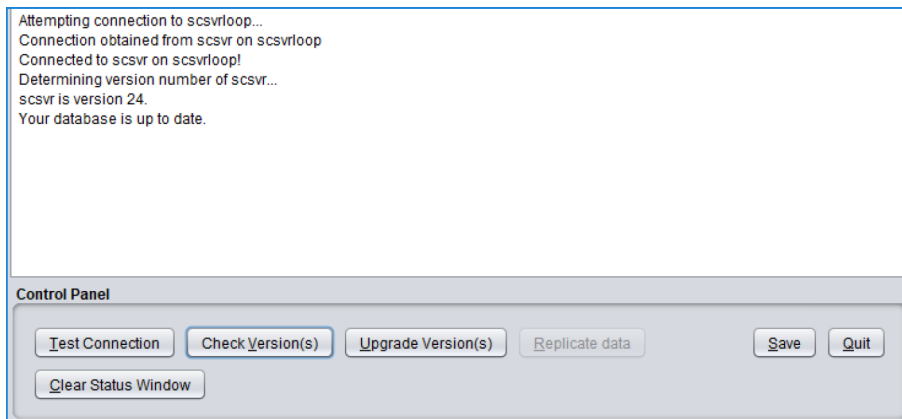


Figure 7: Upgrade Version(s)

4. If the configured database is new or the version is not current, you will see the **Upgrade Version** option. Select the option to upgrade the database to the latest version.
5. If you are configuring a new installation or upgrading to a new version of SCS-VR, the **Replicate Tables** option will display. Choose **YES** if the secondary database is empty. The primary database information will be replicated to the Secondary database. Choose **NO** if you have already created a secondary database.
6. Save the database information.
7. A dialog pops up to confirm you wish to save the configured database to the computer registry. Choose **YES** if you wish to save the database to the computer registry. Choose **NO** if you wish to disregard the information and return to the Configurator.
8. Select **Quit** to exit the utility.

Distinguishing Primary and Backup Servers

Once SCS-VR installation is complete, you need to set the primary server to **Primary** and the backup server to **Backup**.

1. On the primary server, navigate to **Start > All Programs > SCS-VR Setup Console.exe**. Right-click on **SCS-VR Setup Console.exe** and select **Run as administrator**. The **SCS-VR Setup Console** window opens.
2. On the **Configuration** tab in the **Server Name** field, designate a unique name for the server, such as "Primary".
3. Open the **SCS-VR Setup Console** window on the backup server. On the backup server, set the server name to the backup VR.

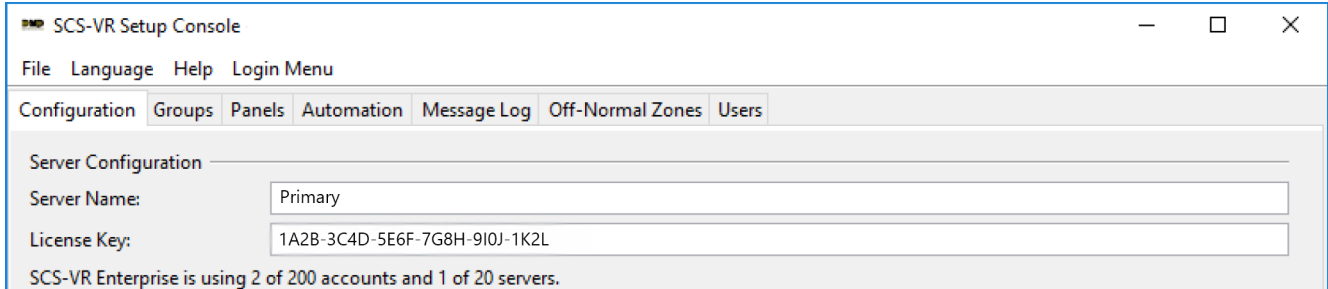


Figure 8: Setup Console

Communication Settings

Changing any of the Communications Settings and selecting **Apply** will clear any pending messages.

Container Format

The format to use when sending messages to automation. The order is determined by the automation server that is communicating with the SCS-VR. An example container format is: %05g%5a %m%13x. Based on the table below, the example would send the following information to the automation server: Group number padded with 5 leading zeros, account number padded with 5 trailing spaces, message payload, and carriage return.

Expected ACK

The expected response from automation when SCS-VR dispatches a message.

Outgoing ACK

The message sent in response to the automation

ACK Code	Meaning
%Nx	N is any number from 0-255
%13x	Carriage return
%a	Account number
%g	Group number
%s	Server number
%S	Server name
%p	Port number for this group
%m	Message payload
%5aC	Account number padded with up to 5 characters, where C is a character
%05a	Account number padded with zeros up to 5 characters

Message Expiration Delay (Hours)

Enter the number of hours the SCS-VR holds a message to automation before discarding it. To never discard the message, enter a zero. Default is **0** (zero).

The following is a list of types of delays for message deletion:

- Checkin Message Deletion Delay (Hours)
- Alarm Message Deletion Delay (Hours)
- Other Message Deletion Delay (Hours)

Test Panel Communication to SCS-VR

If you would like to test SCS-VR connection to a DMP control panel, use the following settings:

- Set **Communication Path** to **NET** or **CELL**.
- Set IP address to the SCS-VR primary server.
- Designate the appropriate port and ensure that a Group has been created on the VR that is enabled and listening for communication.

Configure Windows Authentication Login

SCS-VR Setup Console and the SCS-VR Service run as different users by default. To use Windows Authentication, the database administrator will need to set up logins with appropriate authority on the VR databases.

- If the service and database are on the same machine, the service login will look something like:
NT AUTHORITY\SYSTEM.
- If the service and databade are not on the same machine, the service login will look something like:
<domainname>\<machinename>\$.

Launch the Service

1. Open the **Database Configurator**.
2. Turn on **Use Windows Auth**.
3. Select **Test Connection**.

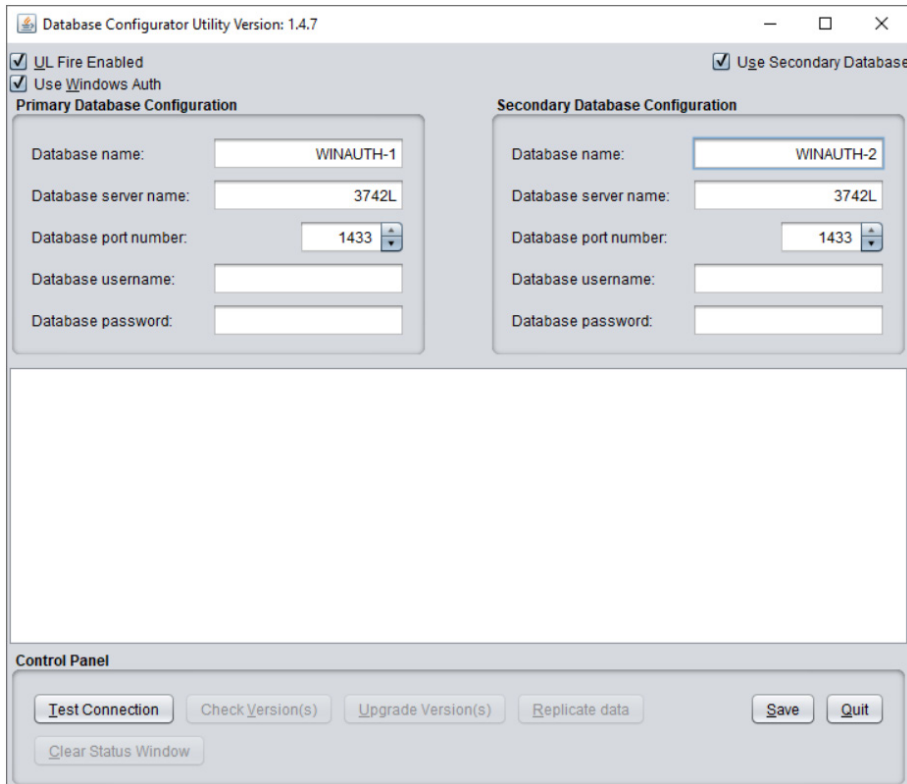


Figure 9: Database Configurator


Setup Console

In the Setup Console, leave the **Username** and **Password** field blank.

User Login Management

Specific User

To set up the service to run for a specific user login, follow the steps below.

 **Note:** If the user's password changes, the admin will need to change the password on this service configuration.

1. In Services, select **SCS-VR**.
2. Go to the **Log On** tab.

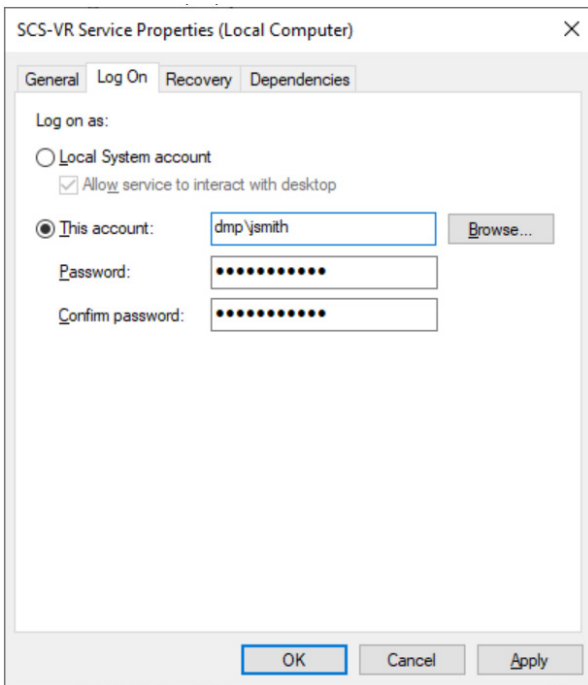


Figure 10: Configure SCS-VR Password

3. Select **This account** and enter the account and password.
4. Select **Apply**.
5. Select **OK**.

Default User

To set up the service to run with the default computer login, set up the logins in SQL SERVER.

Login Permissions

When the VR and database are on the same machine, the default user will be:

NT AUTHORITY\SYSTEM.

1. Double-click the service.
2. Go to **User Mapping**.

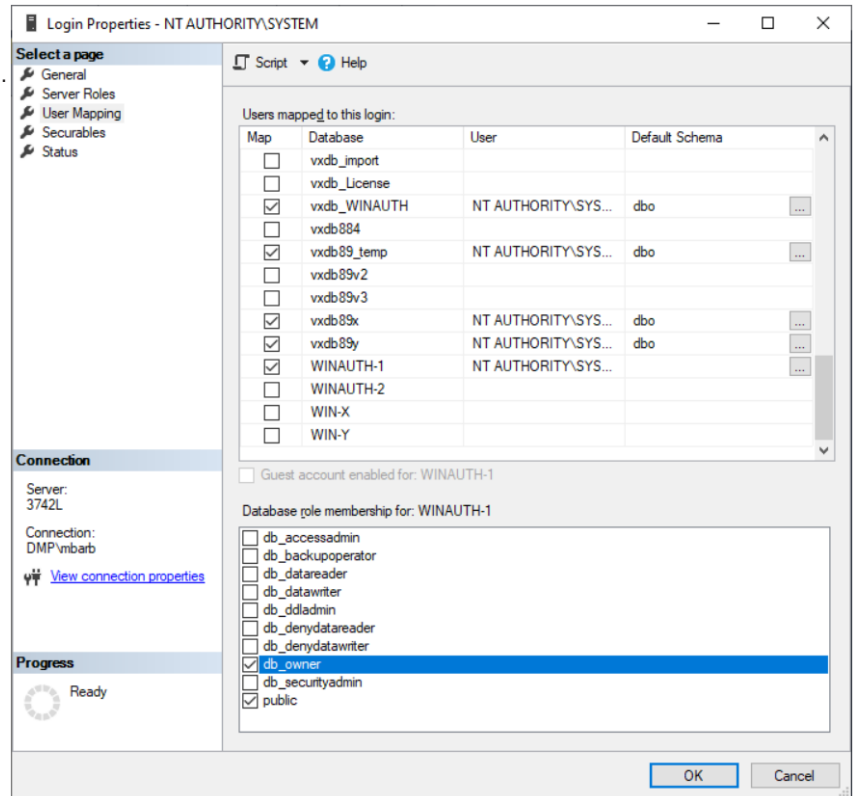


Figure 11: Same Machine Login Permissions

3. Select the **Users mapped to this login**.
4. Select the user permissions under **Database role membership**.
5. Select **OK**.

When the VR and database are on separate machines, the service user will look something like: **<domainname>\<machinename>\$**.

1. Double-click the service.
2. Go to **User Mapping**.
3. Select the **Users mapped to this login**.
4. Select **OK**.

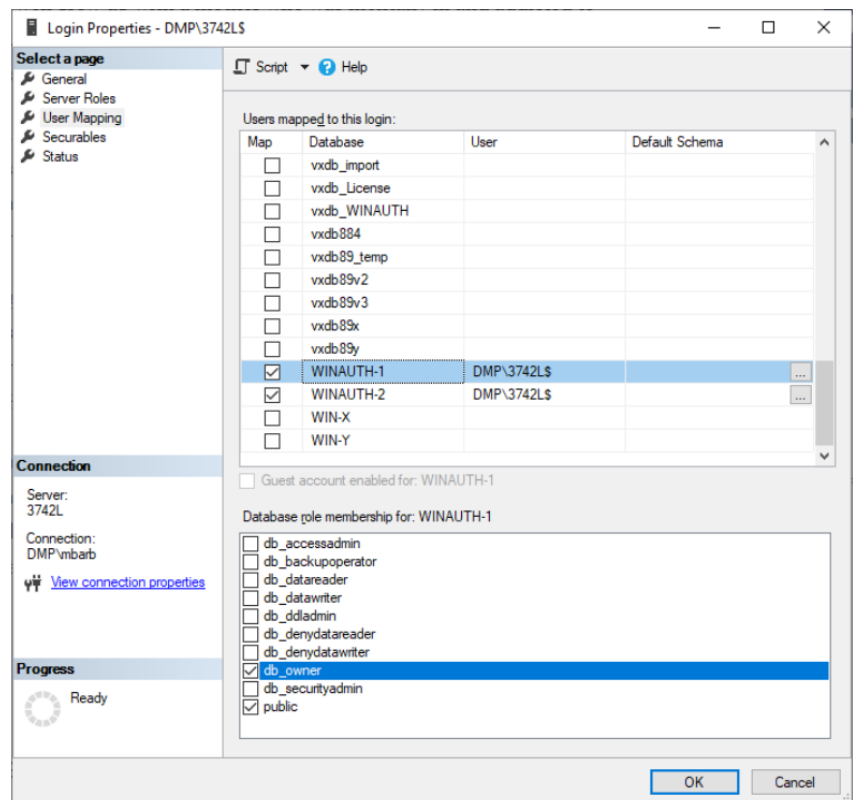


Figure 12: Separate Machine Login Permissions

SCS-VR Viewer

There is a stand-alone Viewer for the SCS-VR that is included with the installation of the SCS-VR Server and may be installed on a separate machine using the same installer.

On the stand-alone machine, you must run the Configurator in order to talk to the primary or backup databases. This configuration must match what is in the SCS-VR Server configuration before opening the Viewer.

The Configurator and Viewer must run as a Windows administrative level user.

The screenshot shows the SCS-VR Configurator window. At the top, there are two checked options: "UL Fire Enabled" and "Use Secondary Database". Below these are two columns of configuration fields. The left column is labeled "Primary Database Configuration" and the right column is labeled "Secondary Database Configuration". Each column contains five fields: "Database name:", "Database server name:", "Database port number:" (with a dropdown menu set to 1433), "Database username:", and "Database password:". At the bottom of the window is a "Control Panel" with several buttons: "Test Connection", "Check Version(s)", "Upgrade Version(s)", "Replicate data", "Save", "Quit", and "Clear Status Window".

Figure 13: Windows Administrative Level User

Once the Configurator has been set up, you may open the Viewer.

The screenshot shows the SCS-VR Viewer window. At the top is a menu bar with "File", "Language", and "Help". Below the menu bar are tabs for "Message Log", "Panels", "Groups", "Automation", and "Configuration". The "Message Log" tab is active. It features a "Receiver Group:" dropdown menu set to "All Receiver Groups", an "Account Numbers:" text box, and a "Filters" section with five checked checkboxes: "Non-Check-in Message", "Check-in Message", "Decryption Failed", "Unrecognizable Message", and "Panel IP Changed". There is also a "Stop Scrolling" checkbox which is unchecked. Below the filters is a table with the following data:

Server	Group	Account	Type	Time	Message	Acknowledge...
Regression n...	1 - 200000000...	157	Non-Check-in Me...	2023-10-24 01:40:37	800001Za\024\t "PN\z 744\744\	
Regression n...	1 - 200000000...	157	Non-Check-in Me...	2023-10-24 01:40:37	800001Za\024\t "PN\z 743\743\	

Figure 14: Open the SCS-VR Viewer

Updating SCS-VR

Step 1: Install the Updated Software

Go to dmp.com/software_downloads to download the updated software.

1. Select the latest version of SCS-VR in the downloads list.
2. Select the appropriate installation for your system.
3. Complete all of the fields in the graphic below.



Note: In the **Serial** field, enter your license key. The license key can be found on the **Configuration** tab in the **Setup Console**.

The form is titled "Serial Check For SCS-VR (64 Bit)". It contains a message: "Please enter your serial number below and click proceed to download the update." Below the message are four input fields labeled "Serial:", "First Name", "Last Name", and "Email". At the bottom of the form is a "Submit" button.

Figure 15: Serial Check

4. Press **Submit**. The update download will begin.
5. In the **SCS-VR Setup Console**, select **Stop Service**.


The screenshot shows the "SCS-VR Setup Console" window. The "Configuration" tab is selected. The "Server Configuration" section includes fields for "Server Name", "License Key" (containing "509F-A05B-640D-4161-5C56-280F"), "Service Code", and "Service Code". The "Database Configuration" section includes fields for "Database Name" (scsvr), "Host Address" (scsvrloop), "Port (Default 1433)" (1433), "Username" (sa), and "Password" (masked). The "Backup Database Configuration" section includes fields for "Backup Database Name", "Backup Host Address", "Backup Port (Default 1433)", "Backup Username", and "Backup Password". Below these sections are checkboxes for "Enable trap checking", "Process Check-In Zero", and "Send Stored Messages". The "Service and Database Control" section has "Start Service" and "Stop Service" buttons. A black arrow points to the "Stop Service" button with the text "Select Stop Service". The status bar at the bottom indicates "SCS-VR Service is currently running." and "Log Configuration: C:\Program Files\SCS-VR\logging.conf".

Figure 16: Stop Service

6. Close the **Setup Console**.
7. Right-click on the installer and select **Run as administrator**. The installer will detect that the VR has been previously installed and prompt you to update the existing installation or choose no to install to a different directory.

8. Select **YES**, updating the existing installation. Select **Next** to continue.
9. Accept the license agreement and select **Next**.
10. Select **Next** to continue.
11. If the service was not stopped and the console was not closed, the updater notifies you. If you close the console and select **Retry** to continue, the updater will stop the service and continue. If you select **NO**, the update will stop.
12. If you chose to retry, the updater will copy JAR files over the previous installation and then display the license key for verification. Select **Next** to continue.
13. Select **Finish** when the updater notifies you that it has finished installing SCS-VR on your server.

Step 2: Test the Connection

1. Run the Configurator as administrator.
2. Select **Test Connection**. After you receive a response, select **Check Version** and when that response is returned, you will select **Upgrade Version(s)**.
3. Select **Save** and the GUI will prompt you to save the settings to the registry.
4. Select **YES**.
5. Select **QUIT**.
 **Note:** When you save and quit the database utility, the SCS-VR console launches and the SCS-VR service restarts.
6. Acknowledge any pending messages and verify the configuration of groups and automation connections.

Upgrade Process for Recommended Configuration

In the recommended production configuration for the SCS-VR, there is a primary and backup SCS-VR, each utilizing a shared primary and backup database. Refer to Figure 11.

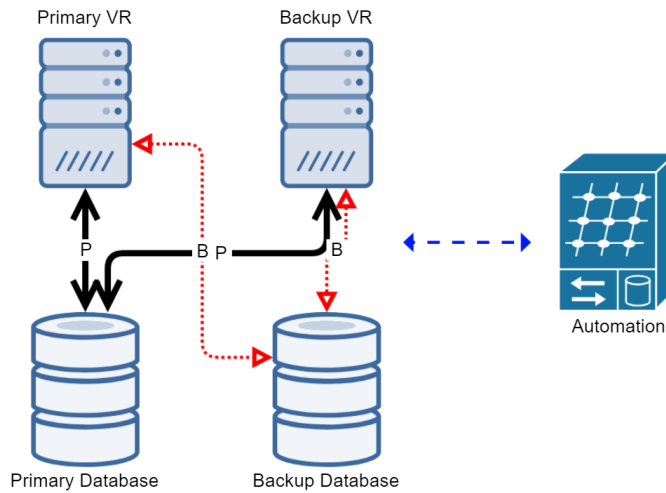


Figure 17: Recommended Configuration

To use this upgrade process, this configuration must be in place and working at the time of upgrade. If you are unsure if you meet these requirements, please contact DMP Technical Support before attempting any upgrades.

Stage 1

1. Redirect traffic on the backup SCS-VR to the primary SCS-VR. Alert users that an update is occurring. Contact your network administrator for assistance.
2. Stop service on the backup SCS-VR.
3. Run the installer as administrator.
4. When **Database Configurator Utility** comes up, deselect **UL Fire Enabled** and **Use Secondary Database**.

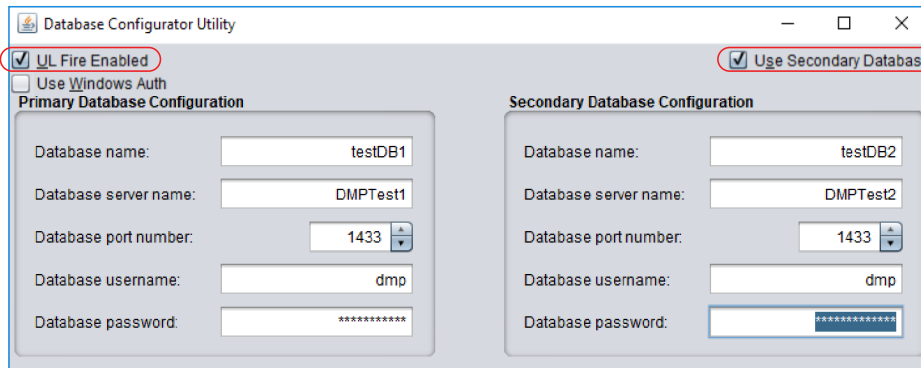


Figure 18: Database Configurator Utility

- Point the primary database at the original backup database. Remove all information for the primary database. **Secondary Database Configuration** will be empty, and your backup database information will be entered in as the primary and only information for a database connection. This separates the backup SCS-VR onto a closed segment, away from production traffic of the network. You can upgrade the backup database and backup SCS-VR first, while leaving your primary SCS-VR and primary database up and running to continue processing alarm signals. When completed, the Configurator shows changes similar to changes between Figure 12 and Figure 13.

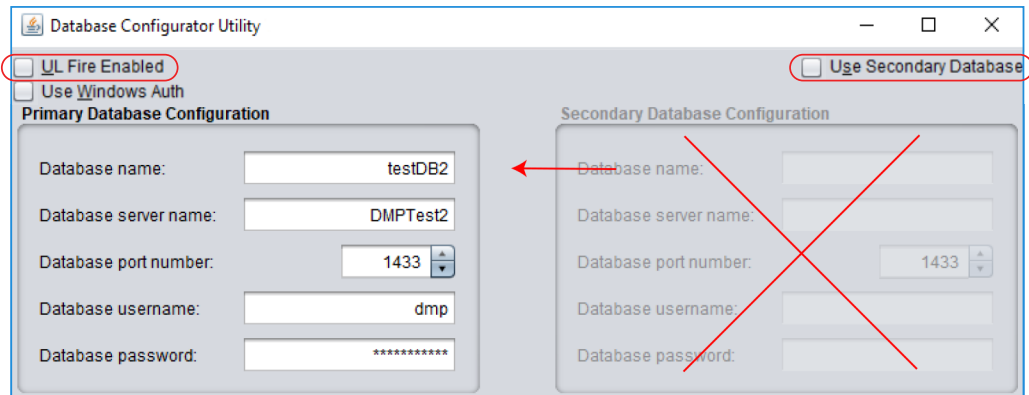


Figure 19: Remove Primary Database Information

- Once your database upgrade is complete and you have saved the changes, close the configurator to launch the **Setup Console**. Ensure the service is running and review your groups page to ensure all your groups are enabled and able to process signals.

Stage 2

You will upgrade the primary receiver and shift traffic to the backup receiver that has just finished its own upgrade during that process.

- Redirect all primary SCS-VR traffic to the backup SCS-VR. This includes NAT, Port Routing, etc. Contact your network administrator for assistance.
- Stop the service on the primary SCS-VR.
- Run the installer as administrator.
- When prompted, keep the database configurations the same for the primary SCS-VR.
- The primary database will update to the latest version, but the secondary database will not. The secondary database was already updated during stage 1.
- Save and close the Configurator. The **Setup Console** will launch.
- Confirm your **Groups** are enabled and that the service is running.
- On the primary SCS-VR, select **Swap to Backup Database**. This flips the database configuration so that the primary SCS-VR uses the old backup database as the new primary database. The original primary database is now the backup. Once complete, ensure your **Groups** are enabled and properly processing signals.

Stage 3

- Stop the service on the backup SCS-VR.
- Run the Configurator as administrator.
- When the **Database Configurator Utility** comes up, select **UL Fire Enabled** and **Use Secondary Database**.
- Fill in the **Secondary Database Configuration** fields with the information for the original primary database.
- Select **Test Connection**.
- Save your settings and exit.
- In the **Setup Console**, confirm that the database information has been stored correctly.
- Ensure final configuration on both SCS-VRs looks like the following: The primary SCS-VR should have the same primary database and the backup SCS-VR should have the same backup database.

Each successive upgrade in the future will see your Primary and Backup databases swap roles as the upgrade completes and you complete your new environment setup.

Upgrade Process for Non-Existing Backup Database

Before Installing the Upgrade

1. Redirect all the backup SCS-VR traffic to the primary SCS-VR. This includes NAT, Port Routing, etc. Contact your network administrator for assistance.
2. Stop the service on the backup SCS-VR. Use the **Database Configurator Utility** to change the primary database to database 2. Start the service again to confirm operation.
3. Navigate to **SQL Management Studio**. Check that the backup SCS-VR has its own UUID in the Servers table of database 2. **Select * from Servers** and **Select * from ServerGroups** to confirm. Each Server should have its own entry in the Servers table in the primary database. There should be matching entries in the secondary database. If both databases do not have matching entries, contact DMP Technical Support for assistance.
4. Stop the service on the backup SCS-VR. Rename SCS-VR file folder to **SCS-VRbkp** once service is stopped to create an immediate restore point.

Installing the Upgrade

1. Install the latest SCS-VR version on the backup SCS-VR. When prompted, upgrade the database as well. Once complete, start the service.
2. Restore any previous panel traffic to the backup SCS-VR. Use network manipulation or panel failover. Contact your network administrator for assistance.
3. Shift all primary SCS-VR traffic to the backup SCS-VR. This includes NAT, Port Routing, etc. Contact your network administrator for assistance.
4. Stop the service on the primary SCS-VR. Rename SCS-VR file folder to **SCS-VRbkp** once service is stopped to create an immediate restore point.
5. Install the latest SCS-VR version on the primary SCS-VR. When prompted, upgrade the database as well. Once complete, start the service.
6. Once both SCS-VR's and databases have been fully upgraded, enter database 2 as backup for the primary SCS-VR. This establishes the primary/backup database failover relationship.
7. Establish database 1 as backup for the backup SCS-VR. This prepares the backup SCS-VR to establish synchronization of both SCS-VR servers using the same primary and backup databases.
8. On the backup SCS-VR, failover the database from database 2 to database 1. Do this by navigating to the **Setup Console** and selecting the **Configuration** tab, then selecting **Swap Database**.

Both the primary SCS-VR and the backup SCS-VR application servers are upgraded to the latest versions as well as the databases. The primary SCS-VR and the backup SCS-VR should both use database 1 as the primary database and database 2 as the backup database.

Upgrade Process for SCS-VR with Full Disaster Recovery

In the recommended production configuration for the SCS-VR, there is a Primary and Backup SCS-VR, each utilizing a shared Primary and Backup Database. Refer to Figure 14.

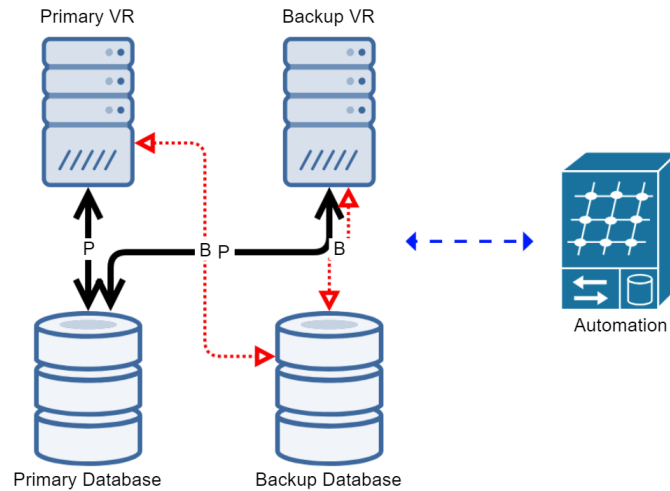


Figure 20: Recommended Configuration

In some environments, additional redundancy is required, and therefore a Disaster Recovery build would be utilized. The process and layout for this environment is very simple, as you simply replicate the original build in a new environment. Refer to Figure 15

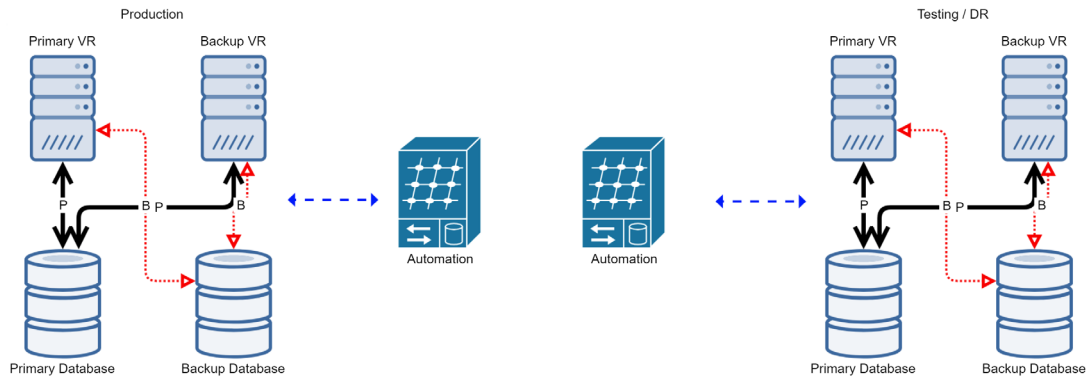


Figure 21: Recommended Environment

Back up all databases immediately prior to upgrade. Apply all necessary Windows updates and patches at least 48 hours prior to upgrade.

If you are unsure you meet configuration requirements, contact DMP Technical Support before attempting any upgrades.

Upgrade Processes

There are two possible upgrade processes with this build depending on how it is configured.

If you have active production traffic going to both environments, use “Upgrade Process for Recommended Configuration” for both environments.

If you do not have active production traffic going to the Testing/DR environment, you can upgrade the entire Test Environment and then follow the “Upgrade Process for Recommended Configuration” in the Production environment.



Designed, engineered, and
manufactured in Springfield, MO
using U.S. and global components.

LT-1135 1.04 23483
© 2023

INTRUSION • FIRE • ACCESS • NETWORKS

2500 North Partnership Boulevard
Springfield, Missouri 65803-8877

800.641.4282 | DMP.com