

Viewpoint™ Database Security Guide

Application Version: 7.0
August 19, 2026

© 2021 Conduent, Inc. All rights reserved. Conduent and Conduent Agile Star are trademarks of Conduent, Inc. and/or its subsidiaries in the United States and/or other countries.

Other company trademarks are also acknowledged.

Document Version: 7.0 (October 2021).

Document Conventions

Convention	Explanation
Bold	For file names, commands, fields, menus, options, and window names.
<code>Courier New</code>	Commands as you should type them.
<code>Lucida Console</code>	Example output generated by the system.
<i>Italics</i>	For configuration variables, including variable portions of file names and URLs. Also indicates a document name.
Note / Blue Callout	The Blue Callout text indicates information that is of special interest or importance, an idea that could be useful or additional information about a product or a feature.
	The Caution icon along with the text indicates actions that can lead to problems in system operation or configuration settings if the instructions are not followed properly.

Document Revision History

This section tracks the initial creation of the document after each major version thereafter.

Ver:	Date	Description	Reviewed / Approved By
1.0	Oct 16, 2012	Initial Release	Team
1.1	Oct 6, 2021	Rebranded adhering to the latest Conduent brand central documentation standards/guidelines.	Technical Writer

Table of Contents

1. Database Security Guide.....	1-1
1.1. Overview.....	1-1
1.1.1. Viewpoint Database Roles.....	1-1
1.1.2. Viewpoint Database Logins.....	1-1
1.2. Implementation.....	1-2
1.2.1. Named Pipes.....	1-2
1.2.2. Database Administrators.....	1-2
1.2.3. Database Creation User.....	1-2
1.2.4. Viewpoint Application Login.....	1-3
1.2.5. Intra-Server Link Login.....	1-4
1.2.6. Review Workflow Login.....	1-6
1.3. Ongoing Maintenance.....	1-6

1. Database Security Guide

1.1. Overview

This document establishes the types of database logins used in a Viewpoint deployment, provides instructions on how to set up these Logins and provides information about ongoing security-related maintenance. Viewpoint leverages Active Directory for some logins, MS SQL Authentication for others. Viewpoint makes use of Server Links and typically requires Named Pipes.

1.1.1. Viewpoint Database Roles

There is one database role – ‘VP_USER’. This role grants the permissions necessary to operate Viewpoint successfully. A role named VP_USER is part of all Viewpoint databases.

1.1.2. Viewpoint Database Logins

Login	User	Permissions
Database Administrator	Database administrator	sysadmin
Database Creation Login	Certificate (cannot log in)	sysadmin
Viewpoint Application Login	All Viewpoint application users	VP_USER role
Intra-Server Link Login	Cross-server operations	VP_USER role
Review Workflow Login	Some Viewpoint Review users	VP_USER role

1.1.2.1. Database Administrators

A Database Administrator is a special login which has full permission to Viewpoint databases. Their purpose is to perform product installations / upgrades and to perform maintenance tasks (index rebuilds, etc.). This login should not be given a Viewpoint application account. Aside from ensuring that Database Administrator(s) have sysadmin rights, Viewpoint imposes no additional rules or requirements. As with any sysadmin user this username/password for this/these users should be kept in confidence.

1.1.2.2. Database Creation Login

This is a “certificate login,” (as opposed to an MS SQL Login) which is utilized during database creation. Because this is a certificate login it is not possible to log in as this user. This login is part of a scheme to temporarily escalate permissions during database creation so that permission-sensitive operations can be performed inside of the database creation stored procedure. The database creation stored procedure is digitally signed. Any alteration of the database creation procedure will invalidate its digital signature, breaking its link to the database creation login. There is no other use for the database creation login. There is one database creation login for each ‘master’ database on a Viewpoint database server instance.

1.1.2.3. Viewpoint Application Login

Viewpoint Application Logins are given access to Viewpoint database assets through the VP_USER role. The Viewpoint best practice is to either create a Viewpoint-specific Active Directory group, or nominate an existing Active Directory group, and create a Login for the group. It is possible to create dedicated MS SQL Logins as application logins, for instance to support remote users.

1.1.2.4. Intra-Server Link Login

The Viewpoint Review and Processing servers have Server Links which connect these servers to each other. A dedicated MS SQL Login is required for each of the database server instances. This Login will have the same name on all servers in an environment. This Login will be granted the VP_USER role on all Viewpoint databases.

1.1.2.5. Review Workflow Login

A dedicated login in the Viewpoint Processing database used to perform workflow operations in the Processing database on behalf of Review users. It is granted the VP_USER role on the Processing LDControl database only.

1.2. Implementation

This section contains instructions on how to set up all of the Viewpoint Database Logins. Typically this is the first step to perform on an installation, after the initial databases have been created.

It is assumed that you are familiar with general MS SQL security concepts and are comfortable working within MS SQL Management Studio. The setup of all users described in this guide must be performed by a database administrator.

1.2.1. Named Pipes

Viewpoint deployments require multiple instances of MS SQL Server (at least one for Review and at least one for Processing). MS SQL Server security requires that if you are using multiple MS SQL Server instances on a single computer, and the MS SQL Server instances will be communicating with any system that is not on the same computer, then MS SQL Server security feature “Named Pipes” will need to be enabled. Please consult with Microsoft documentation for the most up-to-date information on how to enable Named Pipes.

1.2.2. Database Administrators

Database administrators are not Viewpoint users. There are no Viewpoint-specific steps for setting up database administrators beyond your company's own best practices for what permissions a database administrator should have. Generally, this type of login will be a member of the sysadmin server role.

1.2.3. Database Creation User

When Viewpoint creates new databases the owner is changed to 'SA' so that the creating user (some Viewpoint Application User) will not have escalated ('owner') rights on the database. If you wish to nominate a user other than SA to be the owner of newly created databases you will need to alter master stored procedure 'LD_CreateProjectDB_SP', changing the last section to indicate your preferred user name.

The procedure for creating the user and signing the database creation stored procedure is as follows:

1. Produce a certificate to digitally sign the stored procedure. Log into your Processing SQL server as a user with sysadmin rights. Select database 'master'.
2. Open a new query window for database 'master'. Copy the following script into the query window. Change the password (highlighted) to something acceptable by your organization. Do not lose this password – it will be used later on in this process and during some maintenance tasks. Once the password has been changed execute the script.

```
CREATE CERTIFICATE VPDBCcreationCertificate
ENCRYPTION BY PASSWORD = 'configure me'
```

```
WITH SUBJECT = 'Certificate for database creation',
START_DATE = '20120101', EXPIRY_DATE = '20990101'
```

- Now that you have the certificate you need to create a Certificate Login. This is the Login which will be granted rights to create / exchange ownership of databases. Execute the following query to create the Certificate Login:

```
CREATE login dbcertlogin FROM CERTIFICATE VPDBCcreationCertificate
```

- Logins created from certificates or asymmetric keys are used only for code signing. They cannot be used to connect to SQL Server. That is to say, a malicious user cannot log in as this user even if they know the password of the certificate. Grant this login sufficient rights to create Viewpoint database (make this user a sysadmin) by executing the following query:

```
exec sp_addsrvrolemember dbcertlogin, sysadmin
```

- Now that you have a Certificate Login with sysadmin rights, sign the database creation stored procedure with this login's certificate. To do so, copy the following query into a query window, change the password, and execute the query:

```
ADD SIGNATURE TO [LD_CreateProjectDB_SP] BY CERTIFICATE
VPDBCcreationCertificate
WITH PASSWORD = 'configure me'
```

You now have a Certificate Login with rights to create (and reassign ownership of) new databases. It is not possible to sign additional stored procedures without knowing the password – please be sure to keep the password secure. If the database creation stored procedure ever changes you will need to re-sign the stored procedure (see above), as the act of changing the stored procedure will break the signature.

In MS SQL Management Studio this login appears under <server> | Security | Logins. Navigate to this login (“dbcertlogin”), right-click and select “Properties”. Note that the controls are grayed out and “Mapped to certificate” is selected.

Once this task is complete, perform the same steps on the ‘master’ database of the Review SQL Server. The stored procedure is slightly different on the Review server, but has the same name and the same rules apply. You may use the same password, or you may choose to use a different password.

1.2.4. Viewpoint Application Login

All users of Viewpoint applications require a Viewpoint Application Login. Typically Logins are created for Active Directory groups to minimize Viewpoint-specific maintenance requirements. A Viewpoint Application Login is granted the VP_USER role on all Viewpoint databases in their environment. These databases are:

Processing SQL Server instance:

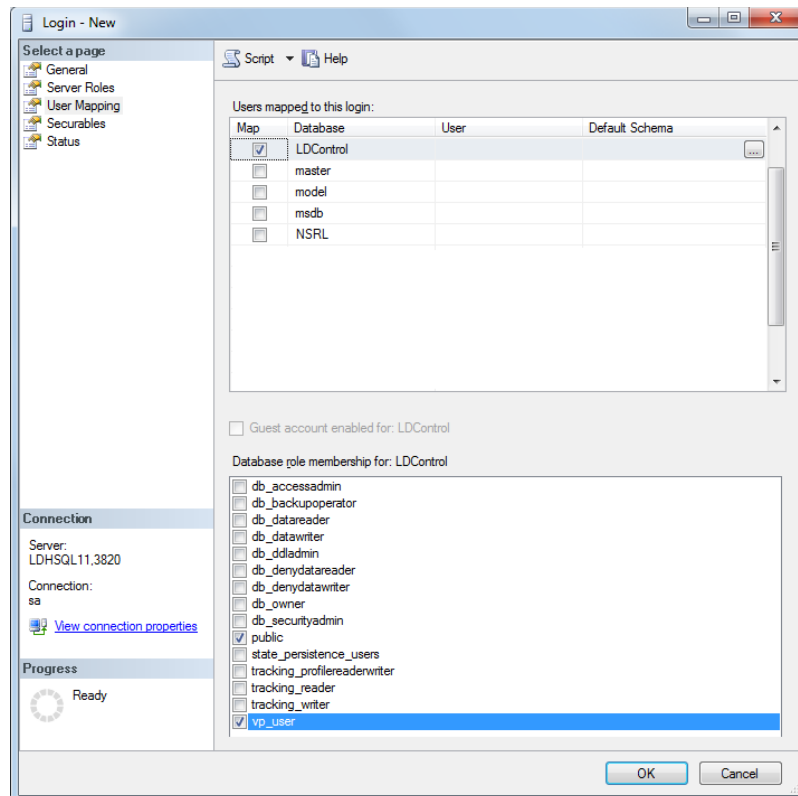
- MASTER
- MODEL
- LDControl
- NSRL
- All Viewpoint project databases (if any Viewpoint projects have been created)

Review SQL Server instance:

- MASTER
- MODEL
- LDControl
- All Viewpoint project databases (if any Viewpoint projects have been created)

The process for granting access to the Login is as follows:

1. Using MS SQL Management Studio, log in to the Processing server instance.
2. Create an MS SQL Login, or locate an existing MS SQL Login.
3. Right-click the Login and select Properties. The Login Properties dialog appears.
4. Select the User Mapping side-bar item.
5. In the top grid is a list of databases. In the bottom grid is a list of roles. Typically the first database in the top grid is LDControl. Checkmark the LDControl database, then checkmark role VP_USER in the bottom grid.



1. Checkmark the other Processing databases, being sure to select the VP_USER role for each. The databases to checkmark are master, model, LDControl, NSRL and any project databases if you have any.
2. Click OK, to commit your changes.
3. Repeat these steps for all Viewpoint Application Logins, if you have more than one. Once this task is complete, perform these same steps on the Review MS SQL Server instance. Note that the Review SQL Server does not have an 'NSRL' database.

1.2.5. Intra-Server Link Login

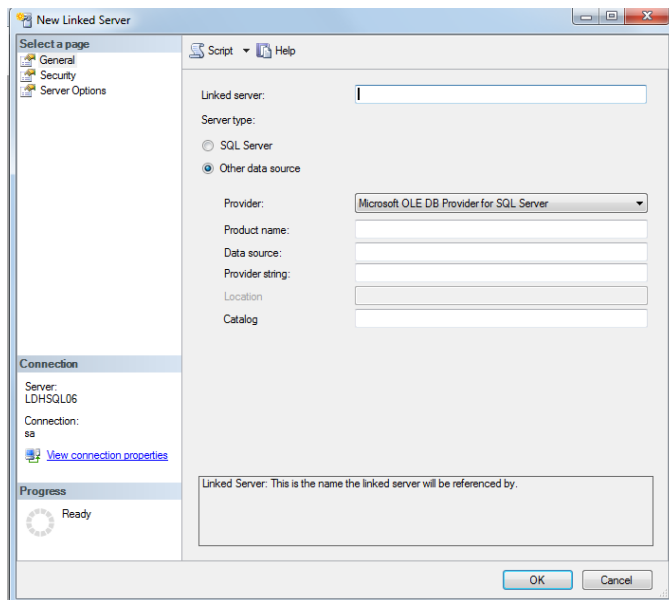
Viewpoint requires the use of MS SQL Server Links. The Intra-Server Link Login is a dedicated Login used to provide authentication when performing operations over server links. The following steps outline the setup of the Intra-Server Link Login and the Server Links themselves.

1. Using MS SQL Management Studio, log in to the Processing server instance.
2. In the main tree select <server name> | Security | Logins. Right-click "Logins" and select "New Login...". The New Login Dialog appears.

3. Checkmark SQL Server Authentication. Name the login VPLink. Select a password which complies with your corporate passwords standards. Uncheck "User must change password at next Login." If you choose to use a password policy which expires passwords after a certain timespan note that the processing and review versions of VPLink, as well as the server link login credentials, will need to be changed at the same time.
4. Click the "User Mapping" side-bar item.
5. In the top grid is a list of databases. In the bottom grid is a list of roles. For each of the following databases checkmark the database name in the top grid and the corresponding "VP_USER" role in the bottom grid:
6. Model
7. LDControl
8. All project databases (if present).
9. Click OK, to create the login.
10. Repeat these steps on the Review server instance.

At this point you have created VPLink on both Processing and Review and have granted the login the VP_USER role on most of the Viewpoint databases (VPLink does not need access to NSRL). Create a "Linked Server" link from the Processing SQL Server to the Review SQL Server. To create a Linked Server:

1. Using MS SQL Management Studio, log in to the Processing server instance.
2. Locate Server Objects | Linked Servers in the main tree. Right-click the Linked Servers node and select "New Linked Server...". The New Linked Server Dialog appears.



3. Enter the name of the Review SQL Server instance into the "Linked server" box. Do not use an IP address – use the domain name of the server instance.
4. Checkmark radio button "SQL Server".
5. Click the "Security" side-bar item. Select "Be made using this security context:." Type the username and password of the Intra-Server Link Login (VPLink) into the username and password boxes.
6. Click the "Server Options" side-bar item. Locate the items "RPC" and "RPC Out". If they are not already set to True set them to True.
7. Click OK, to create the new link.

- Open a new query window. Enter the following query, replacing the highlighted section with the name of the target server, and execute the query. If the query returns successfully (you'll receive a number) then the link has been set up properly. Otherwise, return to the Server Link dialog and resolve the error.

```
select count(*) from [instance name].[LDControl].[dbo].[Project]
```

- Perform these same steps again on the Review server. In the case of the Review server link it should point to the Processing server.

1.2.6. Review Workflow Login

The Workflow Login is created on the Processing database. It is used by Viewpoint Review to initiate certain jobs that run on the (Processing) Workers. Setup is as follows:

- Using MS SQL Management Studio, log in to the Processing server instance.
- In the main tree select <server name> | Security | Logins. Right-click "Logins" and select "New Login...". The New Login Dialog appears.
- Select "SQL server authentication". In the Login name box enter "ReviewWorkflowLogin." Enter a password. Remember the password – you will need it when it comes time to configure Viewpoint Review. Uncheck "User must change password at next Login."
- Click the "User Mapping" side-bar item. In the top grid locate and checkmark LDControl. In the bottom grid locate and checkmark VP_USER.
- Click OK, to create the login.

1.3. Ongoing Maintenance

The following events will occur during the lifetime of your installation which will require security maintenance on your part:

- A new Active Directory Group is to be granted access to Viewpoint
- The new group is to be granted the VP_User role in all applicable databases.
- Alteration of the Database Creation Stored Procedure

From time to time it is useful to alter the settings in the database creation stored procedure (Master. LD_CreateProjectDB_SP). When this stored procedure is changed the digital signature applied to it becomes invalid. If the signature is made invalid, your users will no longer be able to perform the power-user operations required when creating a new database (and changing its owner) and all such operations will fail with security-related error messages.

To determine if the signature on the stored procedure is valid, right-click the stored procedure and select, Properties. In the grid there will be a "Signatures" section:

Recompile	False
 Signatures	
VPDBCcreationCertificate	SIGNATURE BY CERTIFICATE

Note: If this section is not present, then there is not a valid signature on the stored procedure.

If the stored procedure is invalid, you will need to re-sign it. Elsewhere in this document is the command to add a signature to the stored procedure. If you have forgotten the password, the next best recourse is to remove the certificate / certificate login and start the process of securing the database creation stored procedure again. To this end, you will need to remove the login (dbcertuser) and the certificate (VPDBCcreationCertificate). If the Database Creation Stored Procedure is still signed by the certificate, modify the Database Creation Stored Procedure (for example, add a space, etc.) to break the signature (otherwise you cannot delete the certificate).

Once completed, re-run the commands in this document for creating the certificate, creating a certificate login, signing the certificate and granting the login sysadmin rights.