Genesys Interaction Recording Solution Guide

Automated Recovery of Recordings

4/23/2025

Contents

Automated Recovery of Recordings

> **Important**
>
> The Lost Voice Recording (LVR) Recovery Script is not required when using the Voice Processor instead of the Recording Processor Script (RPS).

Starting with GIR release 8.5.216.01, the GIR solution provides automated recovery of recordings that have not been successfully posted for various reasons. The Lost Voice Recording (LVR) Recovery Script automatically goes through these recordings and recovers them. This means completing the posting process of the recordings: posting metadata to Recording Processor Script (RPS) and recordings to WebDAV (in the case of a Media Control Platform machine), and/or posting metadata to Interaction Recording Web Services (RWS) and SpeechMiner Interaction Receiver (in the case of a Recording Processor Script machine).

Some of the reasons that recordings processed by Media Control Platform (MCP) and RPS fail to be posted include:

- The recording storage is not available and MCP cancels the upload process.
- The RPS is not available and MCP does not send metadata to RPS.
- The RPS URL and credentials were incorrectly entered in the IVR Profile. As a result, MCP cannot send metadata to RPS.
- Storage credentials were incorrectly entered in the IVR Profile, causing MCP to fail to upload to WebDAV.
- SpeechMiner Interaction Receiver credentials were incorrectly configured in the IVR Profile.

Recoverable and Unrecoverable Recordings

The LVR Recovery Script categorizes each recording as recoverable or unrecoverable. A recording is considered unrecoverable if any of the following is true:

- The metadata cannot be parsed.
- The LVR Recovery Script cannot find the information it needs to recover the recording within the metadata.
- If recovering for MCP, if a recording is missing metadata or a media file.
- If recovering for MCP and the media file is encrypted, the encryption key is missing.

The LVR Recovery Script attempts to upload unrecoverable recordings to the unrecoverable storage specified in the properties file. Genesys recommends that you monitor the unrecoverable storage location and investigate these recordings to determine what caused the problem.

The LVR Recovery Script attempts to recover recoverable recordings using their IVR Profile and metadata.

> **Important**
> Automated recovery of Genesys Interaction Analytics (GIA) recordings is currently not supported.

Installing LVR Recovery Script

The LVR Recovery Script must be installed on each machine where MCP and/or RPS run. If installing the LVR Recovery Script for both MCP and RPS components (where both components are installed on the same machine), select both components during installation. In the LVR Recovery Script installation directory, there are two configuration files—for recovering recordings for MCP and for recovering recordings for RPS.

Installing on Linux

To install the LVR Recovery Script on Linux, complete the following steps:

1. Perform one of the following:
   - For LVR version 8.5.222.58 (or higher), install Java 17 . You can use the OpenJDK version of the software.
   - For LVR version 8.5.222.55 (or lower), install Java 8. You can use the Oracle or OpenJDK version of the software.

   Note: Genesys recommends using the latest supported version of Java and deprecating any previous versions. See the Genesys Interaction Recording page in the *Genesys Supported Operating Environment Reference* for more details about supported versions.
2. In the directory to which the LVR Recovery Script installation package was copied, locate a shell script called **install.sh**.
3. Run this script from the command prompt by typing **sh** and the file name. For example: **sh install.sh**.
4. When prompted, schedule when you would prefer the LVR Recovery Script to run throughout the day, by entering a comma-separated line of text containing all the times of the day in 24-hour format. For example: 00:30,12:30,01:25. This will schedule the LVR Recovery Script to run every day at 12:30 AM, 12:30 PM, and 1:25 AM. Use a leading zero for a single-digit hour (01:25 instead of 1:25).
5. Configure the LVR Recovery Script.

Installing on Windows

To install the LVR Recovery Script on Windows, complete the following steps:

1. Perform one of the following:
   - For LVR version 8.5.222.58 (or higher), install Java 17 . You can use the OpenJDK version of the software.
   - For LVR version 8.5.222.55 (or lower), install Java 8. You can use the Oracle or OpenJDK version of the software.

   Note: Genesys recommends using the latest supported version of Java and deprecating any previous versions. See the Genesys Interaction Recording page in the *Genesys Supported Operating Environment Reference* for more details about supported versions.
2. In the directory to which the LVR Recovery Script installation package was copied, locate and double-click **Setup.exe** to start the installation.
3. When prompted, schedule when you would prefer the LVR Recovery Script to run throughout the day, by entering a comma-separated line of text containing all the times of the day in 24-hour format. For example: 00:30,12:30,01:25. This will schedule the LVR Recovery Script to run every day at 12:30 AM, 12:30 PM, and 1:25 AM. Use a leading zero for a single-digit hour (01:25 instead of 1:25).
4. Configure the LVR Recovery Script.

Upgrading LVR Recovery Script

To upgrade the LVR Recovery Script, complete the following steps:

1. Back up the **MCP_premise.properties** and **RPS_premise.properties** files.
2. Uninstall the existing version of the LVR Recovery Script.
3. Install the new version of the LVR Recovery Script.
4. Replace the generated **MCP_premise.properties** and **RPS_premise.properties** files with the backup files.

Rescheduling When LVR Recovery Script Runs

To reschedule when the LVR Recovery Script runs each day, reinstall the LVR Recovery Script or manually edit the system's scheduled tasks.

Reinstalling LVR Recovery Script

To reinstall the LVR Recovery Script:

1. Back up the **MCP_premise.properties** and/or **RPS_premise.properties** files by moving them to another directory.
2. Uninstall the LVR Recovery Script.
3. Reinstall the LVR Recovery Script and enter the new scheduling of the LVR Recovery Script.
4. Replace the generated **MCP_premise.properties** and/or **RPS_premise.properties** files with the backup files.

Editing scheduled tasks on Linux

To edit scheduled tasks on Linux:

1. Edit the crontab by running the command: `crontab -e`.
   Each line in the crontab has the following format:

   ```
   minute   hour   day   month   dayofweek   command
   ```

   The first five numbers are when the command will be run. An asterisk (*) means the script is to be run at every instance (every hour, every weekday, and so on) within the time period. The scheduled runs of the LVR Recovery Script are the lines in the crontab that have the following command:

   ```
   java -jar <LVR_install_directory>/recover_LVRs.jar --mode recover --component <component>
    --properties <LVR_install_directory>/<component>_premise.properties
   ```

2. Change the schedule of those lines by editing one or any of the following: `minute, hour, day, month,` or `dayofweek`.
3. Delete a scheduled run by deleting its corresponding line.

For more information about editing the crontab, refer to Linux documentation.

Editing scheduled tasks on Windows

To edit scheduled tasks on Windows:

1. Open the Task Scheduler.
2. Click the Task Scheduler Library on the left. You should see all scheduled tasks.
3. The LVR Recovery Script schedules its runs with the name **IntRcLVRRSPrem64_MCP** for MCP recoveries and **IntRcLVRRSPrem64_RPS** for RPS recoveries.
4. To edit the scheduled task, right-click the task and click **properties**. Go to the **triggers** tab to edit when the task should run.
5. To delete the scheduled task, right-click the task and click **delete**.

Configuring LVR Recovery Script

Configure the LVR Recovery Script in its installation directory. If the LVR Recovery Script is to be used for both MCP and RPS on the same machine, the two different properties files must both be configured.

For MCP, you must configure the following:

- WebDAV storage connection
- Configuration Server connection

For RPS, you must configure the following:

- RWS connection

The following connections can be configured to use TLS:

- Configuration Server
- Recoverable WebDAV for a Tenant
- Unrecoverable WebDAV for a Tenant
- Recording Processor Script
- Interaction Recording Web Services
- SpeechMiner Interaction Receiver

Configuring WebDAV Storage Connection for MCP

You must configure WebDAV if you are using MCP.

Recoverable recordings are uploaded to a WebDAV URL (specified in the recording metadata) using the IVR Profile specified in the configuration environment. No configuration is needed except for ensuring the LVR Recovery Script can communicate with Configuration Server to retrieve IVR Profiles and that the WebDAV server is running.

For unrecoverable recordings, the WebDAV URLs and credentials for each tenant must be specified in the **MCP_premise.properties** file. To specify a tenant's WebDAV information for unrecoverable recordings:

1. Open **MCP_premise.properties**.
2. Add the tenant's name to **lvrrecovery.webDAV.tenants**. Each additional tenant is separated by a comma. The tenant names specified in this file must match the tenant names in the metadata of the corresponding unrecoverable recording.
   Example: `lvrrecovery.webDAV.tenants=tenant1,tenant2,tenant3`
3. Specify the tenant's WebDAV URL under `lvrrecovery.webDAV.<tenantname>.unrecoverable.url`. The directory must already exist or be manually created before running the LVR Recovery Script.

   > **Important**
   > If the tenant's WebDAV URL does not point to a directory in WebDAV, the LVR Recovery Script does not create the directory and, as a result, the unrecoverable recordings will not be uploaded.

4. Specify the tenant's WebDAV username under

`lvrrecovery.webDAV.<tenantname>.unrecoverable.username`.

5. Specify the tenant's WebDAV password under `lvrrecovery.webDAV.<tenantname>.unrecoverable.password`.
6. Create a tenant with the name `UNKNOWN`. It will be used for uploading unrecoverable recordings when the tenant information cannot be recovered.

If a tenant's unrecoverable information is not specified, the LVR Recovery Script does not attempt to upload the unrecoverable recording and the unrecoverable recording will remain in the folder for failed recordings. The recoverable recordings for that tenant will be recovered normally.

Use the following optional properties to configure the maximum number of tolerated upload failures during a recovery for a tenant to WebDAV, as follows:

- **lvrrecovery.webDAV.<tenantname>.unrecoverable.maxToleratedwebDAVFailures**—specifies the maximum tolerated upload failures for the WebDAV server specified in **lvrrecovery.webDAV.<tenantname>.unrecoverable**. If the number of failures exceeds the threshold for a tenant, the LVR Recovery Script stops uploading unrecoverable recordings for this tenant during this run and will try again in the next run.
- **lvrrecovery.webDAV.<tenantname>.recoverable.maxToleratedwebDAVFailures**—specifies the maximum number of tolerated upload failures for the recoverable WebDAV server. The recoverable WebDAV server is the WebDAV server specified in a tenant's IVR profile and a recording's metadata. If the number of failures for a particular WebDAV server exceeds the threshold for a tenant, the LVR Recovery Script stops uploading recoverable recordings for this tenant to the specific WebDAV server during this run and will try again in the next run.

A tenant must be specified in **lvrrecovery.webDAV.tenants** for any related tenant properties for that tenant to work.

Secure connections to WebDAV storage are supported over HTTPS.

Configuring Configuration Server Connection for MCP

These mandatory properties must be configured to run the LVR Recovery Script for MCP:

- **mcp.configserver.host**—The hostname for Configuration Server
- **mcp.configserver.port**—The port for Configuration Server
- **mcp.configserver.appname**— The application name for the Configuration Manager Object (by default, the value is **default**).
- **mcp.configserver.username**—The username to be used for Configuration Server
- **mcp.configserver.password**—The password to be used for Configuration Server

Configuring RWS Connection for RPS

If using the LVR Recovery Script for RPS, complete the following steps:

1. In the **RPS_premise.properties** file, set the mandatory **rp.htccuri** property to the RWS base URI. For example: `http://vagrant.genesys.com:8081`
2. Specify ops credentials for RWS by setting the **rp.opsUser** and **rp.opsPassword** properties in the **RPS_premise.properties** file.
3. (Optional) Configure the default Contact Center ID to be used when it cannot be determined from the metadata by setting the **rp.defaultccid** property in the **RPS_premise.properties** file.

Secure connections to RWS and SpeechMiner Interaction Receiver are supported over HTTPS.

Configuring Transport Layer Security (TLS) Connections (Optional)

The following sections explain how to configure TLS connections.

Configuring a TLS Connection to Configuration Server

1. Ensure that the Configuration Server port is properly configured as an auto-detect port.
2. In the **MCP_premise.properties** file, set the **mcp.configserver.port** property to the Configuration Server auto-detect port.
3. If required, modify the TLS version when connecting to Configuration Server using the **mcp.configserver.defaultTlsVersion** property in the properties file. Supported TLS versions are:
   - TLSv1.1—TLS version 1.1 (the default)
   - TLSv1.2—TLS version 1.2

Configuring a TLS Connection to Recoverable WebDAV for a Tenant

In the **MCP_premise.properties** file, configure the **lvrrecovery.webDAV.<tenantname>.recoverable.trustedCA** property for that tenant's recoverable WebDAV connection as follows:

- If the TLS certificate was issued by a well-known certificate authority such as VeriSign, set the **lvrrecovery.webDAV.<tenantname>.recoverable.trustedCA** parameter to `true`.
- If the TLS certificate was issued by your own certificate authority, set the **lvrrecovery.webDAV.<tenantname>.recoverable.trustedCA** parameter to the path to a file containing the certificate of the CA that generated the certificate. The file containing the certificate must be in PEM format.

> **Important**
>
> If there are intermediate certificate authorities forming a chain of trust, then use the certificate chain containing the intermediate CAs and root CA in PEM format.

- If the TLS certificate is a self-signed certificate, set the **lvrrecovery.webDAV.<tenantname>.recoverable.trustedCA** parameter to the path to the self-

signed certificate. The file containing the certificate must be in PEM format.

- If you do not wish to verify the TLS certificate and use TLS only for encrypted transmission, set the **lvrrecovery.webDAV.<tenantname>.recoverable.trustedCA** parameter to `false`. If verification is not configured, certificates will not be checked if they have expired or the server hostname is matching the certificate's common name or subject alternative name. However, certificates will be checked if they are signed with a strong signature algorithm. Newer Java Runtime Environment 7 versions and Java Runtime Environment 8 disallow MD5 signatures for certificates.

> **Important**
>
> The statement about JRE 7/8 disallowing MD5 signatures for certificates was relevant for Java 7/8 transitions. It is no longer applicable for latest Java versions.

Configuring a TLS Connection to Unrecoverable WebDAV for a Tenant

1. Edit the following files as appropriate:
   - **MCP_premise.properties**—if LVR Recovery Script is recovering recordings for MCP.
   - **RPS_premise.properties**—if LVR Recovery Script is recovering recordings for RPS.
2. Set the **lvrrecovery.webDAV.<tenantname>.unrecoverable.url** property in properties file to use the unrecoverable WebDAV https URL.
3. In the properties file, configure the **lvrrecovery.webDAV.<tenantname>.unrecoverable.trustedCA** property for that tenant's unrecoverable WebDAV connection as follows:
   - If the TLS certificate was issued by a well-known certificate authority such as Verisign, set the **lvrrecovery.webDAV.<tenantname>.unrecoverable.trustedCA** parameter to `true`.
   - If the TLS certificate was issued by your own certificate authority, set the **lvrrecovery.webDAV.<tenantname>.unrecoverable.trustedCA** parameter to the path to a file containing the certificate of the CA that generated the certificate. The file containing the certificate must be in PEM format.

     > **Important**
     >
     > If there are intermediate certificate authorities forming a chain of trust, then use the certificate chain containing the intermediate CAs and root CA in PEM format.

   - If the TLS certificate is a self-signed certificate, set the **lvrrecovery.webDAV.<tenantname>.unrecoverable.trustedCA** parameter to the path to the self-signed certificate. The file containing the certificate must be in PEM format.
   - If you do not wish to verify the TLS certificate and use TLS only for encrypted transmission, set the **lvrrecovery.webDAV.<tenantname>.unrecoverable.trustedCA** parameter to `false`. If verification is not configured, certificates will not be checked if they have expired or the server hostname is matching the certificate's common name or subject alternative name. However, certificates will be checked if they are signed with a strong signature algorithm. Newer Java Runtime

Environment 7 versions and Java Runtime Environment 8 disallow MD5 signatures for certificates.

> **Important**
>
> The statement about JRE 7/8 disallowing MD5 signatures for certificates was relevant for Java 7/8 transitions. It is no longer applicable for latest Java versions.

Configuring a TLS Connection to Recording Processor Script

In the **MCP_premise.properties** file, configure the **mcp.rpTrustedCA** property as follows:

- If the TLS certificate was issued by a well-known certificate authority such as Verisign, set the **mcp.rpTrustedCA** parameter to `true`.
- If the TLS certificate was issued by your own certificate authority, set the **mcp.rpTrustedCA** parameter to the path to a file containing the certificate of the CA that generated the certificate. The file containing the certificate must be in PEM format.

> **Important**
>
> If there are intermediate certificate authorities forming a chain of trust, then use the certificate chain containing the intermediate CAs and root CA in PEM format.

- If the TLS certificate is a self-signed certificate, set the **mcp.rpTrustedCA** parameter to the path to the self-signed certificate. The file containing the certificate must be in PEM format.
- If you do not wish to verify the TLS certificate and use TLS only for encrypted transmission, set **mcp.rpTrustedCA** to `false`. If verification is not configured, certificates will not be checked if they have expired or the server hostname is matching the certificate's common name or subject alternative name. However, certificates will be checked if they are signed with a strong signature algorithm. Newer Java Runtime Environment 7 versions and Java Runtime Environment 8 disallow MD5 signatures for certificates.

> **Important**
>
> The statement about JRE 7/8 disallowing MD5 signatures for certificates was relevant for Java 7/8 transitions. It is no longer applicable for latest Java versions.

Configuring a TLS Connection to Interaction Recording Web Services

1. In the **RPS_premise.properties** file, set the **rp.htccuri** property to use the Interaction Recording Web Services https URL.

2. In the **RPS_premise.properties** file, configure the **rp.rwsTrustedCA** property as follows:
   - If the TLS certificate was issued by a well-known certificate authority such as Verisign, set the **rp.rwsTrustedCA** parameter to `true`.
   - If the TLS certificate was issued by your own certificate authority, set the **rp.rwsTrustedCA** parameter to the path to a file containing the certificate of the CA that generated the certificate. The file containing the certificate must be in PEM format.

     > **Important**
     >
     > If there are intermediate certificate authorities forming a chain of trust, then use the certificate chain containing the intermediate CAs and root CA in PEM format.

   - If the TLS certificate is a self-signed certificate, set the **rp.rwsTrustedCA** parameter to the path of the self-signed certificate. The file containing the certificate must be in PEM format.
   - If you do not wish to verify the TLS certificate and use TLS only for encrypted transmission, set **rp.rwsTrustedCA** to `false`. If verification is not configured, certificates will not be checked if they have expired or the server hostname is matching the certificate's common name or subject alternative name. However, certificates will be checked if they are signed with a strong signature algorithm. Newer Java Runtime Environment 7 versions and Java Runtime Environment 8 disallow MD5 signatures for certificates.

     > **Important**
     >
     > The statement about JRE 7/8 disallowing MD5 signatures for certificates was relevant for Java 7/8 transitions. It is no longer applicable for latest Java versions.

Configuring a TLS Connection to SpeechMiner Interaction Receiver

In the **RPS_premise.properties** file, configure the **rp.speechminerTrustedCA** parameter as follows:

- If the TLS certificate was issued by a well-known certificate authority such as Verisign, set the **rp.speechminerTrustedCA** parameter to `true`.
- If the TLS certificate was issued by your own certificate authority, set the **rp.speechminerTrustedCA** parameter to the path to the CA that generated the certificate. The file containing the certificate must be in PEM format.

  > **Important**
  >
  > If there are intermediate certificate authorities forming a chain of trust, then use the certificate chain containing the intermediate CAs and root CA in PEM format.

- If the TLS certificate is a self-signed certificate, set the **rp.speechminerTrustedCA** parameter to the path to the self-signed certificate. The file containing the certificate must be in PEM format.
- If you do not wish to verify the TLS certificate and use TLS only for encrypted transmission, set the **rp.speechminerTrustedCA** parameter to `false`. If verification is not configured, certificates will not be checked if they have expired or the server hostname is matching the certificate's common name or subject alternative name. However, certificates will be checked if they are signed with a strong signature algorithm. Newer Java Runtime Environment 7 versions and Java Runtime Environment 8 disallow MD5 signatures for certificates.

> **Important**
>
> The statement about JRE 7/8 disallowing MD5 signatures for certificates was relevant for Java 7/8 transitions. It is no longer applicable for latest Java versions.

Configuration File Parameters

Parameter Name	Mandatory	Description	Example
http.connection.timeout	No	The HTTP connection timeout value. This property must be set in seconds. The default HTTP connection timeout value is 60 seconds.	10
http.socket.timeout	No	The HTTP socket timeout value. This property must be set in seconds. The default HTTP socket timeout value is 30 seconds.	10
lvrrecovery.failedfolder	Yes	The folder where failed recordings are stored. This property must be set to match the value in the **failed_folder_path** option in the **[processing]** section of the **rpconfig.cfg** file. If **failed_folder_path** is not set in the **rpconfig.cfg** file, the default value of **<Installation Directory>/RP/failed** is used.	<Installation Directory>/RP/failed
lvrrecovery.maxDirectoryRecurse	No	The maximum directory depth the LVR Recovery Script goes when recovering recordings. Default is a depth of 20.	10
lvrrecovery.timeout	No	The time period, in minutes, during which the LVR Recovery Script attempts to recover recordings. If the LVR Recovery Script does not	60

		finish the recovery within the specified timeout, it exits. If this property is not specified, the timeout is not used.	
lvrrecovery.startdate	No	The date for the LVR Recovery Script to ignore recovery of recordings older than this date. If the time period specified by this property and the **mcp.minimumRecordingAge** property overlaps, this property is ignored. The format of the parameter: YYYY/MM/DD.	2017/01/01
lvrrecovery.maxRetry	No	The number of times the LVR Recovery Script will retry recovering a failed recording if the initial recovery attempt fails. Default is 5 attempts.	10
lvrrecovery.log_dir	No	The directory in which the LVR Recovery Script writes its log files. By default, the log files are written in the installation directory.	<Installation Directory>/logs
mcp.configserver.host	Yes if recovering for MCP	The hostname for Configuration Server.	host.example.com
mcp.configserver.port	Yes if recovering for MCP	The port for Configuration Server.	8888
mcp.configserver.appname	Yes if recovering for MCP	The application name for Configuration Server.	default
mcp.configserver.username	Yes if recovering for MCP	The username for Configuration Server.	username
mcp.configserver.password	Yes if recovering for MCP	The password for Configuration Server.	password
mcp.configserver.defaultTlsVersion	No	The initial TLS version used to connect to Configuration Server over a secure port. Valid versions are TLSv1.1 (the default), TLSv1.2.	TLSv1.1
mcp.minimumRecordingAge	No	LVR Recovery Script ignores MCP recordings that are newer than this property. The time used is when the recording	30

		was written to a disk on this machine, not the start time on the metadata. This is to prevent files still being processed by MCP, to be attempted to be recovered. This property must be set in hours. Default is 24 hours.	
mcp.rpTrustedCA	No	Configures TLS certificate validation when making a secure outbound connection to Recording Processor Script (RPS). Valid values are `true`, `false`, or a path to a trusted certificate authority (CA) bundle. If set to `true`, the certificate is validated. If set to `false`, the certificate is not validated. The CA file must be in PEM format. LVR Recovery Script exits during initialization under the following conditions: the CA path does not exist, the CA file is not a valid PEM file, or the CA file is corrupted. This parameter is optional, and defaults to `false`.	`true`
rp.htccuri	Yes if recovering for RPS	The URI for the Interaction Recording Web Services node.	http://vagrant.genesys.com:8081
rp.opsUser	No	The admin username for Interaction Recording Web Services.	username
rp.opsPassword	No	The admin password for Interaction Recording Web Services.	password
rp.defaultccid	No	The default Contact Center ID (CCID) that the LVR Recovery Script uses when posting metadata if the CCID is unknown.	
rp.rwsTrustedCA	No	Configures TLS certificate validation when making a secure outbound connection to Interaction Recording Web Services (RWS). Valid values are `true`, `false`, or a path to a trusted certificate authority (CA) bundle. If set to `true`, the certificate is validated. If set to `false`, the certificate is not validated. The CA file must be in PEM format. LVR Recovery Script exits during initialization under the	`true`

		following conditions: the CA path does not exist, the CA file is not a valid PEM file, or the CA file is corrupted. This parameter is optional, and defaults to `false`.	
rp.speechminerTrustedCA	No	Configures TLS certificate validation when making a secure outbound connection to SpeechMiner Interaction Receiver. Valid values are `true`, `false`, or a path to a trusted certificate authority (CA) bundle. If set to `true`, the certificate is validated. If set to `false`, the certificate is not validated. The CA file must be in PEM format. LVR Recovery Script exits during initialization under the following conditions: the CA path does not exist, the CA file is not a valid PEM file, or the CA file is corrupted. This parameter is optional, and defaults to `false`.	`true`
lvrrecovery.webDAV.tenants	No	A comma-separated list of tenants that the LVR Recovery Script processes.	UNKNOWN,tenant1,tenant2,tenant3
lvrrecovery.webDAV.<tenantname>.unrecoverable.url	No	The WebDAV URL to be used for unrecoverable recordings for <tenantname>. The tenant must be specified in **lvrrecovery.webDAV.tenants**.	
lvrrecovery.webDAV.<tenantname>.unrecoverable.username	No	The WebDAV username to be used for unrecoverable recordings for <tenantname>. The tenant must be specified in **lvrrecovery.webDAV.tenants**.	
lvrrecovery.webDAV.<tenantname>.unrecoverable.password	No	The WebDAV password to be used for unrecoverable recordings for <tenantname>. The tenant must be specified in **lvrrecovery.webDAV.tenants**.	
lvrrecovery.webDAV.<tenantname>.unrecoverable.maxToleratedwebDAVFailures	No	The maximum number of tolerated upload failures during a recovery for a tenant to unrecoverable WebDAV. Default is 50. The tenant must be specified in **lvrrecovery.webDAV.tenants**.	25
lvrrecovery.webDAV.<tenantname>.recoverable.maxToleratedwebDAVFailures	No	The maximum number of tolerated upload failures during a recovery for a tenant to recoverable WebDAV. Default is 50. The tenant must be specified in **lvrrecovery.webDAV.tenants**.	25

		of tolerated upload failures during a recovery for a tenant to their recoverable WebDAV. The recoverable WebDAV is the WebDAV server specified in the tenant's IVR Profile and a recording's metadata. Default is 50. The tenant must be specified in **lvrrecovery.webDAV.tenants**.	
lvrrecovery.webDAV.<tenantname>	recoverable.trustedCA	Configures TLS certificate validation when making a secure outbound connection to a tenant's recoverable WebDAV. Valid values are `true`, `false`, or a path to a trusted certificate authority (CA) bundle. If set to `true`, the certificate is validated. If set to `false`, the certificate is not validated. The CA file must be in PEM format. LVR Recovery Script exits during initialization under the following conditions: the CA path does not exist, the CA file is not a valid PEM file, or the CA file is corrupted. This parameter is optional, and defaults to `false`. The tenant must be specified in **lvrrecovery.webDAV.tenants**.	`true`
lvrrecovery.webDAV.<tenantname>	unrecoverable.trustedCA	Configures TLS certificate validation when making a secure outbound connection to a tenant's unrecoverable WebDAV. Valid values are `true`, `false`, or a path to a trusted certificate authority (CA) bundle. If set to `true`, the certificate is validated. If set to `false`, the certificate is not validated. The CA file must be in PEM format. LVR Recovery Script exits during initialization under the following conditions: the CA path does not exist, the CA file is not a valid PEM file, or the CA file is corrupted. This parameter is optional, and defaults to `false`. The tenant must be specified in **lvrrecovery.webDAV.tenants**.	`true`

Running LVR Recovery Script Manually

The LVR Recovery Script automatically runs at the times scheduled during installation.

To manually run the LVR Recovery Script to recover recordings, run the following command from the <LVR Installation Directory>:

For MCP:

```
java -jar recover_LVRs.jar --mode recover --component MCP --properties MCP_premise.properties
```

For RPS:

```
java -jar recover_LVRs.jar --mode recover --component RP --properties RPS_premise.properties
```

OR

```
java -jar recover_LVRs.jar --mode recover --component RPS --properties RPS_premise.properties
```