Backup and Restore

Question

How do I back up and restore my Privileged Identity instance? How do I migrate my Privileged Identity instance?

Answer

Backup

1. **Export your encryption key.** The encryption key is required to gain access to stored passwords should it be necessary to restore or to migrate the management console.
    - Go to **Settings > Encryption Settings**.
    - Click **Export**.
    - Provide the exported encryption key along with a name.
    - Click **Open**. The encryption key is then saved at the chosen location.
2. **Export the migration data sub-key.** This step is required for Privileged Identity versions 4.83.5 and prior. If the migration data sub-key is not backed up and restoration of the program occurs, migration steps are replayed against the database. This can lead to problems, which can be resolved in the database. Potential issues include having jobs with incorrect information or users gaining access to systems for which they should not have access. Backup the following sub-key:
    - 32bit systems = HKLM\Software\Lieberman\{RPM | PWC}\MigrationData
    - 64bit systems = HKLM\Software\Wow6432node\Lieberman\{RPM | PWC}\MigrationData

    The keys denote the migration steps taken against the current database. Alternatively, to export the encryption key and the migration data keys, you may export the following registry key:

    - 32bit systems = HKLM\Software\Lieberman
    - 64bit systems = HKLM\Software\Wow6432node\Lieberman
3. **Back up the database used by Privileged Identity.** The backup process for the database may vary. In most cases, you can right-click on the database or file groups and choose **Backup**.
4. **Back up SSH/Telnet Response Files.** Any additional XML response files created for Privileged Identity and corresponding XSD files should be backed up. These files are present only if they have been added by you and are used for SSH/Telnet targets.
5. **Back up Event Sinks.** If any event sinks have been configured, their XML files should be backed up. By default, these are located at **C:\ProgramData\Lieberman\GenericEventServer\Version 1.x\EventSinks\SystemEventSinks**.
6. **Back up integration files.** If your Privileged Identity instance is integrated with another help desk provider such as BMC Remedy, HP Service Manager, etc., the integration configuration files should be backed up. These files are located in subfolders at **C:\ProgramData\Lieberman** and typically have a name similar to **LiebIntegrationName**. These folders and files exist only when an integration has been configured.

Restore

1. **Restore the database.** If you need to restore your database, do so before restoring the application. The restoration process may vary and depends on your database. In most cases, you can choose to restore the database backup.

2. **Restore the registry key collected during backup.** If the database is restored and the Privileged Identity version is restored without replacing the registry keys first, Privileged Identity performs the migration steps on the database again. This could lead to missing data, a failed job, etc.

   For reference, the following registry keys are located at:

   - 32bit systems = HKLM\Software\Lieberman\{RPM | PWC}\MigrationData
   - 64bit systems = HKLM\Software\Wow6432node\Lieberman\{RPM | PWC}\MigrationData

   In older versions of Privileged Identity, specifically 4.83.5 and older, under each key, there is a DWORD value called bStepCompleted. Thie registry key was depcreated in version 4.83.6, and is no longer used to handle database migration checkpoints. It is now necessary only to backup/restore the Privileged Identity program database.

IMPORTANT!

If reverting to a previous version of the database during restoration, delete the registry keys corresponding to that version. Version numbers and their corresponding keys are available at the end of this article.

Note: *RED IM versions 4.83.6 and later no longer use the registry to handle database migration checkpoints. It is necessary to back up and restore the RED IM database.*

Reinstall

1. **Reinstall the Privileged Identity application.** Click **Next** through all steps of the installer. Click **Finish**.
2. **Reimport the registry keys.** If you exported the registry key, simply reimport the registry key and launch the application.
   - If you exported only the encryption key and the migration data key in lieu of the registry key, follow the steps below:
     - Import the data migration key.
     - Launch the application.
     - Follow the mini-setup wizard to reconnect to the database. Make sure you use the same database schema configuration as before.
     - When prompted, import the encryption key.
     - Do not install the web site at this point. Click **OK**.
3. **Register the application.** Go to **Help > Register**. Enter your registration key. If this is a new server and does not share the same NetBIOS name as the last server, you will need a new license key for the new server.
4. **Redeploy the web site.** From the **Settings** menu, select **Manage Web Application > Install Web Application Instance**.

   Note: *For versions 4.81 and later, web site settings are stored in the database. Deployment of the web site will require only reimporting the encryption key and reconnecting to the same database. For versions 4.890 and before, and if you reimport the encryption key only, you will need to reconfigure all settings. If you reimport the registry key, all of these options will already be configured.*

5. **Restore the answer files, event sinks, and help desk integration configuration files.** Restore these files to the same physical path as noted above. If these files are not placed in the same path, it will be necessary to manually edit existing password change jobs to point to wherever the answer files are located. The event sink directory will also have to be manually updated.