



# Veeam Backup for Salesforce

---

Version 3.0

User Guide

September, 2024

© 2024 Veeam Software.

All rights reserved. All trademarks are the property of their respective owners.

No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language in any form by any means, without written permission from Veeam Software (Veeam). The information contained in this document represents the current view of Veeam on the issue discussed as of the date of publication and is subject to change without notice. Veeam shall not be liable for technical or editorial errors or omissions contained herein. Veeam makes no warranties, express or implied, in this document. Veeam may have patents, patent applications, trademark, copyright, or other intellectual property rights covering the subject matter of this document. All other trademarks mentioned herein are the property of their respective owners. Except as expressly provided in any written license agreement from Veeam, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

#### **NOTE**

Read the End User Software License Agreement before using the accompanying software programs. Using any part of the software indicates that you accept the terms of the End User Software License Agreement.

# Contents

<b>CONTACTING VEEAM SOFTWARE.....</b>	<b>6</b>
<b>OVERVIEW.....</b>	<b>7</b>
Solution Architecture .....	8
Data Backup.....	11
Backup Retention.....	12
Data Restore.....	13
How Veeam Backup for Salesforce Restores Object Hierarchy.....	14
<b>PLANNING AND PREPARATION .....</b>	<b>15</b>
System Requirements .....	16
Ports.....	19
Permissions.....	20
Considerations and Limitations.....	22
Sizing and Scalability Guidelines.....	24
PostgreSQL.....	25
Log Storage .....	27
File Storage .....	28
<b>LICENSING.....</b>	<b>29</b>
Installing and Removing License .....	31
Viewing License Information .....	33
<b>DEPLOYMENT .....</b>	<b>34</b>
Installing Veeam Backup for Salesforce on RedHat and Oracle Machines .....	35
Installing Veeam Backup for Salesforce on Ubuntu Machines.....	39
Performing Initial Configuration.....	43
Step 1. Accept License Agreement.....	44
Step 2. Create Local Administrator .....	45
Step 3. Connect to PostgreSQL.....	46
Step 4. Provide License File.....	50
Step 5. Create Connected App.....	51
Step 6. Connect to Salesforce .....	53
Step 7. Set Backup Policy Schedule .....	55
Step 8. Finish Working with Wizard .....	56
<b>ACCESSING VEEAM BACKUP FOR SALESFORCE.....</b>	<b>57</b>
<b>CONFIGURING VEEAM BACKUP FOR SALESFORCE .....</b>	<b>58</b>
Managing Salesforce Organizations.....	59
Adding Organizations.....	60
Editing Organizations.....	61
Removing Organizations .....	65
Managing Companies .....	66

Adding Companies .....	67
Editing Companies .....	68
Removing Companies .....	69
Managing Databases .....	71
Adding Database Connections .....	72
Editing Database Connections .....	74
Removing Database Connections.....	75
Managing Users .....	76
User Roles and Permissions .....	77
Adding Users.....	80
Editing Users .....	82
Removing Users .....	84
Configuring Security Settings .....	85
Changing Connected App Tokens .....	86
Configuring IdP and SSO Settings.....	88
Configuring Encryption Settings.....	92
Managing AWS KMS Connections .....	93
Managing Encryption Keys .....	96
Viewing Audit Trail.....	97
Managing Alerts.....	98
Configuring Notification Settings .....	100
Creating Alerts.....	103
Editing Alerts.....	107
Configuring Advanced Settings .....	108
<b>PERFORMING SALESFORCE BACKUP .....</b>	<b>111</b>
Creating Backup Policies .....	112
Step 1. Launch Add Backup Policy Wizard .....	113
Step 2. Configure Connection to Salesforce Organization.....	114
Step 3. Configure Backup Settings.....	116
Step 4. Enable Backup of Files and Attachments .....	123
Step 5. Configure Encryption Settings .....	124
Step 6. Configure Retention Settings .....	126
Step 7. Finish Working with Wizard.....	128
Starting and Stopping Backup Policies.....	129
Disabling and Enabling Backup Policies .....	130
Editing Backup Policies .....	131
Removing Backup Policies .....	133
Viewing Backup Policy Details.....	134
Viewing Backup Policy Sessions.....	135
<b>VIEWING BACKED-UP DATA .....</b>	<b>138</b>
<b>PERFORMING SALESFORCE RESTORE .....</b>	<b>140</b>

Creating Restore Jobs .....	141
Restoring Records .....	142
Restoring Field Values.....	155
Restoring Files .....	166
Restoring Metadata.....	173
Starting and Stopping Restore Jobs.....	181
Cloning Restore Jobs .....	182
Editing Restore Jobs .....	183
Removing Restore Job Drafts .....	185
Configuring Restore Mapping Settings .....	186
Viewing Restore Job Details .....	189
Viewing Restore Sessions .....	190
<b>PERFORMING SALESFORCE ARCHIVING .....</b>	<b>191</b>
Creating Archival Policies .....	192
Step 1. Launch Add Archival Policy Wizard .....	193
Step 2. Specify Archival Policy Info.....	194
Step 3. Select Organization .....	195
Step 4. Choose Data to Archive .....	196
Step 5. Configure General Settings.....	198
Step 6. Configure Hierarchy Settings.....	200
Step 7. Finish Working with Wizard.....	201
Starting and Stopping Archival Policies .....	202
Disabling and Enabling Archival Policies.....	203
Editing Archival Policies .....	204
Removing Archival Policy .....	205
Viewing Archival Policy Details.....	206
Viewing Archival Policy Sessions .....	207
Collecting Archived Data.....	209
<b>UPDATING VEEAM BACKUP FOR SALESFORCE.....</b>	<b>210</b>
Upgrading Veeam Backup for Salesforce .....	211
Checking for Updates.....	212
Installing Updates.....	213
Viewing Updates History .....	215
<b>GETTING TECHNICAL SUPPORT .....</b>	<b>216</b>
<b>APPENDICES.....</b>	<b>218</b>
Appendix A. Unsupported Objects.....	219
Appendix B. Replacing Security Certificate .....	220

# Contacting Veeam Software

At Veeam Software we value feedback from our customers. It is important not only to help you quickly with your technical issues, but it is our mission to listen to your input and build products that incorporate your suggestions.

## Customer Support

Should you have a technical concern, suggestion or question, visit the [Veeam Customer Support Portal](#) to open a case, search our knowledge base, reference documentation, manage your license or obtain the latest product release.

## Company Contacts

For the most up-to-date information about company contacts and office locations, visit the [Veeam Contacts Webpage](#).

## Online Support

If you have any questions about Veeam products, you can use the following resources:

- Full documentation set: [veeam.com/documentation-guides-datasheets.html](http://veeam.com/documentation-guides-datasheets.html)
- Veeam R&D Forums: [forums.veeam.com](http://forums.veeam.com)

# Overview

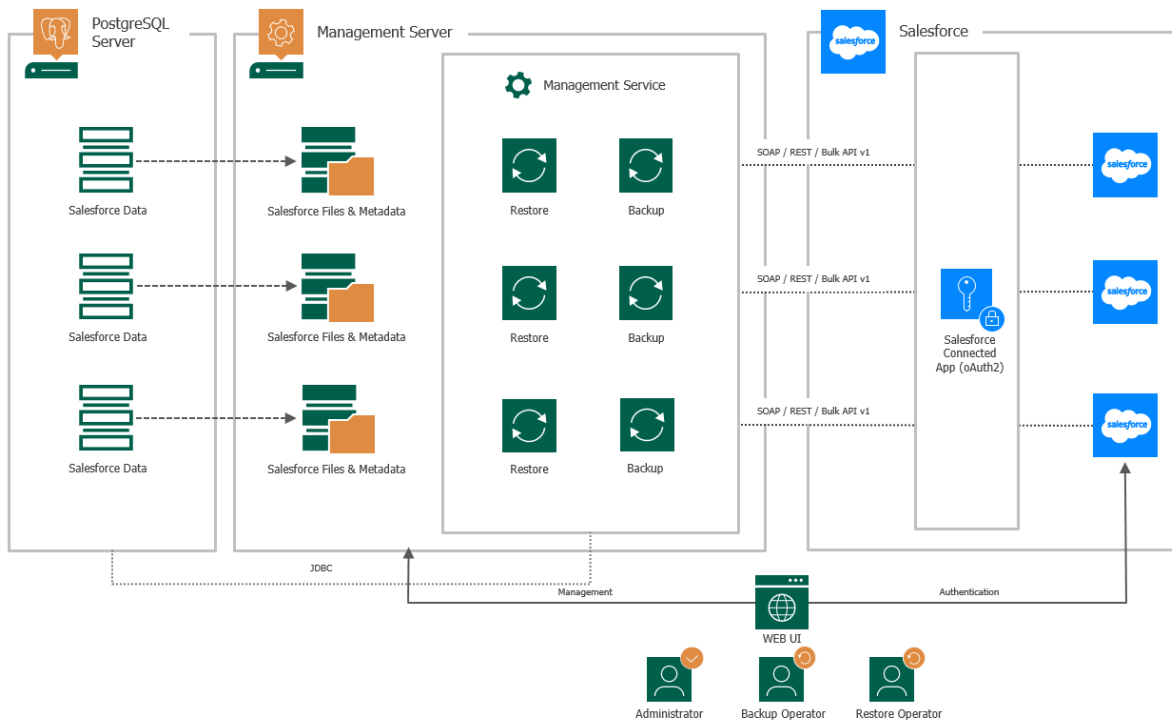
Veeam Backup for Salesforce is a solution developed for data and metadata protection for the Salesforce SaaS platform. With Veeam Backup for Salesforce, you can do the following:

- Run your backup environment anywhere: on-premises, in AWS, Microsoft Azure and so on.
- Protect multiple Salesforce organizations with one installation.
- Back up Salesforce files, data and metadata.
- Encrypt data on the client side with original (built-in) or AWS KMS keys.
- Configure flexible backup schedules for different Salesforce objects to meet the desired RPOs.
- Create high-frequency, near-continuous backups of specific objects.
- Restore files, data and metadata including object hierarchies and custom fields.
- Restore files, fields, records and objects of entire Salesforce organizations.
- Restore data and metadata (including Reports, Profiles, Permission sets, Flows and so on).
- Restore object hierarchy to an unlimited level of depth.
- Restore child and parent relationships.
- Configure granular retention settings at the object level.
- Compare versions of production Salesforce records with versions of backed-up records stored in repositories.
- Compare versions of production Salesforce metadata with versions of backed-up metadata stored in repositories to see line-by-line differences.
- Create real-time alerts for backup, recovery, licensing and connection issues, as well as for any changes in protected data.
- Use Microsoft Entra ID or Salesforce as a single sign-on (SSO) provider to log in the product Web UI.
- Leverage role-based access control (RBAC) if connected using an SSO provider.

# Solution Architecture

The Veeam Backup for Salesforce architecture includes the following components:

- [Management server](#)
- [PostgreSQL server](#)
- [File repositories](#)
- [Log repository](#)
- [Salesforce organizations](#)





# Management Server

The management server is a Linux-based machine where Veeam Backup for Salesforce is installed. The management server performs the following administrative activities:

- Manages infrastructure components.
- Coordinates backup and restore jobs.
- Controls backup policy execution.
- Generates alert notifications that can be sent by email and to specific Slack channels and chats.

## Management Server Components

The management server uses the following components:

- **Management server** (`vbsf-backend`) – manages backup and restore services. It also provides a web interface (Web UI) that allows a user to access the Veeam Backup for Salesforce functionality.
- **Backup service** (`vbsf-backup`) – performs data retrieval from Salesforce.
- **Restore service** (`vbsf-restore`) – performs data upload to Salesforce.
- **Configuration database** – stores application configuration, connection details to Salesforce organizations, backup policies, restore jobs, sessions and so on. This database is created during [initial configuration](#) of Veeam Backup for Salesforce.
- **Veeam Updater** (`veeam-updater`) – allows Veeam Backup for Salesforce to check, view and install product and package updates.

## PostgreSQL Server

To store data and backups of protected Salesforce organizations, Veeam Backup for Salesforce uses PostgreSQL databases. Each protected organization must have a dedicated database. Veeam Backup for Salesforce creates at least 2 database schemas and saves organization data and metadata to the database specified in the [backup policy](#) settings. For more information on databases, see [Managing Databases](#).

One additional database – configuration database – is required to store Veeam Backup for Salesforce configuration. It is possible to combine application configuration schema and Salesforce backup schemas in one database, although it is not recommended for portability reasons.

Since the PostgreSQL server is not a part of the Veeam installation package, you must install and configure it separately. For more information, see [System Requirements](#).

## File Repositories

To store backups of Salesforce files and metadata, Veeam Backup for Salesforce creates a file repository per each protected Salesforce organization on the management server in the following folder: `/opt/vbsf/data`. The name of each file repository contains the path to the folder and organization ID. It is recommended that you create a dedicated partition for the file storage and mount it to the specified directory to prevent any disk capacity issues on the management server. For more information on the required disk capacity, see [System Requirements](#).

# Log Repository

By default, Veeam Backup for Salesforce stores its logs in the following folder: `/var/log/vbsf/`. It is recommended that you create a dedicated partition for the log repository and mount it to the specified directory to prevent any disk capacity issues on the management server. For more information on the required disk capacity, see [System Requirements](#).

# Salesforce Organizations

To protect a Salesforce organization, Veeam Backup for Salesforce uses the native Salesforce API. To allow integration between the product and Salesforce, the Administrator of the protected organization (a Standard User with [specific permissions](#)) creates a Connected App and uses the Administrator account to authorize access to Salesforce data.

To enable access to the product functionality with the help of user roles and scopes, the Administrator configures [single sign-on \(SSO\) authentication](#) with a Microsoft Azure or Salesforce identity provider and [adds new users](#) to the product.

# Data Backup

To back up data of Salesforce organizations, Veeam Backup for Salesforce runs backup policies. A backup policy is a collection of settings that define the way backup operations are performed: what data to back up, where to store backups, when to start the backup process, and so on. Note that each Salesforce organization can be protected by only one backup policy in one Veeam Backup for Salesforce installation.

When creating a backup policy, you can instruct Veeam Backup for Salesforce to do the following:

- Back up Salesforce object data and metadata. For the full list of Salesforce metadata that can be backed up, see [Salesforce Documentation](#).
- Back up files associated with Salesforce objects.
- Back up documents, including *ContentDocument*, *FeedAttachment* and *QuoteDocument* objects. Chatter objects are also supported.
- Exclude specific objects and fields from the backup scope.
- Automatically protect new objects and fields.
- Apply different schedules to launch separate backup sessions for different groups of objects.
- Configure retention policies to remove backed-up data that is older than a specific retention period.
- Encrypt record fields and files at rest.

## How to Protect Salesforce Organizations

To create a backup policy, complete the following steps:

1. [Check considerations and limitations](#).
2. [Add a Salesforce organization](#).
3. [Connect a database that will be used to store backed-up data](#).
4. [Complete the Add Backup Policy wizard](#).

## Related Topics

[Data Restore](#)

# Backup Retention

Veeam Backup for Salesforce retains record restore points for the number of days defined in retention scheduling settings as described in section [Creating Backup Policies](#).

During every successful backup policy session, Veeam Backup for Salesforce creates a new restore point that allows you to roll back to a specific point in time. If Veeam Backup for Salesforce detects that a restore point is older than the specified retention period, the product removes it from the configuration database.

## IMPORTANT

When Veeam Backup for Salesforce deletes a record, all its associated attachments are deleted as well – but only if the following requirements are met:

- The attachments no longer exist in Salesforce.
- The attachments have backups.
- The attachments are older than the specified retention period.

# Data Restore

Veeam Backup for Salesforce offers the following restore options:

- [Restore records](#) – fully restores the content of a record, with all fields that are marked as *updatable* and *creatable* in Salesforce. You can also restore attachments associated with this record and the related object hierarchy.
- [Restore field value](#) – restores specific field values of a Salesforce record. Consider that you can only restore values of existing fields using this type of restore. If any fields no longer exist in Salesforce, you must restore metadata first.
- [Restore metadata](#) – restores Salesforce metadata.
- [Restore files](#) – restores Salesforce files and attachments.

You can restore records, field values and metadata to the most recent state or to any available version.

## In This Section

[How Veeam Backup for Salesforce Restores Object Hierarchy](#)

# How Veeam Backup for Salesforce Restores Object Hierarchy

Consider the following example. You want to restore a record of the **Contact** object:

- This record refers to another record of the **Account** object. In this case, the **Account** object is the 1st level parent for the **Contact** object.
- There are 2 backed-up records in the **Case** object linked to the record you want to restore. The **Case** object is the 1st level child for the **Contact** object. If there are also records in the **CaseMilestone** object that are linked to these 2 records in the **Case** object, the **CaseMilestone** object will be the 2nd level child for the **Contact** object.

## Parent Object Restore

By default, the product restores the 1st level parent records only (that is, the record of the **Account** object from our example). However, you can instruct Veeam Backup for Salesforce to restore parent records of higher hierarchy levels as described at [step 6](#) of the **Restore Records** wizard. While restoring a parent record, the product checks whether the record exists in the Salesforce database:

- If the parent record exists in Salesforce, the product skips the record and does not proceed to higher levels of the parent hierarchy for this record.
- If the parent record does not exist in Salesforce, the product creates the record in Salesforce using the backed-up data.

## Child Object Restore

By default, the product restores the 2nd level child records only (that is, 2 records of the **Case** object and records of the **CaseMilestone** object in our example). However, you can instruct Veeam Backup for Salesforce to restore child records of deeper hierarchy levels as described at [step 6](#) of the **Restore Records** wizard. While restoring a child record, the product checks whether the record exists in the Salesforce database:

- If a child record exists in Salesforce and has the same data as the backed-up record data, the product skips the record.
- If a child record exists in Salesforce, but the record data has changed, the product updates the record using the backed-up data.
- If a child record exists in Salesforce but it is in the Salesforce Recycle Bin, the product restores the record from the Recycle Bin.
- If a child record does not exist in Salesforce, the product creates the record in Salesforce using the backed-up data.

# Planning and Preparation

Before you start installing Veeam Backup for Salesforce, check system requirements for the product components, network ports used for data transmission, required permissions and other prerequisites. For more information on the product components, see [Solution Architecture](#).

## In This Section

- [System Requirements](#)
- [Ports](#)
- [Required Permissions](#)
- [Considerations and Limitations](#)
- [Sizing and Scalability Guidelines](#)

# System Requirements

The machine where Veeam Backup for Salesforce will be deployed, the machines running PostgreSQL servers used to host databases, and the file shares used to store backed-up data must meet the necessary hardware and software requirements.

## Management Server

Specification	Requirement
Hardware	<p><i>CPU:</i> 4 cores (recommended)</p> <p><i>Memory:</i> 4 GB RAM (minimum). If you plan to protect multiple Salesforce organizations, it is recommended that you add 4 GB for the management server and 1 GB per each protected organization.</p> <p><i>Free space:</i> 100 GB (minimum), excluding file and log storage space. For file storage space requirements, see <a href="#">File Storage</a>. For log storage space requirements, see <a href="#">Log Storage</a>.</p> <p><i>Network bandwidth:</i> 10 Mbps (minimum)</p> <p><b>Note:</b> To improve performance of the management server, it is recommended that you use SSDs for databases and file storage.</p>
OS	<ul style="list-style-type: none"><li>• RedHat Linux 8.x, 9.x</li><li>• Oracle Linux 8.x, 9.x</li><li>• AlmaLinux 8.x, 9.x</li><li>• Rocky Linux 8.x, 9.x</li><li>• Ubuntu 20.04.x LTS, 22.04.x LTS</li></ul>
Software	Oracle JDK (Java) 17
File System	<ul style="list-style-type: none"><li>• XFS</li><li>• EXT4</li></ul> <p><b>Note:</b> Due to technical limitations on the number of directory files in EXT4, Veeam Backup for Salesforce may report incorrect storage capacity values when performing file backups. That is why it is recommended that you use the XFS file system even though both systems are fully supported.</p>



# PostgreSQL Servers

Specification	Requirement
Hardware	<p><i>CPU:</i> 4 cores (minimum)</p> <p><i>Memory:</i> 16 GB RAM if the largest object in your Salesforce organization contains no more than 2M records; 32 GB RAM and more if you have objects that contain more than 20M records.</p> <p><i>Free space:</i> The initial backup of Salesforce data requires at least x1.6 more disk space in PostgreSQL since the product stores both the latest and history records. You can calculate the required disk space as described in section <a href="#">Sizing and Scalability Guidelines</a>.</p> <p>To learn how to monitor your data storage and used file space in Salesforce, see <a href="#">Salesforce Documentation</a>.</p> <p><b>Note:</b> To improve performance of PostgreSQL servers, it is recommended that you use SSDs on the machines running the servers.</p>
Software	PostgreSQL 13.x, 14.x, 15.x (version 15.8 is included in the setup)

# File Storage

Specification	Requirement
Hardware	<p>Veeam Backup for Salesforce stores file data and metadata in the <code>/opt/vbsf/data</code> folder on the management server. It is recommended that you create a dedicated partition for the file storage and mount it to the specified directory. Consider that network file shares are not supported.</p> <p>Make sure that you provide your file storage with enough space taking into account the total size of the files used in Salesforce and your daily change rate. To view the amount of space used by your files, open the Salesforce UI, navigate to <b>Setup &gt; Company Information</b> and check the <b>Used File Space</b> field. For more information, see <a href="#">Sizing and Scalability Guidelines</a>.</p> <p><b>Note:</b> To improve performance of the management server, it is recommended that you use SSDs for the file storage.</p>

## Log Storage

Specification	Requirement
<b>Hardware</b>	Veeam Backup for Salesforce stores its logs in the <code>/var/log/vbsf/</code> folder on the management server. It is recommended that you create a dedicated partition for log storage with a minimum of 50 GB of disk capacity and mount it to the specified directory. For more information, see <a href="#">Sizing and Scalability Guidelines</a> .

## Salesforce

Specification	Requirement
<b>Salesforce API</b>	<p>By default, Veeam Backup for Salesforce 3.0 uses Salesforce API version 60.0. Any objects available in later API versions will not be discovered and protected by the product.</p> <p><b>Note:</b> You can change the API version used by the product as described in section <a href="#">Configuring Advanced Settings</a>.</p>

# Ports

The following network ports must be open to ensure proper communication of components in the Veeam Backup for Salesforce infrastructure.

From	To	Protocol	Port	Notes
Web browser (local machine)	Management server	TCP/HTTPS	443	Required to access the Web UI component from a user workstation.
		SSH	22	Required to communicate with the backup service running on the management server.
	Salesforce	TCP/HTTPS	443	Required to communicate with Salesforce entities.
	Microsoft Azure	TCP/HTTPS	443	Required to communicate with Microsoft Azure entities.
Management server	PostgreSQL servers	TCP	5432	Required to communicate with servers hosting databases used to store backed-up data.
	Salesforce	TCP/HTTPS	443	Required to communicate with Salesforce entities.
	SMTP server	TCP	25	Default port used for sending email notifications.
	Veeam License Server (vbsf.butler.veeam.com)	TCP/HTTPS	443	Required to activate licenses, to verify license updates and metering.
	Veeam Update Notification Server (repository.veeam.com)	TCP/HTTPS	443	Required to verify availability of product updates, notify users on these updates and install the updates on the management server.

# Permissions

To perform backup and restore operations, Veeam Backup for Salesforce requires the following permissions to be provided.

## Salesforce API Integration

Account	Required Permissions
<b>Salesforce User</b>	<p>Veeam Backup for Salesforce requires a Standard User with the <i>Salesforce</i> license type to connect to a Salesforce organization to perform backup and restore operations for Salesforce resources. Note that free Salesforce Integration Users cannot perform backup and restore operations.</p> <p>The user whose credentials are used to authorize the connection must be assigned full permissions required to read and modify data:</p> <ul style="list-style-type: none"><li>• System Administrator profile (grants broad permissions immediately, but not all the required ones).</li><li>• Permission set that has the following permissions enabled:<ul style="list-style-type: none"><li>○ <a href="#">Query All Files</a> permission to back up and archive all files.</li><li>○ <a href="#">Modify All Data</a> permission to archive data.</li><li>○ <a href="#">Bulk API Hard Delete</a> permission to use Bulk API while archiving data.</li><li>○ <a href="#">View and Edit Converted Leads</a> permission to restore converted leads.</li><li>○ Permissions for all <a href="#">custom record types of objects</a> to restore records of custom types.</li><li>○ <a href="#">Set Audit Fields upon Record Creation</a> permission to restore original values in audit fields when restoring deleted records.</li><li>○ <a href="#">Update Records with Inactive Owners</a> permission to restore deleted records owned by inactive users.</li><li>○ <a href="#">Update Email Messages</a> permission to restore attachments of email messages.</li></ul></li><li>• Permission set licenses for any managed application license that is required for accessing the data (for example, HVS, CPQ).</li><li>• Feature-based user permissions: Marketing User, Service Cloud User, Knowledge User, Salesforce CRM Content User.</li><li>• Record-based user permissions: for correct archival of different types of object records, the user must have permissions to modify each of those types of records.</li></ul> <p>For sandboxes, any managed application needs to be enabled and license provided to the user. For example, <b>High Velocity Sales</b> requires application activation.</p>

Account	Required Permissions
<b>AWS Key Management Service</b>	<p>The IAM and key policies that Veeam Backup for Salesforce uses when encrypting data with AWS KMS keys must provide permissions to perform the following operations:</p> <ul style="list-style-type: none"> <li>• <i>ListKeys</i> operation to get the list of available keys. Only symmetric keys can be used in Veeam Backup for Salesforce 3.0.</li> <li>• <i>Encrypt</i> operation to encrypt data with AWS KMS keys.</li> <li>• <i>Decrypt</i> operation to decrypt data with AWS KMS keys.</li> <li>• <i>DescribeKey</i> operation to retrieve information about AWS KMS keys.</li> </ul> <p>For more information on the IAM and key policies, see <a href="#">AWS Documentation</a>.</p>
<b>Salesforce Connected App</b>	<p>Veeam Backup for Salesforce establishes secure and encrypted connections to Salesforce using tokens of Connected Apps. When creating and configuring a Connected App, make sure the following OAuth scopes are added to the app:</p> <ul style="list-style-type: none"> <li>• <b>Full access</b> (full)</li> <li>• <b>Perform requests at any time</b> (refresh_token, offline_access)</li> <li>• <b>Access unique user identifiers</b> (openid)</li> </ul> <p>To learn how to create the app, see <a href="#">Performing Initial Configuration</a>.</p> <p><b>Note:</b> The <b>Access unique user identifiers</b> (openid) option applies only if you use <a href="#">Salesforce as an identity provider</a>. For more information on OAuth scopes in Salesforce, see <a href="#">Salesforce Documentation</a>.</p>

## Veeam Backup for Salesforce Components

Account	Required Permissions
<b>PostgreSQL Database User</b>	<p>Veeam Backup for Salesforce creates databases and database schemas to store Salesforce data and metadata. Therefore, the database user must be granted permissions to create schemas and databases.</p> <p><b>Note:</b> If you do not grant the user permissions to create databases, you will have to manually create databases on PostgreSQL servers first, and then add databases to Veeam Backup for Salesforce as described in section <a href="#">Adding Databases</a>, before you create any backup policies.</p>

# Considerations and Limitations

When you plan your deployment of Veeam Backup for Salesforce, keep in mind the following limitations and considerations.

## Supported Salesforce Offerings

- Salesforce provides multiple offerings that are built on one Salesforce Platform – Sales Cloud, Service Cloud, Financial Cloud, Health Cloud and Education. Veeam Backup for Salesforce 3.0 supports backup of all data and objects available on the Salesforce Platform if these resources can be retrieved using the Salesforce API version 60 and earlier. This means that if an object or data cannot be obtained using standard Salesforce API requests, backup of these objects is not supported.

Salesforce Marketing Cloud is built on another platform and is not protected by the product.

- Both Salesforce Classic and Lightning Experience interfaces are supported.
- Salesforce sandbox organizations as well as Salesforce production organizations can be protected by Veeam Backup for Salesforce.
- All Salesforce API-enabled editions are supported: Developer, Enterprise, Performance, Professional (API access must be enabled), Unlimited.

## Backup and Restore

- Backup and restore of *EmailTemplate*, *Document*, *Report* and *Dashboard* types of metadata objects located in private folders are not supported since Salesforce does not provide API to export and restore this type of data.
- Backup of *KnowledgeArticle* types of objects is not supported.
- Backup of *BigObject* types of objects is not supported.
- Backup of Salesforce objects listed in [Appendix A. Unsupported Objects](#) is not supported.
- Backup of certain metadata types is unsupported due to Salesforce limitations. For more information, see [Salesforce Documentation](#).
- Backup and restore of *TenantSecret* types of objects is not supported.
- Backup of embedded images added to *ContentNote* types of objects is not supported.
- Backup of embedded images in rich text area fields is supported only if the fields are not encrypted.
- Restore of the *MobileApplicationDetail* and *MailmergeTemplate* types of content is not supported.
- Restore of embedded images deleted from *ContentNote*, *FeedItem* and *FeedComment* types of objects is not supported.
- *FeedAttachment* types of objects can be restored only as part of *FeedItem* object hierarchy restore. Note that *ContentVersion* objects can be restored only if they were added as attachments (not embedded images) to *FeedItem* objects.

## Time Zone

The product Web UI uses the time zone of a machine from which you access Veeam Backup for Salesforce. However, the management server and databases use the UTC time zone for all operations.

## Salesforce User

- Set the English language in the locale and account language settings for the user in Salesforce. It is required for error handler to work properly.
- Make sure that you have assigned the user all the [required permissions](#).

# Sizing and Scalability Guidelines

This section is intended for professionals who search for a best practice answer to sizing-related issues, and assumes you have already read the whole Veeam Backup for Salesforce User Guide.

Be aware that a best practice is not the only answer available. It will fit in the majority of cases but can also be totally wrong under different circumstances. Make sure you understand the implications of the recommended practices, or request assistance. If in doubt, reach out to Veeam professionals on Veeam R&D Forums.



# PostgreSQL

To provide stable operation of a PostgreSQL server, make sure that you have enough disk space and compute resources allocated to the server and the following recommended settings configured.

## General Recommendations

- It is highly recommended that you install PostgreSQL on a dedicated server.
- It is recommended that you back up PostgreSQL databases on a regular basis. You can use [Veeam Backup & Replication](#) for this purpose.

## Disk Size Calculation

When calculating the disk space required for the PostgreSQL server, take into account your desired data set, daily change rate and the retention policy settings. The initial backup of Salesforce data requires at least x1.6 more disk space in PostgreSQL since the product creates both the latest and history records. All further backups are incremental and consume the same amount of disk space as original records occupy in the Salesforce database.

You can use the following formula to calculate the required disk space:  $(\text{Salesforce Used Data Space} * 1.6) + (\text{Size of Added Data} * \text{Planned Period of Data Backup}) + (\text{Size of Changed Data} * \text{Number of Backups Within Your Retention Period})$ .

### TIP

To check the amount of space currently occupied by your data in the Salesforce database, open the Salesforce UI and navigate to **Setup > Company Information**.

Consider the following example:

- *Salesforce Used Data Space* – your Salesforce database initially stores 200 GB of data.
- *Size of Added Data* – 10,000 records of 2 KB each are added to the Salesforce database daily (that is,  $10,000 * 2 \text{ KB} / 1024 = 0.02 \text{ GB}$ ).
- *Planned Period of Data Backup* – data is planned to be backed up daily for a period of 5 years (that is,  $5 * 365 \text{ days} = 1825 \text{ days}$ ).
- *Size of Changed Data* – 10,000 records of 2 KB each are changed in the Salesforce database each backup cycle (that is,  $10,000 * 2 \text{ KB} / 1024 = 0.02 \text{ GB}$ ).
- *Number of Backups Within Your Retention Period* – backup is performed every hour (that is, 24 backups per day) while the retention period is set to 180 days.

In this case, the amount of the disk space required for the PostgreSQL server will be calculated as follows:  $(200 \text{ GB} * 1.6) + (0.02 \text{ GB} * 1825) + (0.02 \text{ GB} * 24 * 180) = 320 \text{ GB} + 36.5 \text{ GB} + 86.4 \text{ GB} = 443 \text{ GB}$ .

# PostgreSQL Configuration Settings

Consider adjusting the default settings in the `postgresql.conf` configuration file as follows:

Parameter	Value
<code>max_connections</code>	300 or more*
<code>superuser_reserved_connections</code>	7
<code>shared_buffers</code>	20% of RAM
<code>random_page_cost</code>	1.1
<code>work_mem</code>	15% of RAM
<code>maintenance_work_mem</code>	128 MB
<code>max_wal_size</code>	3 GB
<code>min_wal_size</code>	2 GB
<code>checkpoint_completion_target</code>	0.9
<code>effective_io_concurrency</code>	200
<code>effective_cache_size</code>	60% of RAM

\*Veeam Backup for Salesforce requires about 20 connections to one PostgreSQL database for management operations, about 50 connections per one backup policy and 10 connections per one custom backup schedule. To avoid performance issues, it is recommended that you set the maximum allowed number of connections to 300 in the PostgreSQL database configuration. You may need to adjust this number later based on the number of created backup policies and schedules.

# Log Storage

Logs can consume significant amount of disk space. The total log size depends on the log retention policy and daily change rate in your organizations. If the management server runs out of space, Veeam Backup for Salesforce will fail to run. To provide stable operation of the product, consider the following:

- Before you deploy Veeam Backup for Salesforce, create a dedicated partition for log storage and allocate to it at least 10 % of the [file and data space used in Salesforce](#). For example, if you have 200 GB of files and 300 GB of data in your Salesforce organization, you must allocate at least 50 GB to this partition. Then, you must mount the partition to the `/var/log/vbsf/` folder.
- After you deploy Veeam Backup for Salesforce, specify for how long you want to retain the product logs. To do that, modify the `logging.backup.file.retention`, `logging.restore.file.retention` and `logging.backend.file.retention` parameter values as described in section [Configuring Advanced Settings](#).

# File Storage

As Veeam Backup for Salesforce stores Salesforce file data and metadata in the same format as they are stored in Salesforce, files can consume significant amount of disk space. The total file size depends on the file retention policy and daily change rate in your organizations. To provide stable operation of the product, consider the following:

- Before you deploy Veeam Backup for Salesforce, create a dedicated partition for file storage and mount this partition to the `/opt/vbsf/data/` folder. When you configure a backup policy, Veeam Backup for Salesforce verifies whether disk space available in the specified directory is enough for the amount of data that will be backed up and raises a warning in case of insufficient storage capacity. That is why it is recommended that you mount additional storage to the specified location to prevent the shortage of storage capacity.
- The product deletes backed-up files from its file repository according to the [configured retention settings](#) only. That means if you manually delete a file in Salesforce, it will not be automatically deleted from the repository.

# Licensing

A product license is required for Veeam Backup for Salesforce to run. Each product license can be used to protect one or multiple Salesforce organizations. Each product license can be used in one or multiple product installations.

Veeam Backup for Salesforce is licensed per User. A User is defined as a [Standard User](#) with the *Salesforce* or *Salesforce Platform* license type reported by the Salesforce Classic or Salesforce Lightning platform. However, this applies only to Salesforce user licenses consumed by protected production organizations since Users of Salesforce sandbox organizations do not consume any license units. The latter means that you can protect as many sandbox organizations as you want – but only if the total number of Salesforce users in these organizations does not exceed the limit of licensed Users in your Veeam license.

The Veeam license is also not required for:

- Salesforce user licenses consumed by Developer Edition organizations.
- Salesforce Chatter Free, Chatter Only, Chatter External, Partner Community, Customer Community, Customer Community Plus user licenses.
- Salesforce Identity licenses.

If the total number of reported user licenses of all Salesforce production organizations protected by Veeam Backup for Salesforce management servers that use the same license key exceeds the limit of license units for more than 10 Users or 10% of licensed units (whichever is greater), you will be able neither to perform backup operations nor to add new Salesforce organizations that you want to protect – until you update the license.

## IMPORTANT

The management server must have the outbound internet access to communicate with Salesforce API, Veeam License and Update Notification servers. If the connection is lost, Veeam Backup for Salesforce will not be able to activate new licenses, will continue operating for 30 days under the current license, and then halt all backup operations.

# License Types

Veeam Backup for Salesforce is available in the following license editions:

- **Community Edition** – the built-in license that allows you to protect up to 50 Users free of charge. This license comes without any technical support. Only community and best-effort technical support are available.
- **NFR, Evaluation**– the licenses that can be used for product demonstration, training or education. These licenses are not for resale or commercial use. For more information, see [Veeam End User License Agreement \(EULA\)](#).
- **Subscription** – the subscription-based license that expires at the end of the subscription term. The maximum number of users protected by Veeam Backup for Salesforce depends on the number of units specified in your license.

To purchase the license, it is required to provide the production ID of a Salesforce organization that you will protect with Veeam Backup for Salesforce. If you plan to protect more than one production organization, you can provide the ID of any of these organizations. To learn how to find the Salesforce Organization ID, see [Salesforce Documentation](#).

To work with Veeam Backup for Salesforce, you can use either the *Foundation* license package (available for the *Community Edition* and *Subscription* license types) or *Advanced* license package (available for the *Evaluation*, *NFR* and *Subscription* license types). The *Foundation* license package allows you to perform backup and restore operations, while the *Advanced* license package allows you to perform backup, restore and archival operations. To learn how to obtain a license, contact a Veeam sales representative at [Sales Inquiry](#).

## TIP

When the Veeam license expires, Veeam Backup for Salesforce offers a grace period to ensure a smooth license update and to provide sufficient time to install a new license file. The duration of the grace period is 30 days after the expiration of the license. During this period, you can perform all types of data protection operations. After the grace period is over, Veeam Backup for Salesforce stops processing all objects and files, and disables all scheduled backup and archival policies. You must update your license before the end of the grace period.

# Installing and Removing License

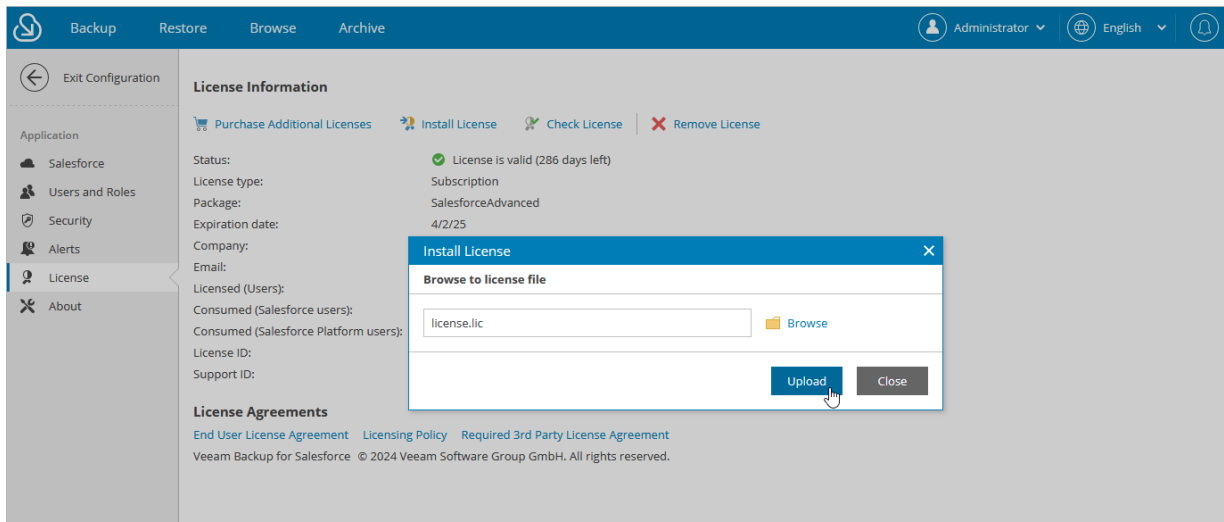
On the **License** tab, you can see the current license details, install a new license or remove the currently used license.

To purchase new license, renew or add more licenses, you can contact Veeam partners or request a quote from a Veeam sales representative. For more information, see the [Veeam website](#).

## Installing License

To install or update a license installed on the management server, do the following:

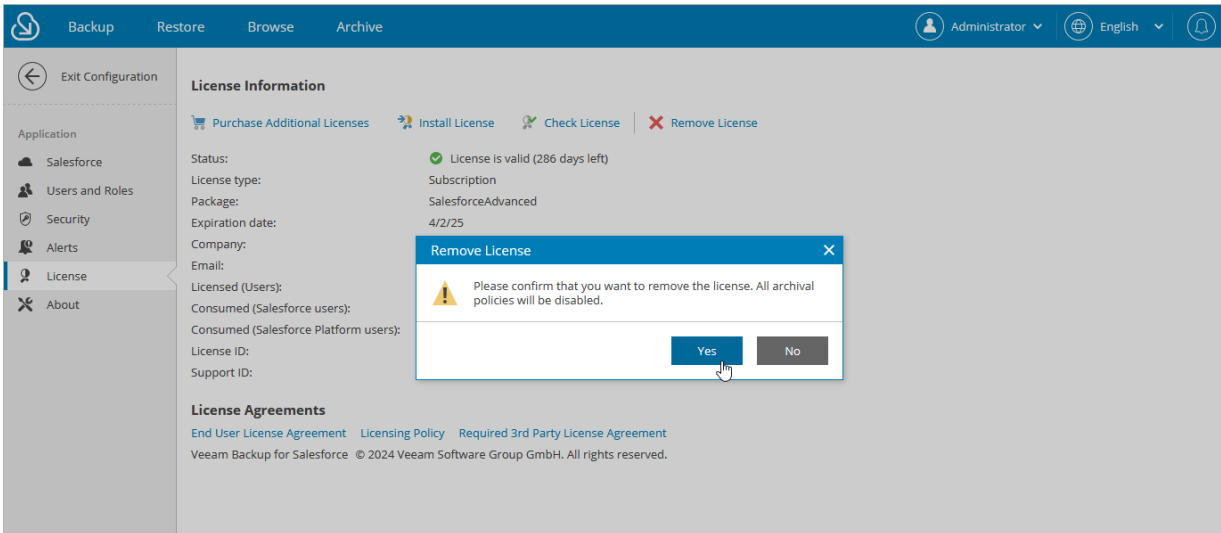
1. Switch to the **Configuration** page.
2. Navigate to **License**.
3. Click **Install License**.
4. In the **Install License** window, click **Browse** to browse to a license file, and then click **Upload**.



# Removing License

To remove a license installed on the management server if you no longer need it:

1. On the **License** tab, click **Remove License**.
2. In the **Remove License** window, click **Yes** to confirm that you want to remove the license.



## IMPORTANT

- If you remove the license, Veeam Backup for Salesforce will automatically switch back to the built-in *Community Edition* license. In this case, you will be able to protect maximum 50 Salesforce licensed users. For more information on license editions, see [Licensing](#).
- If you change the license package from *Advanced* to *Foundation*, archiving will be no longer available and all existing archival policies will be disabled.



# Viewing License Information

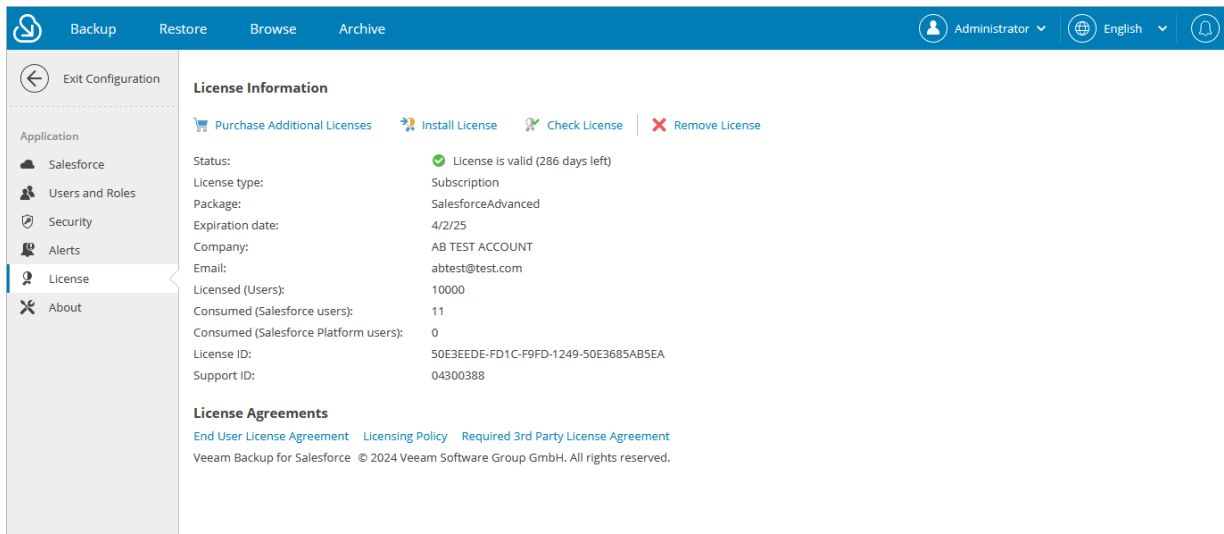
The license validity is verified by the Veeam License Server right after the installation and, then, periodically once a week. You can also verify the license manually, to do that:

1. Switch to the **Configuration** page.
2. Navigate to **License** and click **Check License**.

During license validation, the counts of users per protected Salesforce organization are reported to Veeam Backup for Salesforce, and then used in license metering and billing. In case licensing servers cannot be reached and new licenses cannot be installed, the grace period starts automatically from the last successful license check date.

The **License information** section provides general information on the Veeam Backup for Salesforce license:

- **Status** – the license status. The status depends on the license edition, the number of days remaining until license expiration and the license check result.
- **License type** – the license type (*Community Edition, Evaluation, NFR, Subscription*).
- **Package** – the license package (*Foundation, Advanced*).
- **Expiration date** – the date when the license will expire.
- **Company** – the name of a company to which the license was issued.
- **Email** – the email of a contact person specified in the contract.
- **Licensed (Users)** – the total number of licensed Users.
- **Consumed (Salesforce Users)** – the total number of consumed *Salesforce* user licenses across all protected Salesforce production organizations.
- **Consumed (Salesforce Platform Users)** – the total number of consumed *Salesforce Platform* user licenses across all protected Salesforce production organizations.
- **License ID** – the unique identification number of the license file.
- **Support ID** – the unique identification number of the Veeam support contract.



# Deployment

You can install Veeam Backup for Salesforce on a virtual or a physical machine.

Before you begin installation, check the following prerequisites:

1. Make sure that the machine where you plan to install Veeam Backup for Salesforce meets the minimal [system requirements](#) and the [required ports](#) are open. You must be also able to access the Salesforce authentication webpage from the machine.

It is recommended that you install Veeam Backup for Salesforce on a new or empty machine so that the management server does not conflict with other applications. Consider having enough free disk space for the log, metadata and file storage. For more information on the required disk space, see [System Requirements](#).

2. To install Veeam Backup for Salesforce software packages, you must use the root or super user account to install the system components and services.
3. If you have SELinux installed, you must allow `httpd` to connect to the network. To do that, run the following command:

```
sudo setsebool -P httpd_can_network_connect on
```

# Installing Veeam Backup for Salesforce on RedHat and Oracle Machines

You can install Veeam Backup for Salesforce on a RedHat or Oracle machine automatically using the installation script or manually.

## Installing Product Using Script

To install Veeam Backup for Salesforce, complete the following steps:

1. Set the Linux system locale to UTF-8 running the following command:

```
sudo localectl set-locales LANG=en_US.UTF-8
```

2. Log out of the current session and log back in to apply the new locale settings.
3. Download the installation script to the machine where you want to deploy Veeam Backup for Salesforce running the following command:

```
sudo curl https://repository.veeam.com/yum/el/vbsf-install-script.sh --output ./vbsf-install-script.sh
```

4. Run the script:

```
sudo sh ./vbsf-install-script.sh
```

The Linux package manager will install the Veeam software repository. When the repository is installed, the manager will start installation of Veeam Backup for Salesforce and dependencies, and run configuration checks.

After all configuration checks complete successfully, you will be prompted to run the server configuration script on the Linux host. For more information, see [Configuring Server Settings](#).

# Installing Product Manually

To install Veeam Backup for Salesforce, complete the following steps:

1. Update all installed Linux packages and their dependencies running the following command:

```
sudo yum update -y
```

2. Set the Linux system locale to UTF-8 running the following command:

```
sudo localectl set-locales LANG=en_US.UTF-8
```

3. Log out of the current session and log back in to apply the new locale settings.
4. Download the Veeam software repository installation package (veeam-release) from the [Veeam Download page](#):

```
sudo curl http://repository.veeam.com/yum/el/veeam-repo-1.0.1-6.x86_64.rpm --output veeam-repo.rpm
```

5. Install the Veeam software repository:

```
sudo yum install -y ./veeam-repo.rpm
```

6. Install the product from the Veeam software repository:

```
sudo yum install -y vbsf
```

The Linux package manager will start installation of Veeam Backup for Salesforce and dependencies, and then run configuration checks.

After all configuration checks complete successfully, you will be prompted to run the server configuration script. For more information, see [Configuring Server Settings](#).

```
update-alternatives: using /usr/lib/jvm/java-11-openjdk-amd64/bin/rmid to provide /usr/bin/rmid (rmid) in auto mode
update-alternatives: using /usr/lib/jvm/java-11-openjdk-amd64/bin/rmiregistry to provide /usr/bin/rmiregistry (rmiregistry) in auto mode
update-alternatives: using /usr/lib/jvm/java-11-openjdk-amd64/bin/pack200 to provide /usr/bin/pack200 (pack200) in auto mode
update-alternatives: using /usr/lib/jvm/java-11-openjdk-amd64/bin/unpack200 to provide /usr/bin/unpack200 (unpack200) in auto mode
update-alternatives: using /usr/lib/jvm/java-11-openjdk-amd64/lib/jexec to provide /usr/bin/jexec (jexec) in auto mode
Setting up vbsf (2.0.0-3813) ...
Generate product key
Created symlink /etc/systemd/system/multi-user.target.wants/vbsf-backend.service → /lib/systemd/system/vbsf-backend.service.
Created symlink /etc/systemd/system/multi-user.target.wants/vbsf-restore.service → /lib/systemd/system/vbsf-restore.service.

=====

The package "Veeam Backup for Salesforce" has been installed.
To begin with server configuration, please run the script:
sudo sh /opt/vbsf/server-configuration.sh

=====

Scanning processes...
Scanning linux images...

Running kernel seems to be up-to-date.
No services need to be restarted.
No containers need to be restarted.
No user sessions are running outdated binaries.
```

# Configuring Server Settings

To perform server configuration, run the configuration script:

```
sudo sh /opt/vbsf/server-configuration.sh
```

To complete server configuration, do the following:

1. Confirm that you have enough disk space to store backup data.

## NOTE

To store backups of Salesforce files and metadata, Veeam Backup for Salesforce will create a file repository per each protected Salesforce organization on the management server in the following folder:

`/opt/vbsf/data`. If you want to change the folder, modify the `data.storage.location` parameter value as described in section [Configuring Advanced Settings](#).

2. Choose whether you want to install PostgreSQL on the management server.

When installing PostgreSQL locally on the management server, Veeam Backup for Salesforce will run the installation script and create two users: the **postgres** user – the root database user, and the **vbsf** user – the local user. The **vbsf** user will be automatically provisioned into the default application configuration.

User credentials will be automatically generated and saved to the `/opt/vbsf/vbsf-backend/config/vbsf_default_credentials.properties` file. If you change the created passwords using the PostgreSQL standard methods, the passwords stored in the file will not automatically change and will become invalid.

## NOTE

You may want to install PostgreSQL locally on the management server to host the configuration database which will help you avoid connectivity issues. It is recommended that you create databases that will be used to protect production and sandbox Salesforce organizations on remote PostgreSQL servers. Creating the databases on the management server may cause disk space issues.

3. Confirm that you want to configure Firewalld to allow incoming HTTPS connections through port 443. This is required to access the Web UI component from a user workstation. For more information, see [Ports](#).
4. Choose whether you want to automatically configure nginx settings required for the management server to work properly.

It is recommended that you allow Veeam Backup for Salesforce to configure nginx automatically. To learn how to configure nginx manually, see this [Veeam KB article](#).

After the automatic nginx configuration completes, Veeam Backup for Salesforce displays the web address that will be used to launch the initial configuration wizard. The address contains an IPv4 address of the server and a token used to authorize the user access.

## TIP

If you accidentally close the terminal or the connection session during installation, or if you configure nginx manually, run the `sh /opt/vbsf/access_token.sh` command on the machine where Veeam Backup for Salesforce is installed to get the web address URL.

5. Copy the automatically generated URL and paste it into a web browser to proceed with the [initial configuration](#) of Veeam Backup for Salesforce.

## IMPORTANT

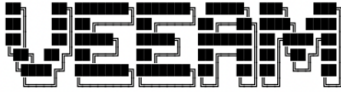
By default, the URL contains an IP address of the management server. If the specified IP address is not available over HTTPS, replace it with the public IP of the management server or the DNS name configured for the machine where the Veeam Backup for Salesforce is installed.

```
Firewalld will be configured to allow incoming https connections.

Do you want to proceed? (Yes/No): y
Rules updated
Rules updated (v6)

Configuration of nginx
=====
This step will configure the nginx service. Configuration will create or replace the following files:
%{_sysconfdir}/nginx/sites-available/vbsf-frontend.conf
%{_sysconfdir}/nginx/default.d/https.conf
%{_sysconfdir}/nginx/certs

Proceed with nginx configuration? (Yes/No): y
-----
Synchronizing state of nginx.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable nginx
Nginx configuration is finished.
```



```
*****

Veeam Backup for Salesforce installation is complete!
Please follow the link below to finish product configuration:
https://10.10.123.123/?access_token=573fbb77-e12d-75ee-e385-f80ec8dadd5f

*****
```

# Installing Veeam Backup for Salesforce on Ubuntu Machines

You can install Veeam Backup for Salesforce on an Ubuntu machine automatically using the installation script or manually.

## Installing Product Using Script

To install Veeam Backup for Salesforce, complete the following steps:

1. Set the Ubuntu system locale to UTF-8 running the following command:

```
sudo localectl set-locales LANG=en_US.UTF-8
sudo update-locale
```

2. Log out of the current session and log back in to apply the new locale settings.
3. Download the installation script to the machine where you want to deploy Veeam Backup for Salesforce running the following command:

```
sudo curl https://repository.veeam.com/apt/stable/amd64/vbsf-install-script.sh --output ./vbsf-install-script.sh
```

4. Run the script:

```
sudo bash ./vbsf-install-script.sh
```

The Ubuntu package manager will install the Veeam software repository. When the repository is installed, the manager will start installation of Veeam Backup for Salesforce and dependencies, and run configuration checks.

After all configuration checks complete successfully, you will be prompted to run the server configuration script on the Ubuntu host. For more information, see [Configuring Server Settings](#).

## Installing Product Manually

To install Veeam Backup for Salesforce, complete the following steps:

1. Update all installed Ubuntu packages and their dependencies running the following command:

```
sudo apt update -y
```

2. Set the Ubuntu system locale to UTF-8 running the following command:

```
sudo localectl set-locales LANG=en_US.UTF-8
sudo update-locale
```

3. Log out of the current session and log back in to apply the new locale settings.
4. Download the Veeam software repository installation package (veeam-release) from the [Veeam Download page](#):

```
sudo curl http://repository.veeam.com/apt/stable/amd64/veeam-repo_1.0.0-13_amd64.deb --output veeam-repo.deb
```

5. Install the Veeam software repository:

```
sudo apt install -y ./veeam-repo.deb
```

6. Install the product from the Veeam software repository:

```
sudo apt-get -y update
sudo apt install -y vbsf
```

The Ubuntu package manager will start installation of Veeam Backup for Salesforce and dependencies, and then run configuration checks.

After all configuration checks complete successfully, you will be prompted to run the server configuration script. For more information, see [Configuring Server Settings](#).

```
update-alternatives: using /usr/lib/jvm/java-11-openjdk-amd64/bin/rmid to provide /usr/bin/rmid (rmid) in auto mode
update-alternatives: using /usr/lib/jvm/java-11-openjdk-amd64/bin/rmiregistry to provide /usr/bin/rmiregistry (rmiregistry) in auto mode
update-alternatives: using /usr/lib/jvm/java-11-openjdk-amd64/bin/pack200 to provide /usr/bin/pack200 (pack200) in auto mode
update-alternatives: using /usr/lib/jvm/java-11-openjdk-amd64/bin/unpack200 to provide /usr/bin/unpack200 (unpack200) in auto mode
update-alternatives: using /usr/lib/jvm/java-11-openjdk-amd64/lib/jexec to provide /usr/bin/jexec (jexec) in auto mode
Setting up vbsf (2.0.0-3813) ...
Generate product key
Created symlink /etc/systemd/system/multi-user.target.wants/vbsf-backend.service → /lib/systemd/system/vbsf-backend.service.
Created symlink /etc/systemd/system/multi-user.target.wants/vbsf-restore.service → /lib/systemd/system/vbsf-restore.service.
=====

The package "Veeam Backup for Salesforce" has been installed.

To begin with server configuration, please run the script:
sudo bash /opt/vbsf/server-configuration.sh
=====

Scanning processes...
Scanning linux images...

Running kernel seems to be up-to-date.
No services need to be restarted.
No containers need to be restarted.
No user sessions are running outdated binaries.
```



# Configuring Server Settings

To perform server configuration, run the configuration script:

```
sudo bash /opt/vbsf/server-configuration.sh
```

To complete server configuration, do the following:

1. Confirm that you have enough disk space to store backup data.

## NOTE

To store backups of Salesforce files and metadata, Veeam Backup for Salesforce will create a file repository per each protected Salesforce organization on the management server in the following folder:

`/opt/vbsf/data`. If you want to change the folder, modify the `data.storage.location` parameter value as described in section [Configuring Advanced Settings](#).

2. Choose whether you want to install PostgreSQL on the management server.

When installing PostgreSQL locally on the management server, Veeam Backup for Salesforce will run the installation script and create two users: the **postgres** user – the root database user, and the **vbsf** user – the local user. The **vbsf** user will be automatically provisioned into the default application configuration.

User credentials will be automatically generated and saved to the `/opt/vbsf/vbsf-backend/config/vbsf_default_credentials.properties` file. If you change the created passwords using the PostgreSQL standard methods, the passwords stored in the file will not automatically change and will become invalid.

## NOTE

You may want to install PostgreSQL locally on the management server to host the configuration database which will help you avoid connectivity issues. It is recommended that you create databases that will be used to protect production and sandbox Salesforce organizations on remote PostgreSQL servers. Creating the databases on the management server may cause disk space issues.

3. Confirm that you want to configure firewall to allow incoming HTTPS connections through port 443. This is required to access the Web UI component from a user workstation. For more information, see [Ports](#).
4. Choose whether you want to automatically configure nginx settings required for the management server to work properly.

It is recommended that you allow Veeam Backup for Salesforce to configure nginx automatically. To learn how to configure nginx manually, see this [Veeam KB article](#).

After the automatic nginx configuration completes, Veeam Backup for Salesforce displays the web address that will be used to launch the initial configuration wizard. The address contains an IPv4 address of the server and a token used to authorize the user access.

## TIP

If you accidentally close the terminal or the connection session during installation, or if you configure nginx manually, run the `sh /opt/vbsf/access_token.sh` command on the machine where Veeam Backup for Salesforce is installed to get the web address URL.

5. Copy the automatically generated URL and paste it into a web browser to proceed with the [initial configuration](#) of Veeam Backup for Salesforce.

## IMPORTANT

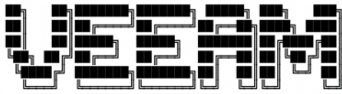
By default, the URL contains an IP address of the management server. If the specified IP address is not available over HTTPS, replace it with the public IP of the management server or the DNS name configured for the machine where the Veeam Backup for Salesforce is installed.

```
UFW will be configured to allow incoming https connections.

Do you want to proceed? (Yes/No): y
Rules updated
Rules updated (v6)

Configuration of nginx
=====
This step will configure the nginx service. Configuration will create or replace the following files:
%{_sysconfdir}/nginx/sites-available/vbsf-frontend.conf
%{_sysconfdir}/nginx/default.d/https.conf
%{_sysconfdir}/nginx/certs

Proceed with nginx configuration? (Yes/No): y
-----
Synchronizing state of nginx.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable nginx
Nginx configuration is finished.
```



```
*****

Veeam Backup for Salesforce installation is complete!
Please follow the link below to finish product configuration:
https://10.10.123.123/?access_token=573fbb77-e12d-75ee-e385-f80ec8dadd5f

*****
```

# Performing Initial Configuration

To start working with Veeam Backup for Salesforce, you must perform the initial configuration of the management server. To do that, in a web browser, navigate to the web address that has been automatically generated by Veeam Backup for Salesforce during installation. The address must contain a public IPv4 address or DNS name of the server that is available over HTTPS, and a token used to authorize the first user access.

The unique token is not dependent on the host name. If the host is accessible by several IP addresses, or you have configured a proper domain name, you can replace the host address with the more appropriate one.

## IMPORTANT

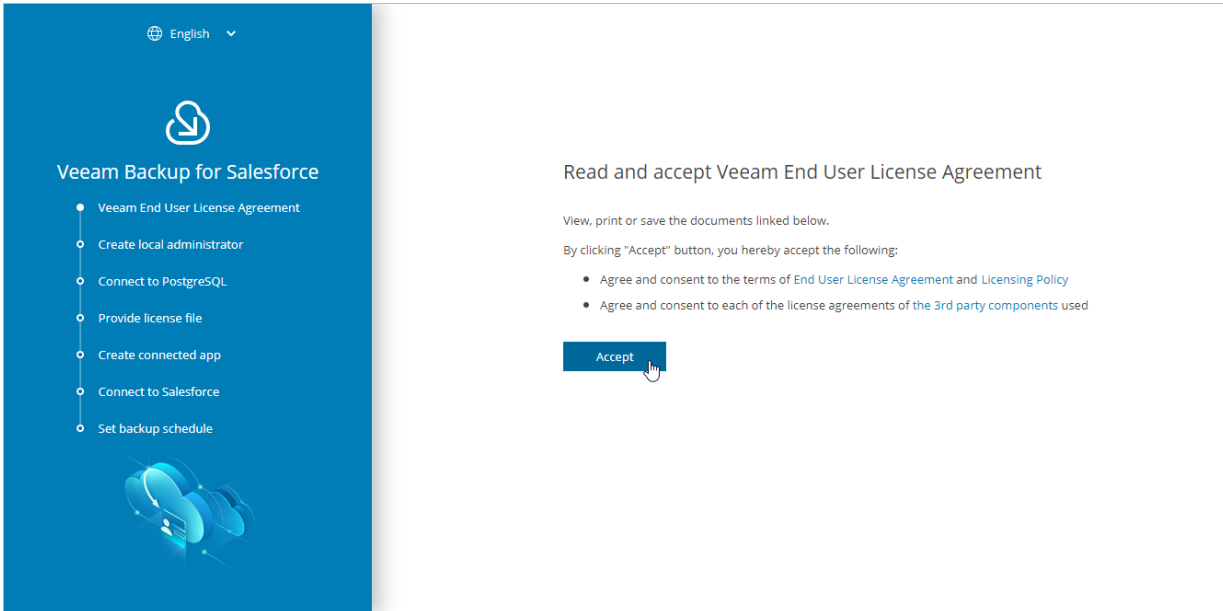
- Internet Explorer is not supported. To access Veeam Backup for Salesforce, use the latest versions of Microsoft Edge, Mozilla Firefox (except Mozilla Firefox for Linux), Safari and Google Chrome.
- You must be able to access the Salesforce authentication webpage from the machine that you use to log in to Veeam Backup for Salesforce.
- The management server is using a self-signed SSL certificate for nginx. However, this certificate is not trusted and will trigger a browser certificate warning. You can replace the certificate manually to the trusted one as soon as you finish the configuration, as described in [Appendix B. Replacing Security Certificate](#).

To configure the management server, complete the initial configuration wizard:

1. [Read and accept license agreement.](#)
2. [Create the default administrator.](#)
3. [Connect to a PostgreSQL database.](#)
4. [Provide a Veeam Backup for Salesforce license file.](#)
5. [Create a Salesforce Connected App.](#)
6. [Connect to a Salesforce organization.](#)
7. [Specify backup schedule settings.](#)
8. [Finish working with the wizard.](#)

# Step 1. Accept License Agreement

At the **Veeam End User License Agreement** step of the wizard, read and accept the Veeam license agreement, Veeam licensing policy and 3rd party components license agreements. If you reject the agreements, you will not be able to continue initial configuration.

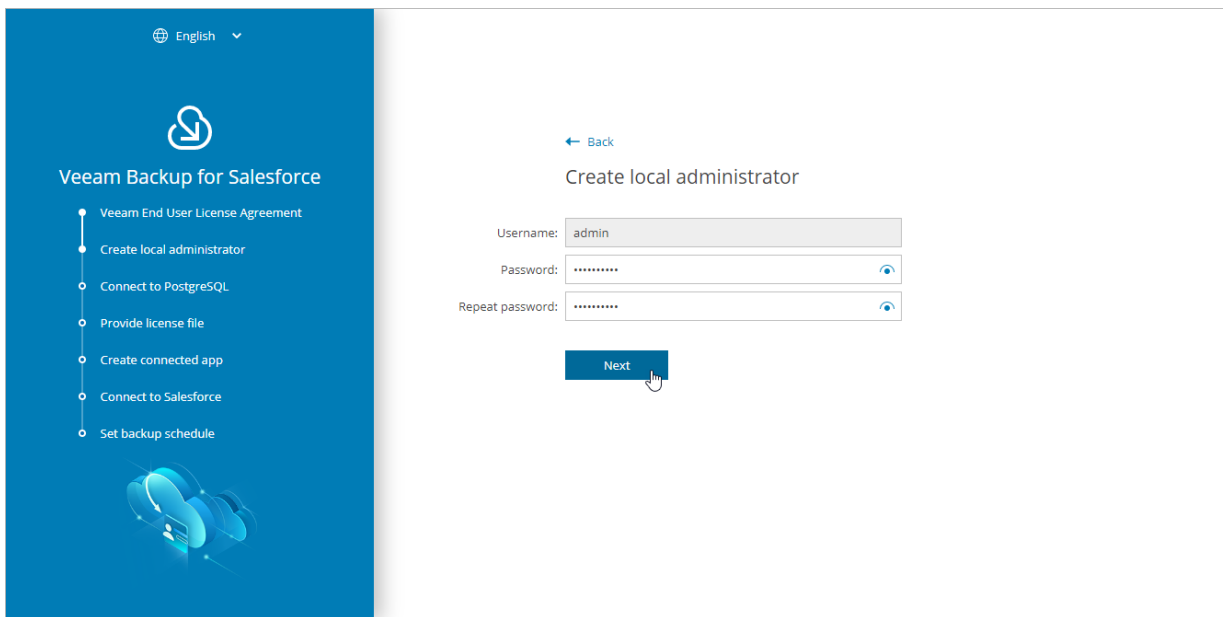


## Step 2. Create Local Administrator

At the **Create local administrator** step of the wizard, specify a password for the local administrator account. The password must contain uppercase and lowercase Latin letters and special characters (!@#\$%^&`~\*()\_-+=[]{};:\",./<>?). The minimum length of the password is 8 characters. You can change the password of the local administrator as described in section [Editing Users](#).

This is the only local user account that can perform all operations in Veeam Backup for Salesforce including configuration of [IdP and SSO settings](#). Consider that you will not be able to remove or change this account using the Web UI.

After you finish the initial configuration, you will be able to add other users and assign them granular permissions. For more information, see [Managing Users](#).



The screenshot displays the 'Create local administrator' step of the Veeam Backup for Salesforce wizard. On the left, a blue sidebar contains the Veeam logo and a list of steps: 'Veeam End User License Agreement', 'Create local administrator' (highlighted), 'Connect to PostgreSQL', 'Provide license file', 'Create connected app', 'Connect to Salesforce', and 'Set backup schedule'. The main content area shows a 'Back' link, the title 'Create local administrator', and three input fields: 'Username' with the value 'admin', 'Password' (masked with dots), and 'Repeat password' (also masked with dots). Each password field has an eye icon for visibility toggling. A 'Next' button is positioned below the fields, with a mouse cursor hovering over it.

## Step 3. Connect to PostgreSQL

At the **Connect to PostgreSQL** step of the wizard, [specify connection settings](#) that will be used to access the following databases:

- The configuration database that will be used to store product data, backup policies, restore jobs, sessions and so on.
- A database that will be used to store backups of all objects, fields, records and relationships of the Salesforce organization connected at [step 6](#) of the wizard.

### NOTE

If you perform configuration of the existing deployment of Veeam Backup for Salesforce, specify connection settings that will be used to access the existing configuration database.

You can also [configure a web proxy](#) that will be used by Veeam Backup for Salesforce to access Salesforce and the Veeam License Server if the management server is not connected to the internet.

## Step 3a. Connect to Database

To configure connection settings, do the following at the **Connect to PostgreSQL** step of the wizard:

1. In the **PostgreSQL address** field, specify the DNS name or IP address of a PostgreSQL server that will host the databases.
2. In the **Port** field, choose a network port that will be used by Veeam Backup for Salesforce to connect to the PostgreSQL server. The default port number is 5432.
3. Use the **Username** and **Password** fields to provide credentials of the PostgreSQL user that will be used to access the databases. The user must be assigned permissions required to create database schemas.

Keep in mind that if you want Veeam Backup for Salesforce to be able to create the required databases automatically, the user must also be assigned permissions required to create databases. Otherwise, you have to create the empty databases on the specified server manually beforehand.

### NOTE

If you have chosen the option to automatically install PostgreSQL on the management server during Veeam Backup for Salesforce deployment, this step will contain the predefined values: in the **PostgreSQL address** field, the address of the management server will be specified, in the **Username** and **Password** fields, credentials of the **vbsf** PostgreSQL user created when installing PostgreSQL will be provided.

By default, Veeam Backup for Salesforce creates new databases with the following names:

- **vbsf\_backup** – the name used for the database that will store the backed-up data.
- **vbsf\_application** – the name used for the configuration database.

If you want to rename the databases or specify the existing ones, set the **Customize** toggle to *On*, and specify the custom names.

### TIP

During the initial configuration, you will be prompted to connect to a Salesforce organization that will be protected by a backup policy, which is automatically created by the product. You can skip the default policy creation and connect to a database later [when creating a backup policy](#).



## Veeam Backup for Salesforce

- Veeam End User License Agreement
- Create local administrator
- **Connect to PostgreSQL**
- Provide license file
- Create connected app
- Connect to Salesforce
- Set backup schedule



### Connect to PostgreSQL server

PostgreSQL address: localhost

Port: 5432

Username: vbsf

Password: (configured password)

Customize:  On ⓘ

#### Application databases

Configuration database: veeam

Salesforce data: veeam\_data

Skip backup policy creation

#### Proxy server settings

Proxy server connection: Not configured...

Next



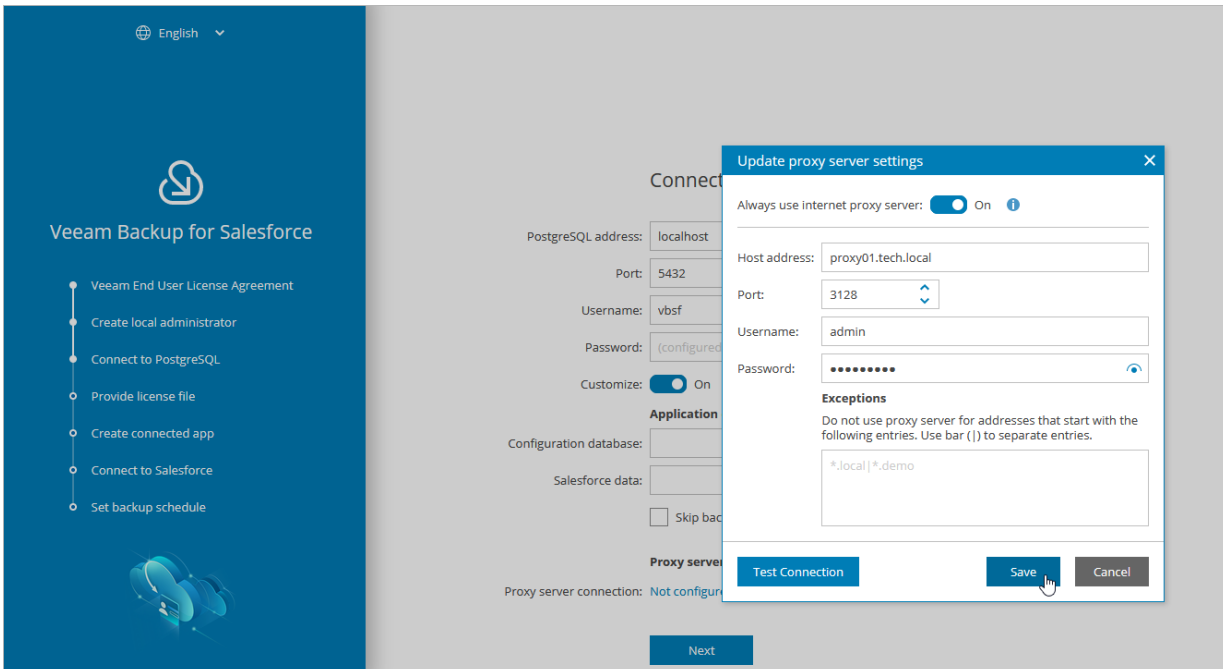
# Step 3b. Connect to Proxy Server

If you want to connect to the internet through a web proxy, do the following:

1. In the **Proxy server settings** section of the **Connect to PostgreSQL** step of the wizard, set the **Customize** toggle to *On*.
2. Click the link in the **Proxy server connection** field.
3. Specify the following settings in the **Update proxy server settings** window:
  - a. Set the **Always use internet proxy server** toggle to *On*.
  - b. In the **Host address** field, enter the IP address or FQDN of the web proxy.
  - c. In the **Port** field, enter the port that will be used on the web proxy for HTTP or HTTPS connections.
  - d. [Applies only if the web proxy requires authentication] Use the **Username** and **Password** fields to provide credentials of the user account configured on the web proxy to access the internet.
  - e. In the **Exceptions** section, you can specify a domain name which you do not want Veeam Backup for Salesforce to access through the configured web proxy. To specify multiple domain names, use a pipe-separated list.
  - f. Click **Apply**.

## TIP

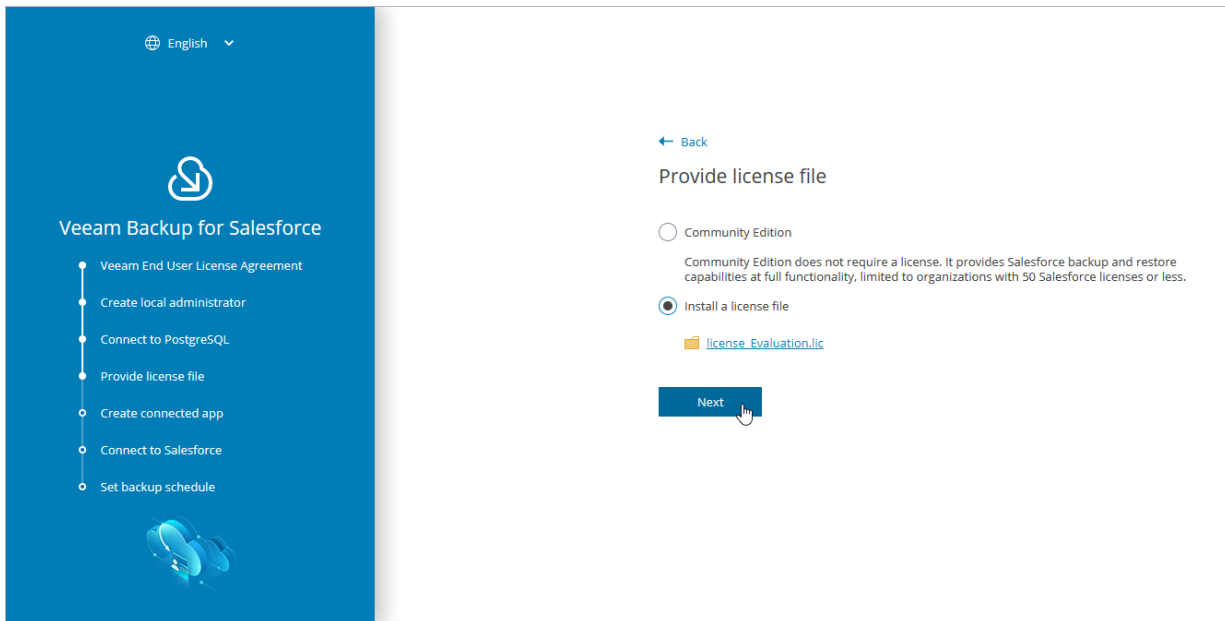
You can skip this step and provide the web proxy settings later. To do that, modify the `proxy.settings` parameter values as described in section [Configuring Advanced Settings](#).



# Step 4. Provide License File

At the **Provide license file** step of the wizard, select the **Install a license file** option and browse to the license file supplied to you by Veeam. After you install the license file, Veeam Backup for Salesforce will connect to the Veeam License Server and start the license validation process. As soon as validation completes, you will be able to proceed to the next step of the wizard.

If you do not have a valid license, you can [get a 30-day trial license key](#) or proceed with the wizard without providing a license. To proceed with the wizard without providing a license, select the **Community Edition** option. In this case, the built-in *Community Edition* license that allows you to protect Salesforce organizations with up to 50 Users will be installed. For more information on license types, see [Licensing](#).



# Step 5. Create Connected App

At the **Create Connected App** step of the wizard, you must configure a Connected App in Salesforce. Security credentials of the Connected App will be used to authorize access to all Salesforce organizations protected by this Veeam Backup for Salesforce installation.

Salesforce Connected App allows Veeam Backup for Salesforce to authenticate with Salesforce and get access to resources that will be protected. You can create the Connected App in any Salesforce organization. To learn how to create the Connected App, see [this Veeam KB article](#).

## NOTE

You will be able to change the Connected App as described in section [Changing Connected App Tokens](#), but you must consider that after changing the Connected App, you will have to re-authorize all Salesforce connections added to Veeam Backup for Salesforce.

When you create the Connected App, consider the following:

- Creation of the Connected App and any changes to its configuration will take up to 10 minutes to apply on the Salesforce side.
- The Connected App must be assigned the **Full access (full)**, **Perform requests at any time** (refresh\_token, offline\_access) and **Access unique user identifiers** (openid) OAuth scopes. For more information on OAuth scopes in Salesforce, see [Salesforce Documentation](#).
- The following options must be enabled: **Enable oAuth Settings**, **Require Secret for Web Server Flow** and **Require Secret for Refresh Token Flow**.
- The callback URL specified in the *Callback URLs* list of the Connected App must match the management server FQDN that you use to access the Veeam Backup for Salesforce Web UI.

Consider the following example:

You installed Veeam Backup for Salesforce on the machine with the following IP address: *172.12.0.1*. To properly configure the Connected App, you have copied the URL from the **Callback URL** field at the **Create connected app** step of the initial configuration wizard and added it to the Connected App *Callback URLs* list.

Later, you decide to create the following DNS name for the machine running Veeam Backup for Salesforce: *acme.internal.com*. In this case, you must add the following callback URL to the Connected App *Callback URLs* list: *https://acme.internal.com*.

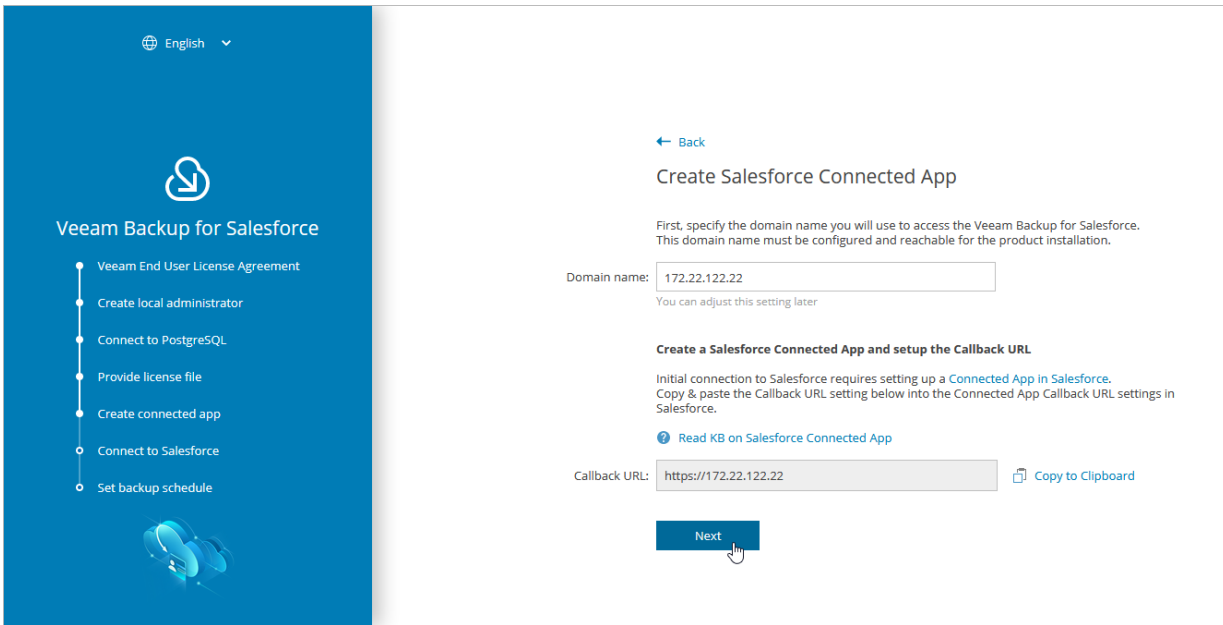
After that, your *Callback URLs* list will contain the following URLs:

- <https://172.12.0.1>
- <https://acme.internal.com>

## IMPORTANT

You can protect multiple Salesforce organizations using a single Veeam Backup for Salesforce installation. However, due to the Salesforce Connected App limit of 5 authorizations per client, authorization issues may occur when you have several product installations leveraging the same Connected App. That is why it is recommended that you create a dedicated Connected App for each product deployment.

For more information on Salesforce OAuth Authorization Flows and Connected Apps, see [Salesforce Documentation](#).



# Step 6. Connect to Salesforce

At the **Connect to Salesforce** step of the wizard, connect to a Salesforce organization that will be automatically added to Veeam Backup for Salesforce and protected by the default backup policy. The backup policy is created by Veeam Backup for Salesforce during the initial configuration unless you disabled the default policy creation at [step 3](#) of the wizard. For more information on backup policies, see [Performing Backup](#).

To connect to the organization, do the following:

1. Choose whether you want to connect to a Salesforce organization hosted on a production instance, sandbox instance or custom domain.

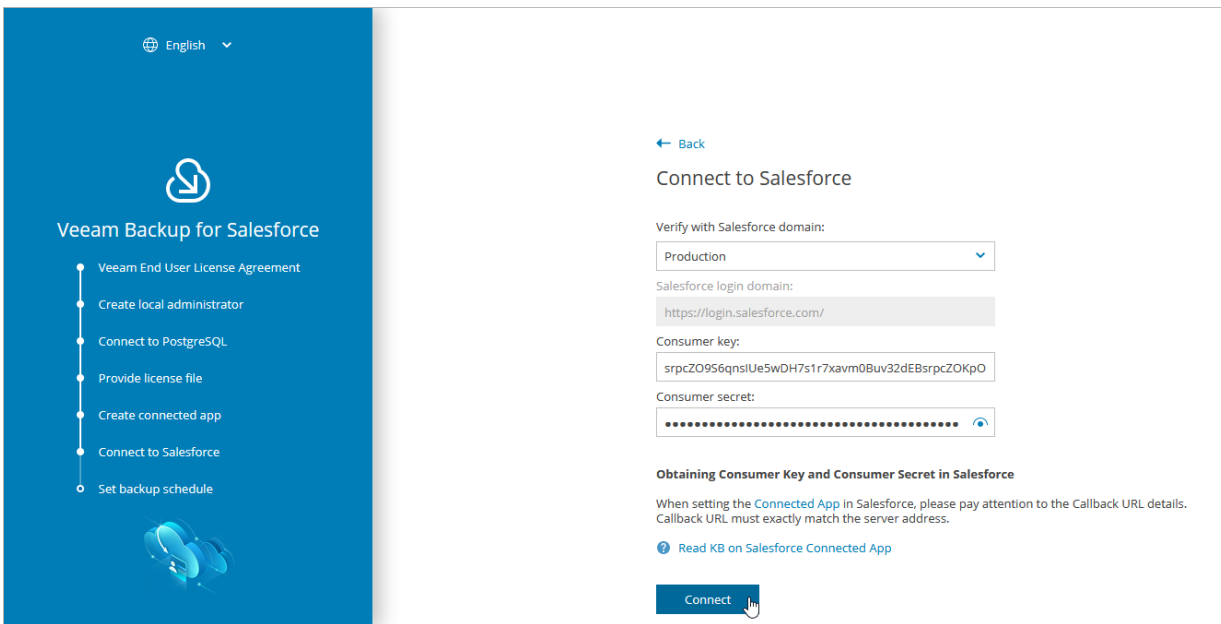
If you select the **Custom** option, you must also provide the organization domain name. If you specify a *lightning.force.com*, *my.salesforce-sites.com* or *my.site.com* domain names, keep in mind that the product will automatically change this name to *my.salesforce.com*.

2. Provide the consumer key and consumer secret created in the Connected App, and click **Connect**. You will be redirected to the Salesforce authentication webpage.

To learn how to create the key and the secret, see [this Veeam KB article](#).

## IMPORTANT

It takes up to 10 minutes for Salesforce to apply any changes in a Connected App. During this time you may get an error that key and secret pair is not active or a callback URL is configured incorrectly.



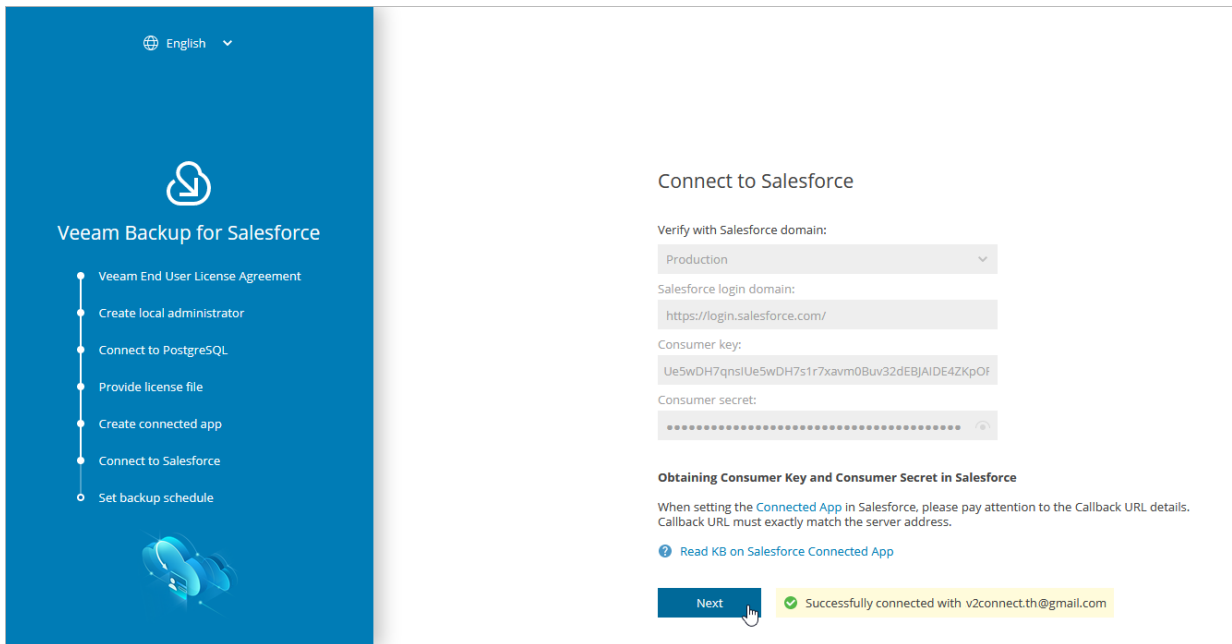
3. On the Salesforce authentication webpage, enter credentials of an account created in the Salesforce organization that you want to protect, and click **Log in**.

The specified account must be assigned permissions required for Veeam Backup for Salesforce to be able to perform backup and restore operations. For more information, see [Required Permissions](#).

## NOTE

Veeam Backup for Salesforce does not have access to Salesforce user credentials. To authorize and access Salesforce data, Veeam Backup for Salesforce uses OAuth tokens of the Connected App created during the [initial configuration](#). You can change the Connected App as described in section [Changing Connected App Tokens](#), but you must consider that after changing the Connected App, you will have to re-authorize all Salesforce connections added to Veeam Backup for Salesforce.

4. Back to the **Veeam Backup for Salesforce** wizard, click **Next** to proceed with the initial configuration.



# Step 7. Set Backup Policy Schedule

[Applies only if you have not selected the **Skip backup policy creation** check box]

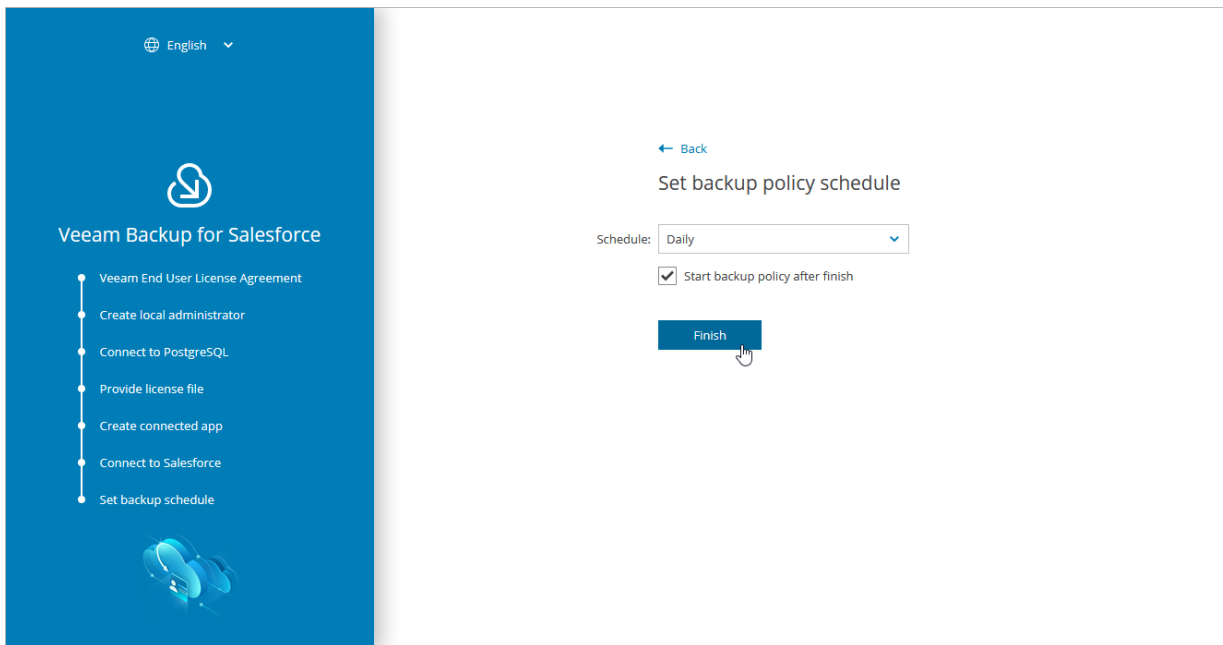
At the **Set backup schedule** step of the wizard, choose one of the built-in schedules that will be used to run the backup policy:

- **Hourly** – select this schedule if you want the backup policy session to be launched at the beginning of every hour.
- **Daily** – select this schedule if you want the backup policy session to be launched every day at 00:00 UTC.
- **Weekly** – select this schedule if you want the backup policy session to be launched every Sunday at 00:00 UTC.

You can change these settings later as described in section [Editing Backup Policies](#).

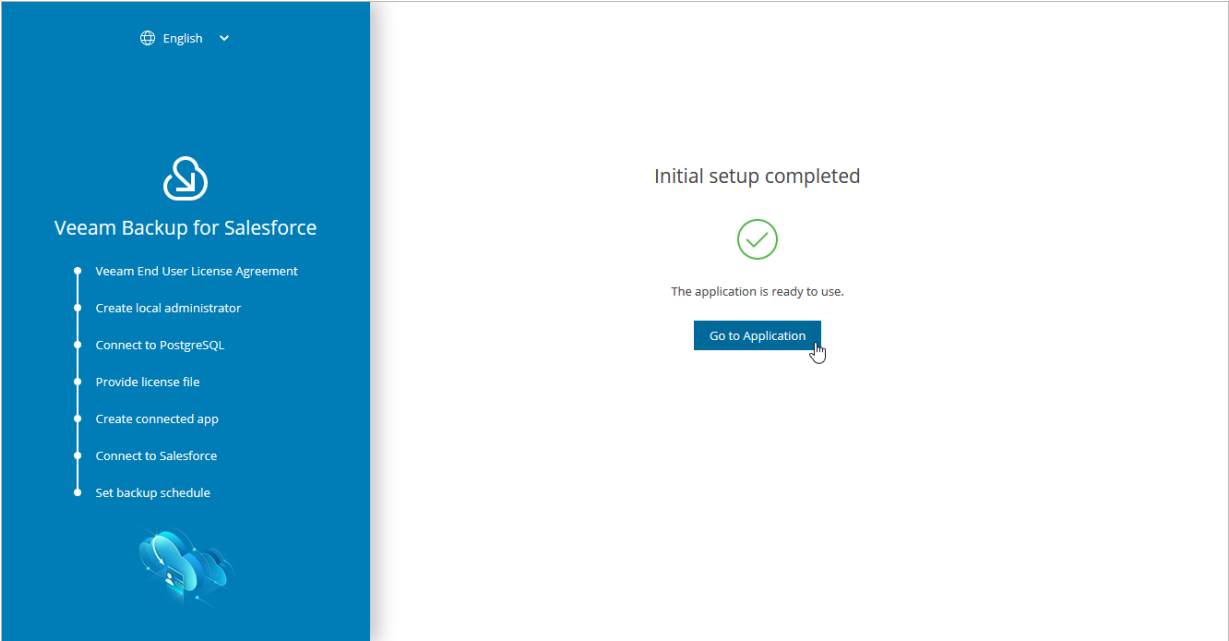
## TIP

If you want Veeam Backup for Salesforce to start a backup session for the Salesforce organization right after the initial configuration process completes, select the **Start backup policy after finish** check box.



# Step 8. Finish Working with Wizard

At the last step of the wizard, click **Go to Application**. After the initial configuration process completes, Veeam Backup for Salesforce will open the product Web UI.





# Accessing Veeam Backup for Salesforce

To access Veeam Backup for Salesforce, in a web browser, navigate to the Veeam Backup for Salesforce web address. The address consists of a public IPv4 address or a DNS name of the machine where Veeam Backup for Salesforce is installed. Keep in mind that the website is available over HTTPS only.

## IMPORTANT

Internet Explorer is not supported. To access Veeam Backup for Salesforce, use the latest versions of Microsoft Edge, Mozilla Firefox (except Mozilla Firefox for Linux), Safari or Google Chrome.

## Logging In

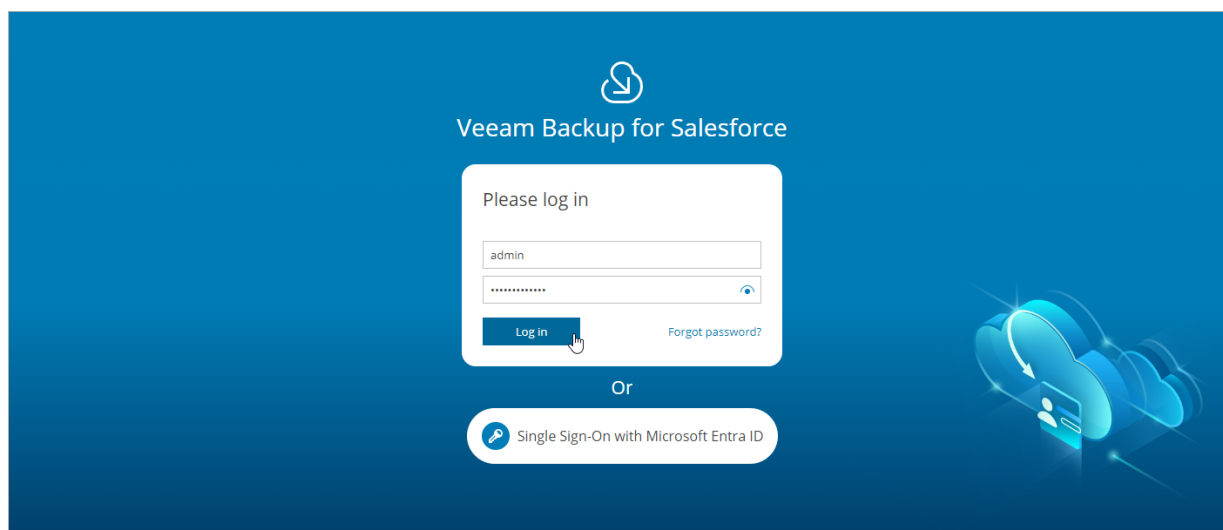
To log in to Veeam Backup for Salesforce, do the following:

1. In the **Username** and **Password** fields, specify credentials of a Veeam Backup for Salesforce user.

If you log in for the first time, use credentials of the default Administrator that was created after the product installation. In future, you can add other user accounts to grant access to Veeam Backup for Salesforce. For more information, see [Managing Users](#).

2. Click **Log in**.

If you have previously connected a Microsoft Entra ID or enabled a Salesforce organization as an identity provider in Veeam Backup for Salesforce, you can click **Single Sign-On with Microsoft Entra ID** or **Single Sign-On with Salesforce**. You will be redirected to the authorization page. If you have not logged in yet, log in to the identity provider portal. After that, you will be redirected to the Veeam Backup for Salesforce page as an authorized user. To learn how to configure the identity provider in Veeam Backup for Salesforce, see [Configuring IdP and SSO Settings](#).



## Logging Out

To log out, at the top right corner of the Veeam Backup for Salesforce page, click the user name and then click **Log out**.

# Configuring Veeam Backup for Salesforce

Right after you perform the [initial configuration](#), you can start working with Veeam Backup for Salesforce. If you want to add users that can access Veeam Backup for Salesforce, to add databases used to protect Salesforce organizations, and to configure additional settings, follow the instructions in these sections:

- [Managing Salesforce Organizations](#)
- [Managing Companies](#)
- [Managing Databases](#)
- [Managing Users](#)
- [Configuring Security Settings](#)
- [Configuring Encryption Settings](#)
- [Viewing Audit Trail](#)
- [Managing Alerts](#)
- [Configuring Advanced Settings](#)

# Managing Salesforce Organizations

Salesforce organizations can be added to Veeam Backup for Salesforce either automatically when you create [backup policies](#) or manually as described in section [Adding Organizations](#). When you connect to a Salesforce organization, the basic organization details and the OAuth authentication tokens of the Connected App are saved to the configuration database.

## NOTE

Veeam Backup for Salesforce does not have access to Salesforce user credentials. To authorize and access Salesforce data, Veeam Backup for Salesforce uses OAuth tokens of the Connected App created during the [initial configuration](#). You can change the Connected App as described in section [Changing Connected App Tokens](#), but you must consider that after changing the Connected App, you will have to re-authorize all Salesforce connections added to Veeam Backup for Salesforce.

Salesforce organizations added to Veeam Backup for Salesforce are grouped to companies. For more information on companies, see [Managing Companies](#).

## In This Section

- [Adding Organizations](#)
- [Editing Organizations](#)
- [Removing Organizations](#)

# Adding Organizations

To add a new Salesforce organization, do the following:

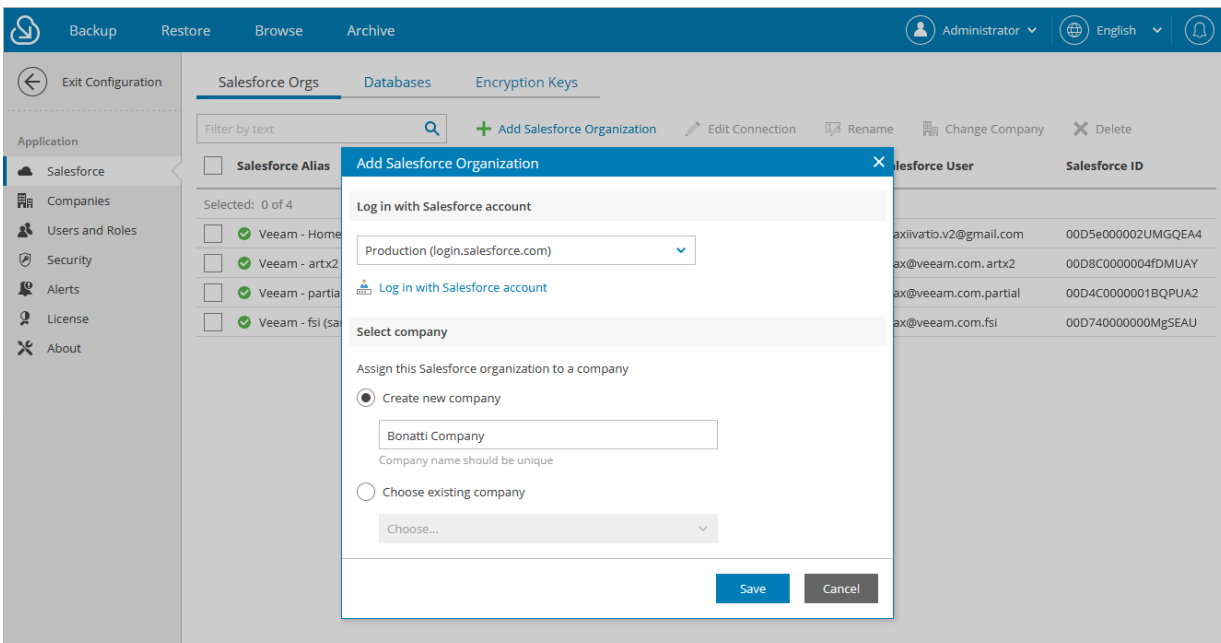
1. Switch to the **Configuration** page.
2. Navigate to **Salesforce > Salesforce Orgs.**
3. Click **Add Salesforce Organization**. The **Add Salesforce Organization** window will open.
4. In the **Log in with Salesforce account** section, connect to a Salesforce organization that you want to add. To do that:
  - a. Choose whether you want to use a Salesforce organization hosted on a production instance, sandbox instance or custom domain. If you select the **Custom** option, you must also specify the organization domain name.
  - b. Click **Log in with Salesforce account**. You will be redirected to the Salesforce authentication webpage.
  - c. On the Salesforce authentication webpage, enter credentials of a Salesforce user of the organization that you want to add, and click **Log in**. After that, you will be redirected back to the **Add Salesforce Organization** window in Veeam Backup for Salesforce.

The specified Salesforce user must be assigned permissions required for Veeam Backup for Salesforce to be able to perform backup and restore operations. For information, see [Required Permissions](#).

5. In the **Add Salesforce Organization** window, in the **Select company** section, choose whether you want to assign the organization to an existing or to a new company:
  - If you want to add a new company to Veeam Backup for Salesforce and to assign the organization to it, select the **Create new company** option, and specify a name for the new company.
  - If you want to assign the organization to an existing company, select the **Choose existing company** option, and choose the necessary company from the drop-down list.

For a company to be displayed in the list of available companies, it must be created as described in section [Adding Companies](#).

6. Click **Save**.



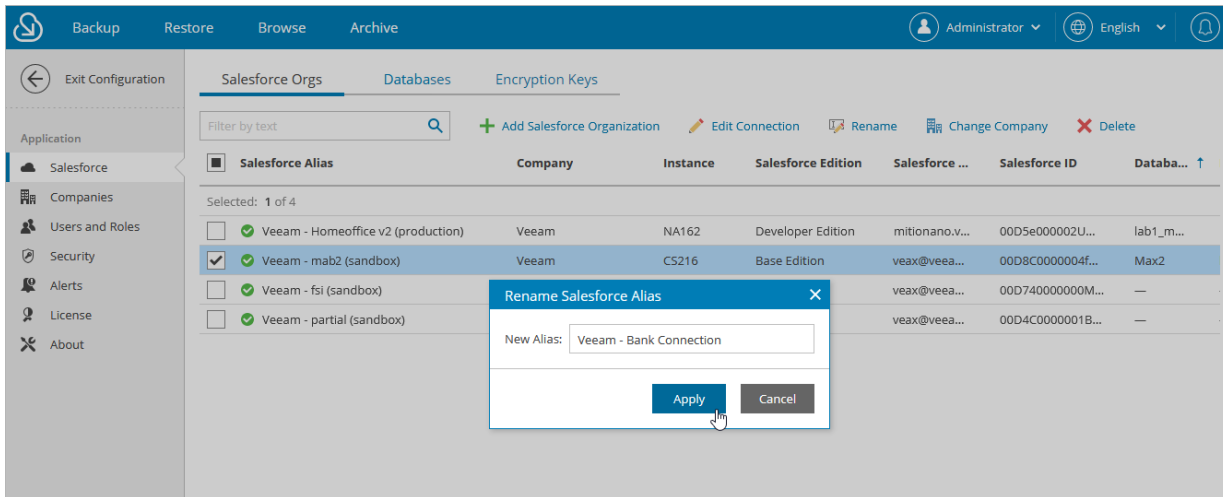
# Editing Organizations

For each Salesforce organization added to the configuration database, you can change the alias – organization name displayed in the Veeam Backup for Salesforce Web UI, [edit connection settings](#) and re-assign the organization to another company.

## Renaming Organizations

When you connect to a Salesforce organization, Veeam Backup for Salesforce automatically collects basic organization details and uses the organization ID to create an alias. To change the alias, do the following:

1. Switch to the **Configuration** page.
2. Navigate to **Salesforce > Salesforce Orgs**.
3. Select the necessary organization and click **Rename**.
4. In the **Rename Salesforce Alias** window, specify a new name that will be displayed in the **Salesforce Alias** column of the **Salesforce Orgs** tab, and click **Apply**.

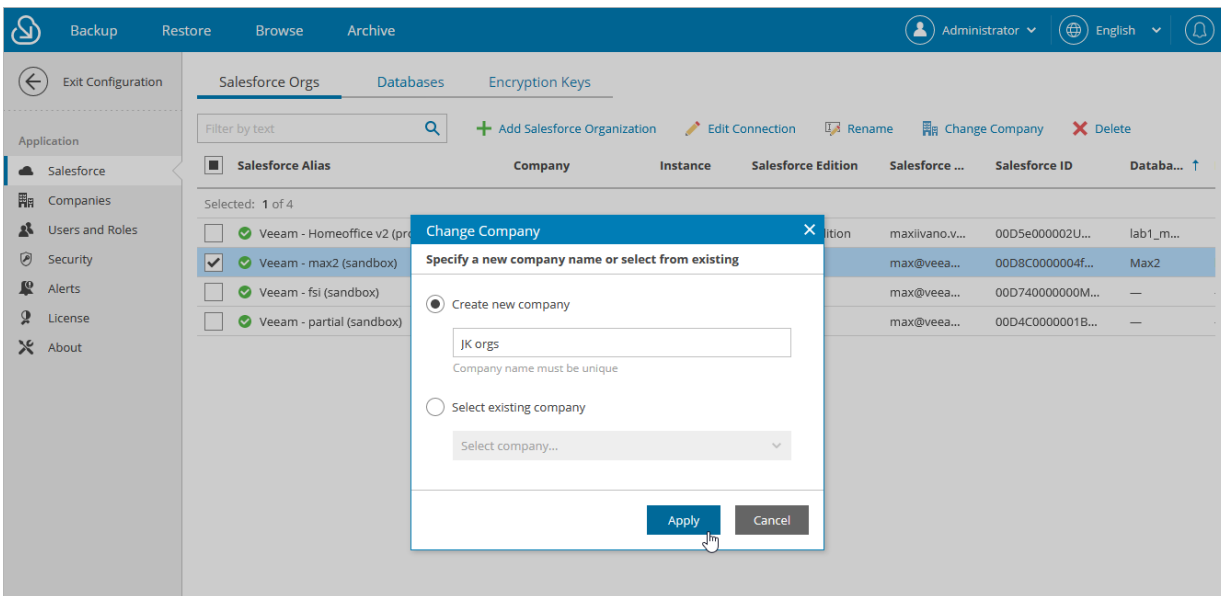


# Changing Company

To assign organizations to another company, do the following:

1. Switch to the **Configuration** page.
  2. Navigate to **Salesforce > Salesforce Orgs.**
  3. Select the necessary organization, and click **Change Company.**
  4. In the **Change Company** window:
    - a. Choose whether you want to assign the organization to an existing or to a new company.
      - If you want to add a new company to Veeam Backup for Salesforce and to re-assign the organization to this company, select the **Create new company** option, and specify a name for the new company.
      - If you want to re-assign the organization to an existing company, select the **Select existing company** option, and choose the necessary company from the drop-down list.
- For a company to be displayed in the list of available companies, it must be created as described in section [Adding Companies](#).

b. Click **Apply**.



## Editing Connections

To authorize connections to Salesforce organizations, Veeam Backup for Salesforce uses the Salesforce Connected App specified either during the [initial configuration](#) or on the Connected App tab as described in section [Changing Connected App Tokens](#). When you change the Connected App, connections to all Salesforce organizations added to Veeam Backup for Salesforce must be re-authorized. To do that, you can reconnect to organizations in [backup policy settings](#) or edit connection settings for the organizations.

## IMPORTANT

If you enable enhanced domains in Salesforce, URLs of your Salesforce organizations will change and backup policies will fail to connect to Salesforce. To resolve the issue, edit the connection URL of the Salesforce organization when it is in the failed state. The link to change the URL will appear at the **Connect** step of the **Edit Salesforce organization** wizard.

For more information on enhanced domains, see [Salesforce Documentation](#).

To edit connection settings for a Salesforce organization, do the following:

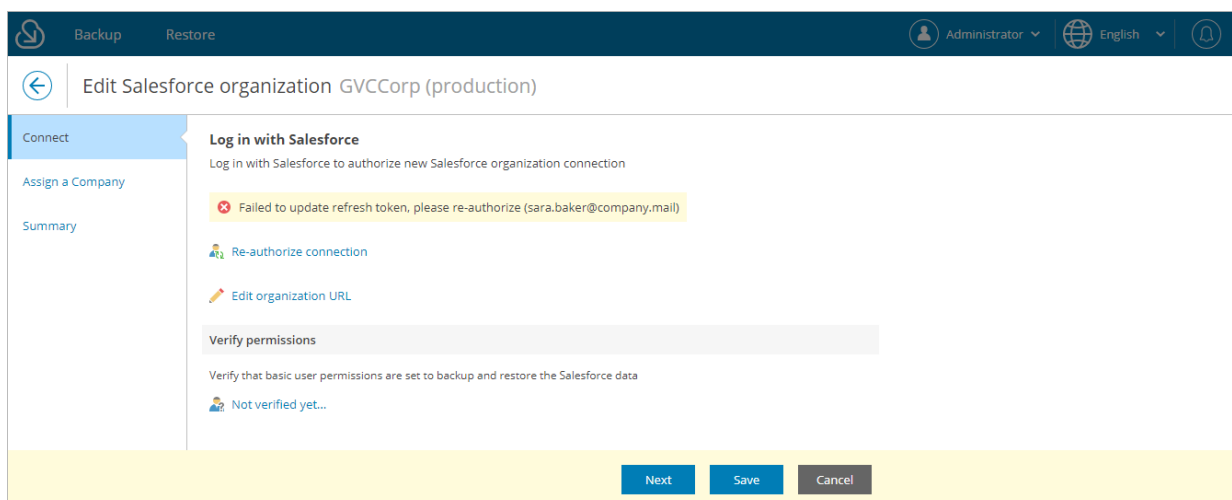
1. Switch to the **Configuration** page.
2. Navigate to **Salesforce > Salesforce Orgs**.
3. Select the necessary organization and click **Edit Connection**.  
The **Edit Salesforce organization** wizard will open.
4. At the **Connect** step of the wizard:
  - a. To re-authorize connection to the organization, click **Re-authorize connection**. You will be redirected to the Salesforce authentication webpage.

On the Salesforce authentication webpage, enter credentials of the Salesforce user and click **Log in**. The specified user must be assigned permissions required for Veeam Backup for Salesforce to be able to perform backup and restore operations. For information, see [Required Permissions](#).

## NOTE

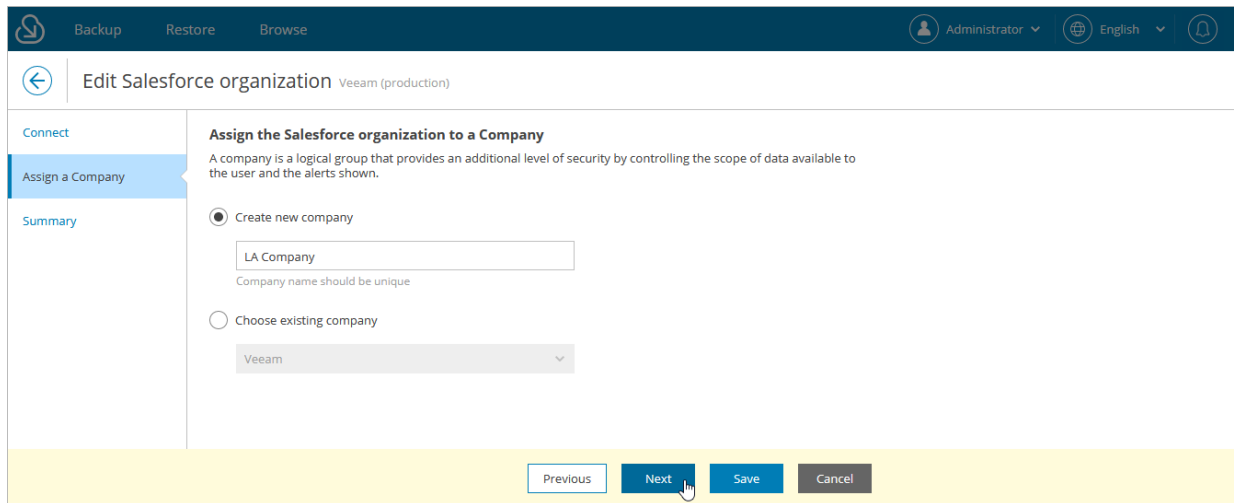
Veeam Backup for Salesforce does not store credentials of the Salesforce user used to log in to Salesforce. To authorize in Salesforce and access Salesforce data, Veeam Backup for Salesforce uses the Connected App.

- b. [This step applies only if you have enabled enhanced domains in Salesforce] To edit the connection URL of the Salesforce organization, click **Edit organization URL**, provide the new URL in the **Edit organization URL** window and click **Apply**.
- c. To verify whether permissions assigned to the specified user are enough to perform backup and restore operations, click the link in the **Verify permissions** section and wait for the check to complete. If any of the permissions are missing, you must grant them in the Salesforce console manually as described in [Salesforce documentation](#).

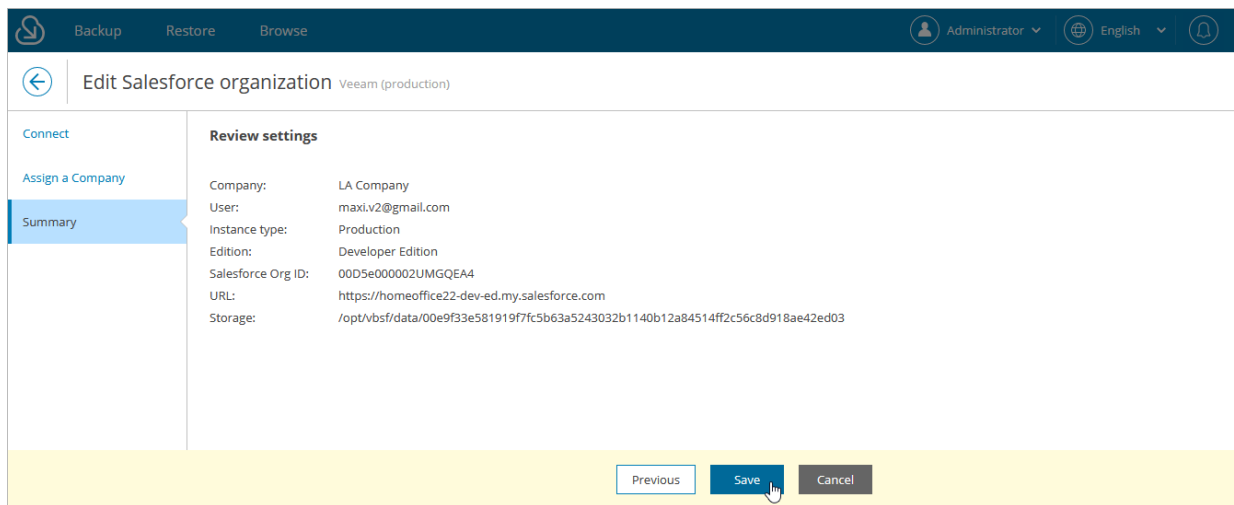


- At the **Assign a Company** step of the wizard, choose whether you want to re-assign the organization to another company:
  - If you want to add a new company to Veeam Backup for Salesforce and to re-assign the organization to this company, select the **Create new company** option, and specify a name for the new company.
  - If you want to re-assign the organization to an existing company, select the **Choose existing company** option, and choose the necessary company from the drop-down list.

For a company to be displayed in the list of available companies, it must be created as described in section [Adding Companies](#).



- At the **Summary** step of the wizard, review configured settings and click **Save**.





# Removing Organizations

Veeam Backup for Salesforce allows you to permanently remove a Salesforce organization from the configuration database if you no longer need it.

## IMPORTANT

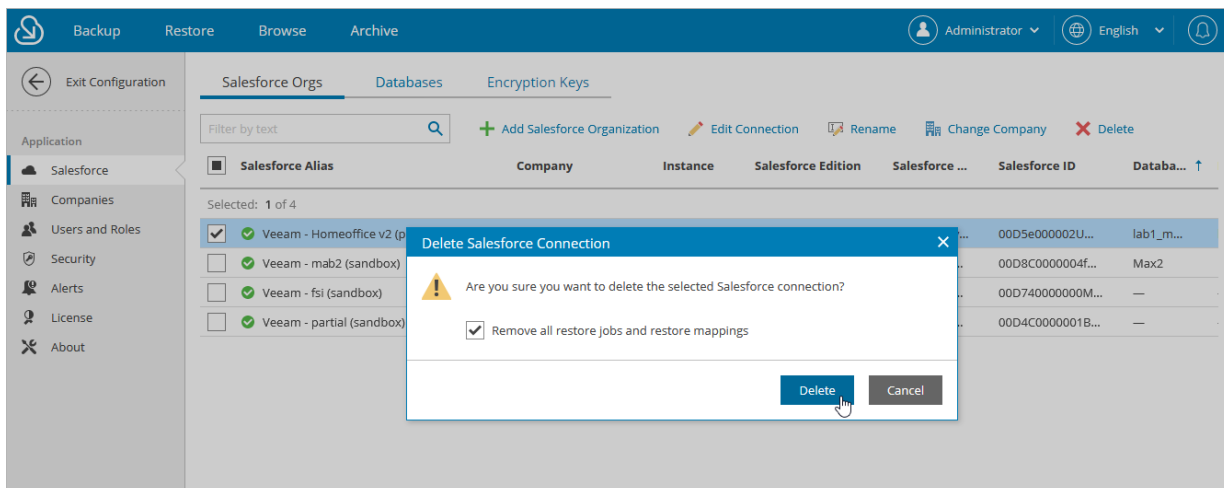
You cannot remove a Salesforce organization that is currently protected by a backup policy. To remove the organization, delete the backup policy first as described in section [Removing Backup Policies](#).

To remove an organization, do the following:

1. Switch to the **Configuration** page.
2. Navigate to **Salesforce > Salesforce Orgs**.
3. Select the necessary organization and click **Delete**.
4. In the **Delete Salesforce Connection** window, select the **Remove all restore jobs and restore mappings** check box and click **Delete**.

## NOTE

When you remove an organization, the backed-up data (data, metadata and files) is not deleted automatically. Veeam Backup for Salesforce continues storing the data for the security reasons. You can further use this data to restore objects and fields if you add the organization back to the management server. If you do not need the backed-up data, you can manually delete a database used to store the data of this organization from the server where the database is hosted and delete files and attachments from the location specified in the [backup policy](#) protecting the organization.



# Managing Companies

Companies are logical groups that provide an additional level of security by controlling the scope of data available to the user and the alerts shown. Using companies, you can group Salesforce organizations added to Veeam Backup for Salesforce and give users granular access only to organizations that belong to a specific company. For more information, see [Adding Users](#).

A company is created automatically when you [connect to a Salesforce organization](#) during the initial configuration of the management server. You can also [add companies manually](#), [edit created companies](#), [re-assign company organizations](#) and [remove companies](#).

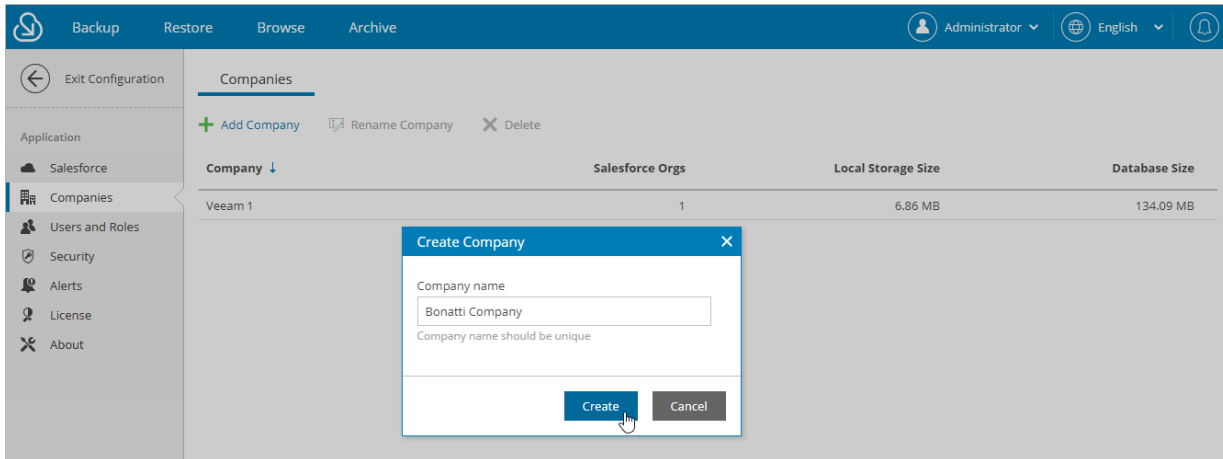
## TIP

To track the disk space used by backed-up files of a Salesforce organization, check the **Local Storage Size** column on the **Companies** tab. To track the disk space used by the backed-up database of the Salesforce organization, check the **Database Size** column on the **Companies** tab.

# Adding Companies

To add a new company, do the following:

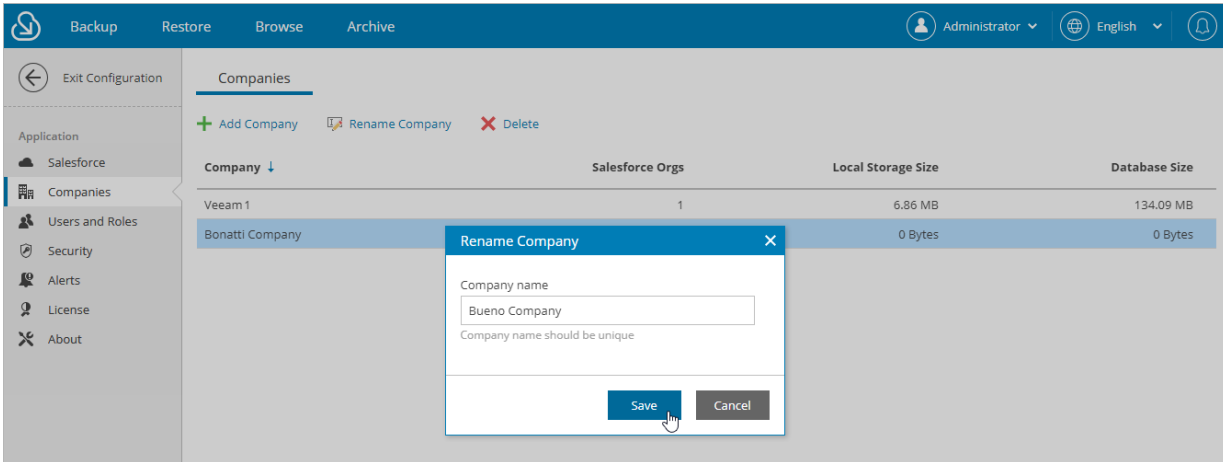
1. Switch to the **Configuration** page.
2. Navigate to **Companies**.
3. Click **Add Company**.
4. In the **Create Company** window, specify a name of a new company and click **Create**.



# Editing Companies

For each company, you can change the displayed name specified while adding the company to Veeam Backup for Salesforce:

1. Switch to the **Configuration** page.
2. Navigate to **Companies**.
3. Select the necessary company and click **Rename Company**.
4. In the **Rename Company** window, specify a new name for the company and click **Save**.



# Removing Companies

Veeam Backup for Salesforce allows you to permanently remove a company from the configuration database if you no longer need it. When you remove a company, Veeam Backup for Salesforce verifies whether you have assigned any Salesforce organizations to this company, and if yes, suggests you to re-assign the organizations to another company.

## IMPORTANT

When you remove a company and re-assign organizations to another company:

- Users that have company-wide permissions to the new company will automatically get permissions to access data of all re-assigned Salesforce organizations.
- Users that have permissions to access the removed company or any Salesforce organizations belonging to this company and do not have permissions to access the new company will not be assigned permissions to access new company automatically.
- Users that have the same roles in the removed and the new companies with permissions to access specific organizations within the company will retain the permissions to the same organizations.

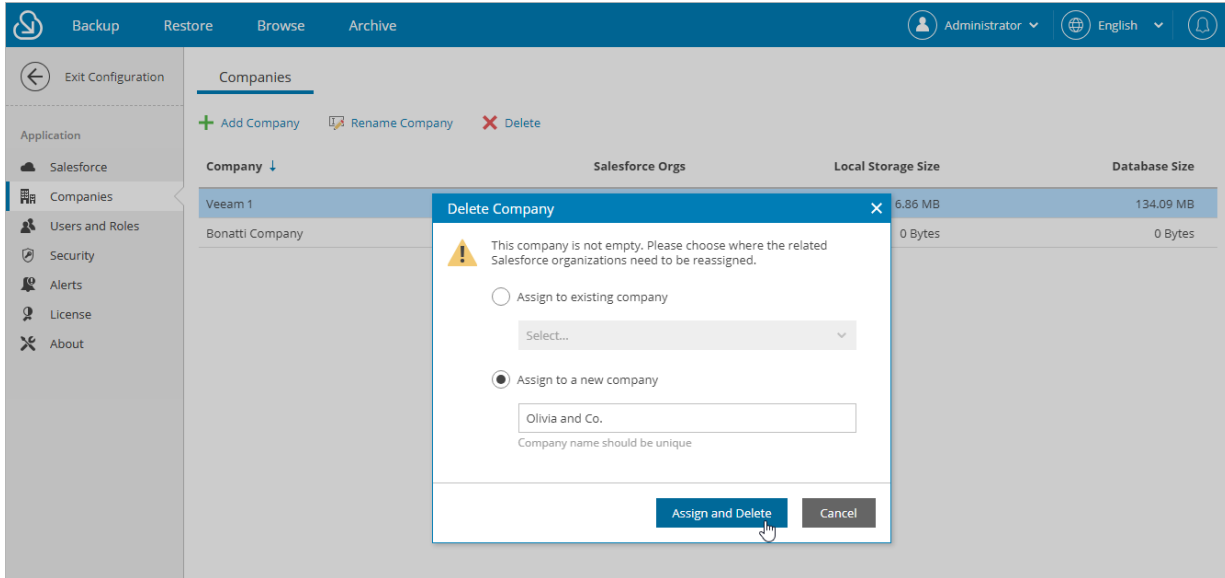
Consider the following example: *User\_1* has the *Restore operator* role for *organization\_1* that belongs to *company\_1* and the *Restore operator* role for *organization\_2* that belongs to *company\_2*. You remove *company\_1* and re-assign *organization\_1* to *company\_2*. In this case, *user\_1* will retain his permissions of the *Restore operator* role to *organization\_1* and *organization\_2* in *company\_2*.

To remove a company, do the following:

1. Switch to the **Configuration** page.
2. Navigate to **Companies**
3. Select the necessary company and click **Delete**.
4. [Applies if any Salesforce organizations are assigned to the selected company] In the **Delete Company** window:
  - a. Choose whether you want to assign the organizations to an existing or to a new company:
    - If you want to re-assign organizations belonging to the removed company to an existing company, select the **Assign to existing company** option, and choose the necessary company from the drop-down list.

For a company to be displayed in the list of available companies, it must be created as described in section [Adding Companies](#).
    - If you want to add a new company to Veeam Backup for Salesforce and to re-assign organizations to this company, select the **Assign to a new company** option, and specify a name for the new company.

b. Click Assign and Delete.



# Managing Databases

To store backed-up data and metadata of Salesforce organizations, Veeam Backup for Salesforce uses PostgreSQL databases. One database can be used to protect only one organization. You can add databases to Veeam Backup for Salesforce before or during the creation of [backup policies](#).

## In This Section

- [Adding Databases](#)
- [Editing Databases](#)
- [Removing Databases](#)

# Adding Database Connections

When you create a [backup policy](#), you can add a new database without closing the **Add Backup Policy** wizard or connect to a database that has been added to Veeam Backup for Salesforce beforehand as described in this section.

To add a PostgreSQL database to Veeam Backup for Salesforce, do the following:

1. Switch to the **Configuration** page.
2. Navigate to **Salesforce > Databases**.
3. Click **Add Database**.

The **Add Database Connection** window will open.

4. In the **PostgreSQL Server Connection** section of the window, choose whether the database will be hosted on one of the PostgreSQL servers to which Veeam Backup for Salesforce is already connected or establish connection to a new PostgreSQL server.

If you chose to connect to a new server, you must configure the new connection settings:

- a. In the **PostgreSQL address** field, specify the DNS name or IP address of a PostgreSQL server that will host the database.
- b. In the **Port** field, choose a network port that will be used by Veeam Backup for Salesforce to connect to the PostgreSQL server. The default port number is 5432.
- c. Use the **Username** and **Password** fields to provide credentials of the PostgreSQL user that will be used to access the databases. The user must be assigned permissions required to create database schemas.

Note that if you want Veeam Backup for Salesforce to be able to create the required databases automatically, the user must also be assigned permissions required to create databases. Otherwise, you have to create empty databases on the specified server manually beforehand. For more information, see [Permissions](#).

5. In the **Create or connect to a database** section of the window, use the **Database name** and **Connection label** fields to specify a name for the database and a connection label that further will be used as the database name displayed in the Veeam Backup for Salesforce Web UI.

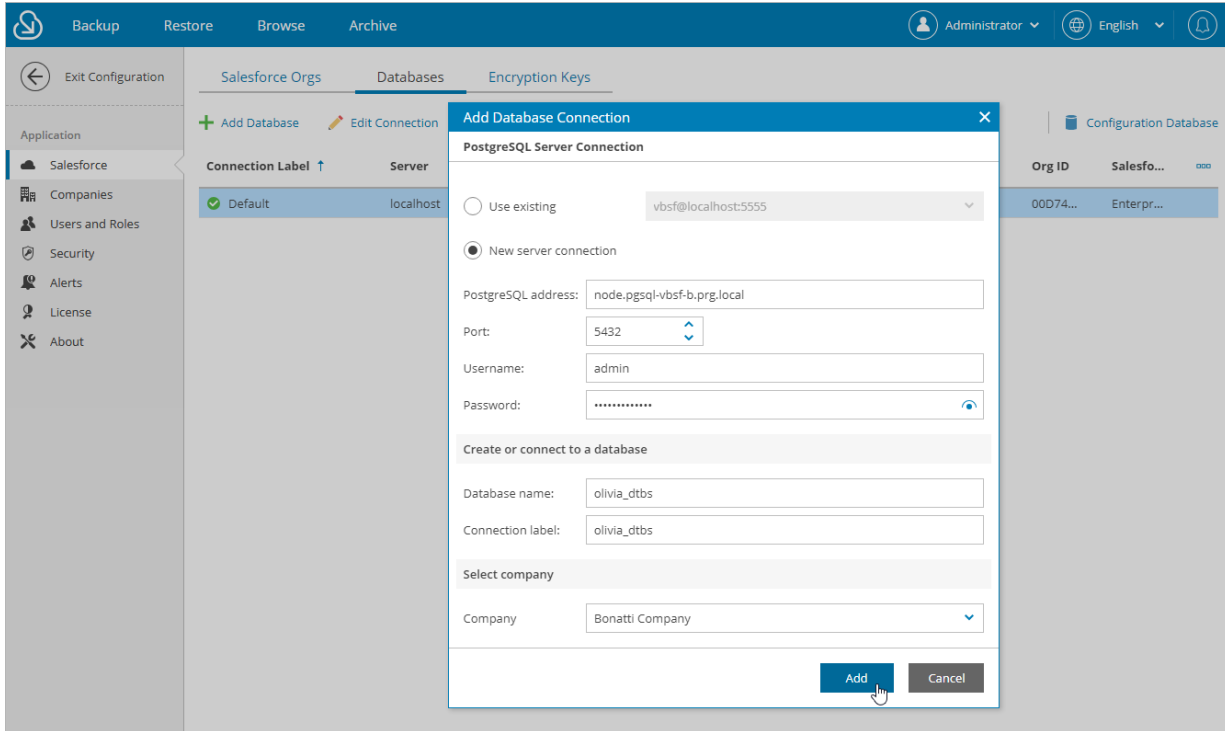
## IMPORTANT

Backed-up data of a Salesforce organization can be stored either in an empty database, or in any other database whose schema and organization ID match the schema and organization ID of the source database.

6. In the **Select company** section of the window, choose a company that manages a Salesforce organization whose backed-up data and metadata you want to store in this database. For more information on companies, see [Managing Companies](#).



## 7. Click Add.



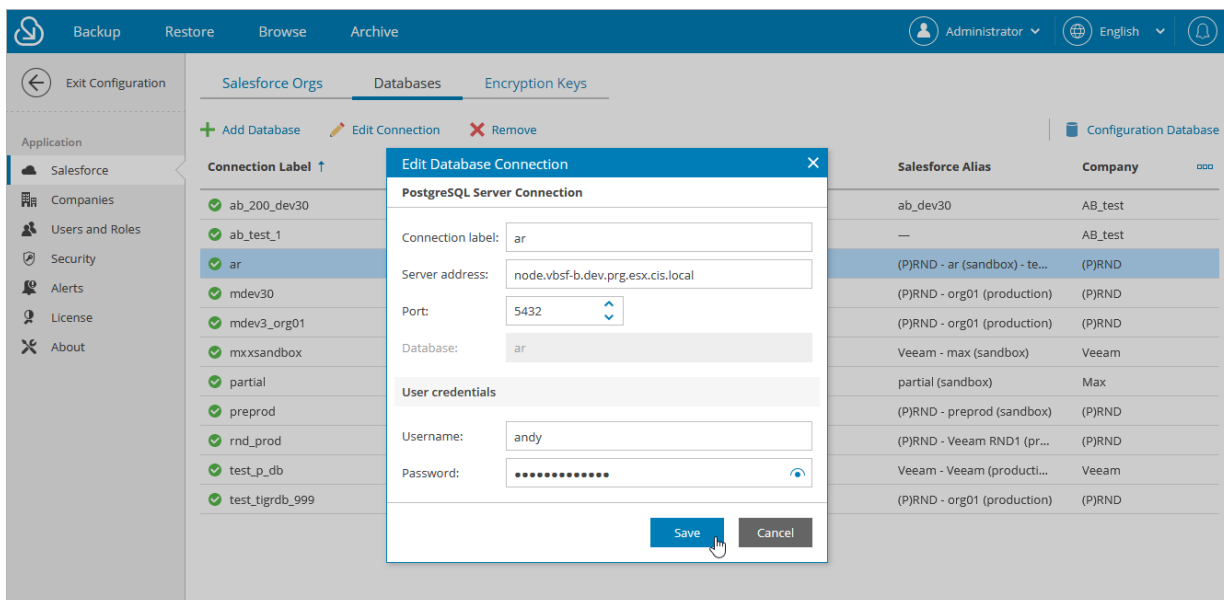
# Editing Database Connections

For each PostgreSQL database, you can modify the configuration settings specified while adding the database connection:

1. Switch to the **Configuration** page.
2. Navigate to **Salesforce > Databases**.
3. Select the necessary database from the list and click **Edit Connection**.
4. In the **Edit Database Connection** window, you can change the connection label used as the database name displayed in the Veeam Backup for Salesforce Web UI, the server address, the network port and the database user. If you change credentials of the user, keep in mind that the new user must be assigned permissions required to create database schemas.

## NOTE

You cannot edit connection settings for the Veeam Backup for Salesforce configuration database, but you can change user credentials used to connect to this database. To do that, click **Configuration Database** and provide new credentials in the **Edit Database Connection** window.



# Removing Database Connections

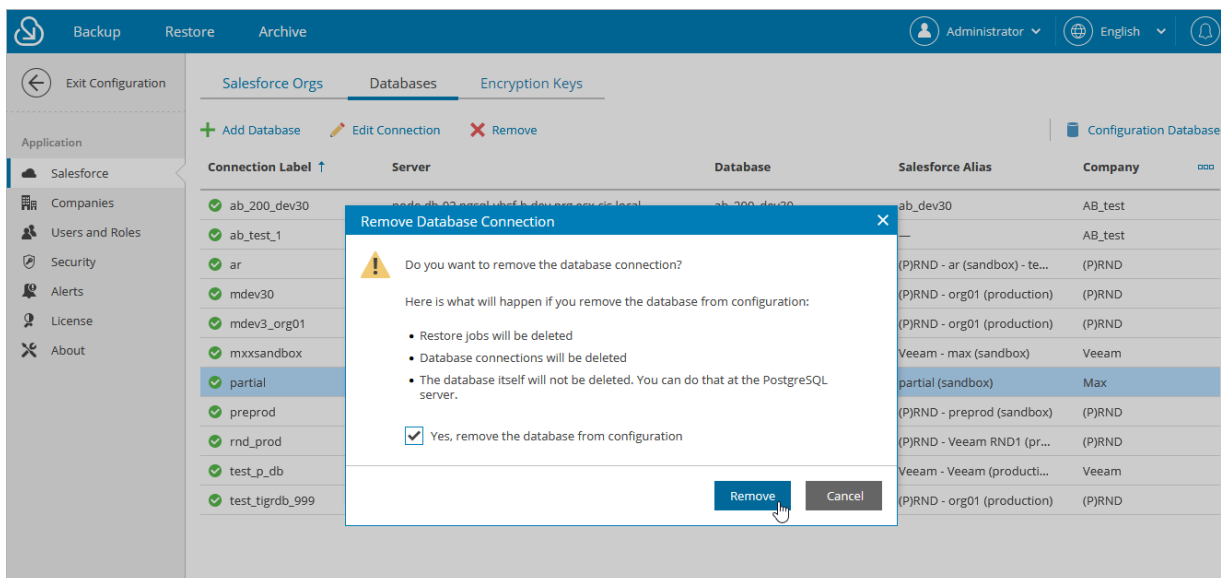
You can remove a database from Veeam Backup for Salesforce if you no longer need it. However, the database will not be deleted from the host server – it can be further reconnected to the same or to another Veeam Backup for Salesforce server and used to protect the same organization. If you do not need the data stored in the database anymore, you can delete it from the host server manually.

## NOTE

You cannot remove a database that is currently used by Veeam Backup for Salesforce to protect a Salesforce organization. If you want to remove the database, connect to another database in the [backup policy settings](#).

To remove a database from Veeam Backup for Salesforce, do the following:

1. Switch to the **Configuration** page.
2. Navigate to **Salesforce > Databases**.
3. Select the necessary database and click **Remove**.
4. In the **Remove Database Connection** window, acknowledge the operation and click **Remove**.



# Managing Users

Veeam Backup for Salesforce can be fully managed by a single built-in administrator account created during initial configuration. However, it is recommended that you configure an identity provider (IdP), create a user with the *Administrator* role and then use the configured IdP to access Veeam Backup for Salesforce.

## In This Section

- [User Roles and Permissions](#)
- [Adding Users](#)
- [Editing Users](#)
- [Removing Users](#)

# User Roles and Permissions

Veeam Backup for Salesforce controls access to its functionality with the help of user roles and scopes. A role defines what operations users can perform and a scope defines to which companies and Salesforce organizations the permissions apply.

There are 4 user roles that you can assign to user groups and users working with Veeam Backup for Salesforce:

- **Administrator** – can perform all configuration actions, backup and restore operations. This role gives a user access to the full product functionality (except for the IdP configuration).
- **Backup Operator** – can create and manage backup policies, manage protected data and perform all restore and archival operations. You can limit access to companies and Salesforce organizations for users when assigning this role. For more information, see [Adding Users](#).
- **Restore Operator** – can only perform restore operations. You can limit access to companies and Salesforce organizations for users when assigning this role. For more information, see [Adding Users](#).
- **Viewer** – can monitor backup and restore processes without performing any operations. You can limit access to companies and Salesforce organizations for users when assigning this role. For more information, see [Adding Users](#).

The following table describes the functionality available to users with different roles in the Veeam Backup for Salesforce UI. Note that users with *Backup Operator*, *Restore Operator* and *Viewer* roles assigned will have the described permissions only within the scope specified when adding these users.

Tab	Functionality	Administrator	Backup Operator	Restore Operator	Viewer
Backup	Managing backup policies, performing backup	Full	Full	Viewing backup policies and sessions	Viewing backup policies and sessions
	Downloading backup session logs	Full	Full	-	-
Restore	Managing restore jobs, performing restore	Full	Full	Full	Viewing restore jobs and sessions
	Downloading restore session logs	Full	Full	Full	-
Browse	Viewing backed-up data, performing restore	Full	Full	Full	-
Archive	Managing archival policies, performing archiving	Full	Full	Viewing archival policies and sessions	Viewing archival policies and sessions

Tab	Functionality	Administrator	Backup Operator	Restore Operator	Viewer
	Downloading archival session logs	Full	Full	Full	-
<b>Configuration</b>					
<b>Salesforce</b>	Managing companies	Full	-	-	-
	Managing Salesforce organizations	Full	Adding and viewing Salesforce organizations	-	-
	Managing databases	Full	Full	-	-
	Managing encryption keys	Full	Full	-	-
<b>Users and Roles</b>	Managing users	Full	-	-	-
<b>Security</b>	Managing Connected App	Full	-	-	-
	Managing identity provider	Local administrator only	-	-	-
	Managing key management service	Full	Full	-	-
	Managing audit trail	Full	-	-	-
<b>Alerts</b>	Managing notifications	Full	Full*	-	-
	Managing connection settings	Full	-	-	-

Tab	Functionality	Administrator	Backup Operator	Restore Operator	Viewer
<b>License</b>	Managing license	Full	Viewing license information	-	-
<b>About</b>	Downloading product logs	Full	-	-	-
	Configuring advanced settings	Full	-	-	-

\*Does not apply to alerts created for the *License* and *File storage size* types of events. For more information on event types, see [Managing Alerts](#).

# Adding Users

To add a user or group of users, do the following:

1. Configure IdP settings as described in section [Configuring IdP and SSO Settings](#).
2. Switch to the **Configuration** page.
3. Navigate to **Users and Roles > Users**.
4. Click **Add User**.

You will be redirected to the authorization page of the configured identity provider. If you have not logged in yet, log in to the identity provider portal. After that, you will be redirected to the Veeam Backup for Salesforce page as an authorized user.

## NOTE

If you [connected a Microsoft Entra ID as an identity provider](#) in Veeam Backup for Salesforce and want to add a group of users, make sure that all users in the group have an email in the connected Microsoft Entra ID. Otherwise, they will not be able to log in to the product.

5. In the **Assign Roles** window:
  - a. Click **Select user or group** to choose the necessary IdP user or group of users.
  - b. Use the **Role** drop-down list to select a user role that will be assigned to the selected user or group of users. For more information on user roles, see [User Roles and Permissions](#).

If a user belongs to multiple groups, the user will inherit the most privileged role from all the roles assigned to these groups.
  - c. Use the **Company** and **Organization** drop-down lists to specify the scope of resources to which the selected user or group of users will have access in Veeam Backup for Salesforce.

## NOTE

You cannot limit the scope of resources for the *Administrator* role. By default, this role provides access to all companies and Salesforce organizations added to Veeam Backup for Salesforce.

- d. Click **Assign Role**.
- e. Perform steps b-d for each role that you want to assign to the selected user or group of users.

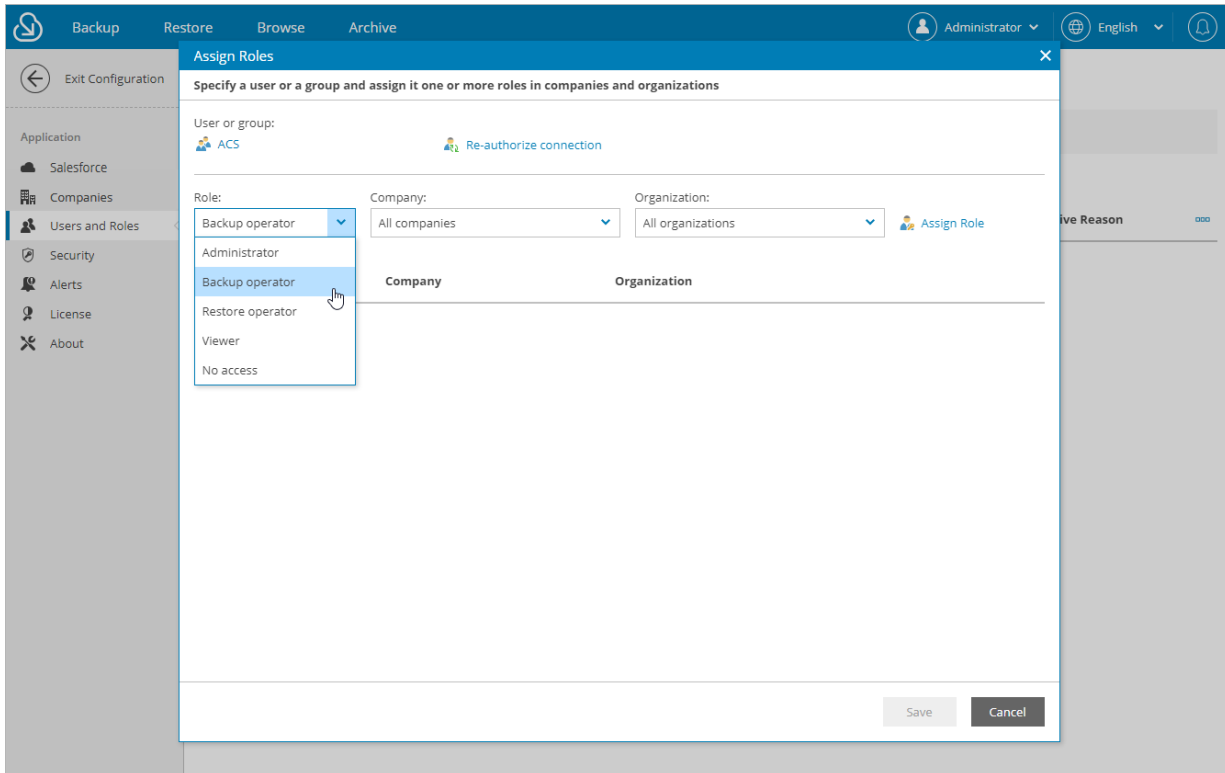
Make sure that the permissions of the assigned roles do not overlap each other. Otherwise, one role may override another, and Veeam Backup for Salesforce will display a warning.

## TIP

You can unassign roles from the selected user or group of users. To do that, click the cross button in the necessary row of the user roles table.



f. Click **Save**.



# Editing Users

Veeam Backup for Salesforce allows you to edit settings of users added to the configuration database, activate and deactivate users.

## IMPORTANT

If you change IdP settings, all users added to Veeam Backup for Salesforce using these settings will become inactive. If you want to enable access for these users, choose the previously configured identity provider and save the settings. For more information on configuring an identity provider, see [Configuring IdP and SSO Settings](#).

## Editing Local Administrator

You cannot modify settings of the local administrator created during the [initial configuration](#) from the Web UI. You can only reset the password of the administrator using the terminal. To do that, connect to the machine running Veeam Backup for Salesforce using SSH, run the `/opt/vbsf/reset_password.sh` script, provide and confirm the new password. The password must contain uppercase and lowercase Latin letters and special characters (!@#\$%^&`~\*()\_-+=[]{};\:'"|,./<>?). The minimum length of the password is 8 characters.

## Editing IdP Users

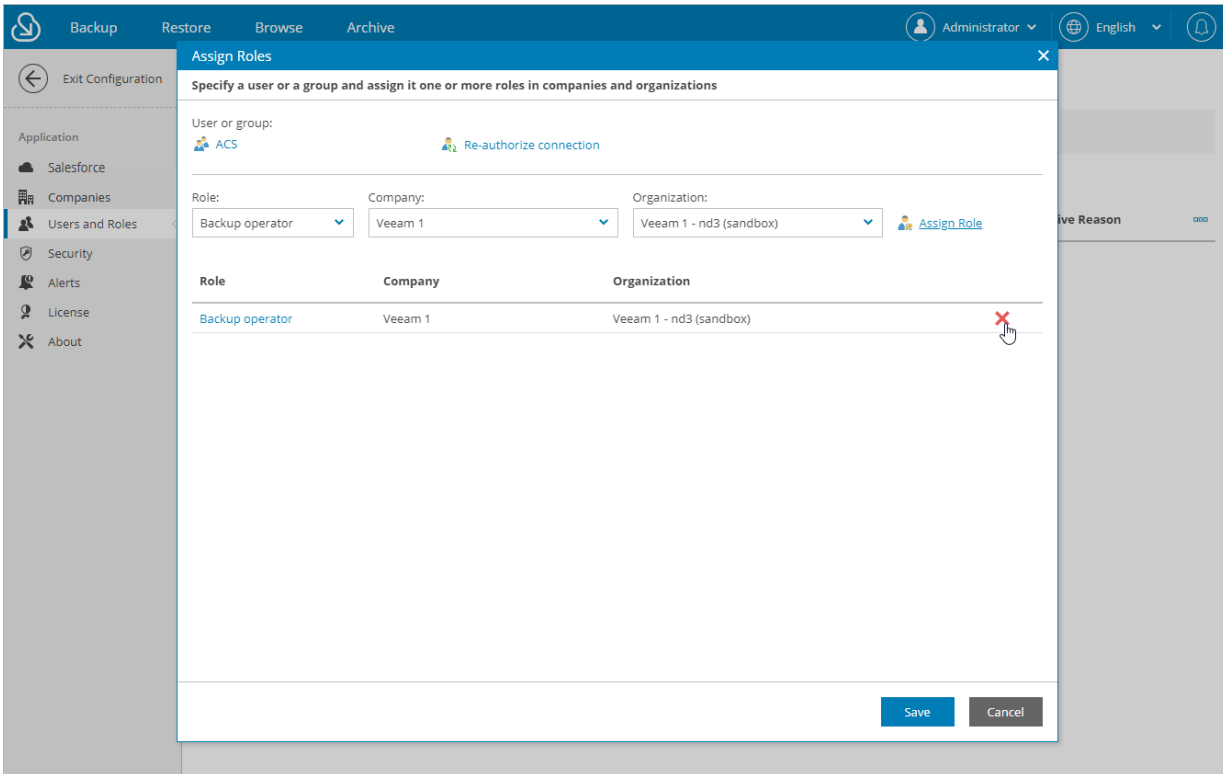
You can edit permissions assigned to users and user groups in Veeam Backup for Salesforce. To do that:

1. Switch to the **Configuration** page.
2. Navigate to **Users and Roles > Users**.
3. Select the necessary user or group of users, and click **Edit**.
4. In the **Edit User Settings** window, do one of the following:
  - To unassign a role from the user or group of users, click the cross button in the necessary row of the user roles table.
  - To assign a new role to the user or group of users, follow the instructions provided in [Adding Users](#).

The changes will immediately apply after you finish working with the wizard. This will result on user access to the Veeam Backup for Salesforce functionality. However, all backup policies, archival policies and restore jobs started and scheduled by this user will not be affected.

## NOTE

If you rename a group of users in Microsoft Azure Entra ID, Veeam Backup for Salesforce does not automatically update the record in the configuration database. To update the group name in the product Web UI, select the group, click **Edit** and re-save the record.

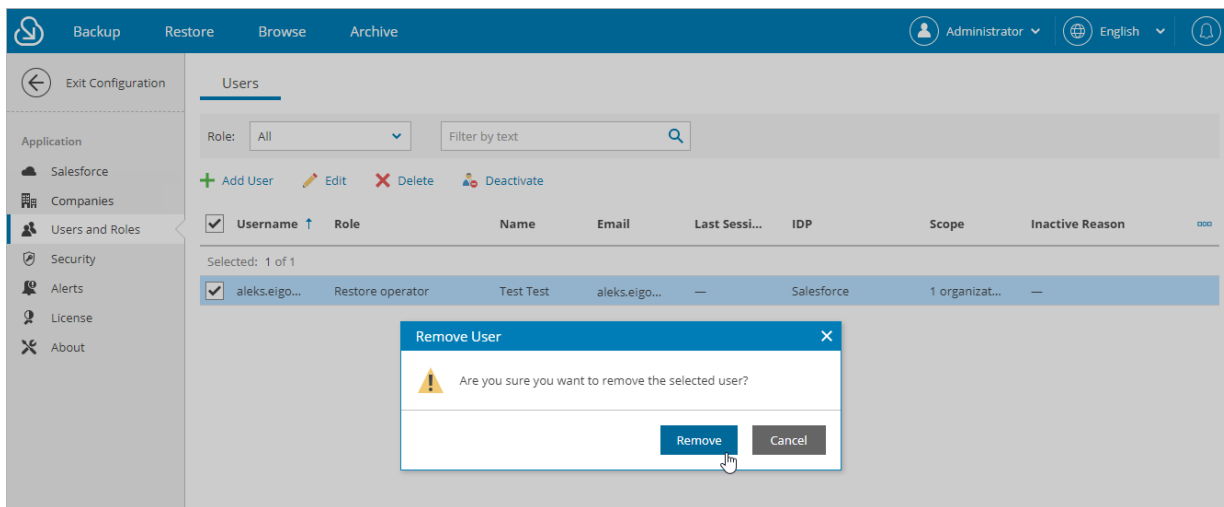


# Removing Users

Veeam Backup for Salesforce allows you to permanently remove users and user groups from the configuration database:

1. Switch to the **Configuration** page.
2. Navigate to **Users and Roles > Users**.
3. Select the necessary user or group and click **Delete**.
4. In the **Remove User** window, click **Remove** to acknowledge the operation.

The changes will immediately apply after you click **Remove**. However, all backup policies, archival policies and restore jobs started and scheduled by this user will not be affected.



# Configuring Security Settings

Veeam Backup for Salesforce allows you to change Salesforce Connected App used to authenticate with Salesforce and get access to resources that will be protected, configure single sign-on (SSO) authentication, and view information on various product events.

## In This Section

- [Changing Connected App Tokens](#)
- [Configuring IdP and SSO Settings](#)

# Changing Connected App Tokens

Salesforce Connected App allows Veeam Backup for Salesforce to authenticate with Salesforce and get access to resources that will be protected. You can create the Connected App in any Salesforce organization. To learn how to create the Connected App, see [this Veeam KB article](#).

## IMPORTANT

You can protect multiple Salesforce organizations using a single Veeam Backup for Salesforce installation. However, due to the Salesforce Connected App limit of 5 authorizations per client, authorization issues may occur when you have several product installations leveraging the same Connected App. That is why it is recommended that you create a dedicated Connected App for each product deployment.

For more information on Salesforce OAuth Authorization Flows and Connected Apps, see [Salesforce Documentation](#).

During the [initial configuration](#), you are prompted to provide the Connected App OAuth tokens that are further used by Veeam Backup for Salesforce for the authentication process. However, you can change these tokens later in the Veeam Backup for Salesforce Web UI.

## IMPORTANT

If you change the Connected App tokens, you must re-authorize all connections to Salesforce organizations added to Veeam Backup for Salesforce. Otherwise, all backup and restore operations will fail.

To re-authorize connections to Salesforce organizations, either navigate to **Configuration > Salesforce > Salesforce Orgs** and edit connections as described in section [Editing Organizations](#), or navigate to **Backup**, launch the **Edit Backup Policy** wizard for each created backup policy, and follow instructions provided in [Step 2. Configure Connection to Salesforce Organization](#).

## Changing Tokens

To change the OAuth tokens, do the following:

1. Switch to the **Configuration** page.
2. Navigate to **Security > Connected App**.
3. Click **Change Connected App Tokens**, and then click **Proceed** in the **Confirm Operation** window to acknowledge the operation.
4. Specify the type of the Salesforce organization where your Connected App is created.
5. Use the **Consumer key** and **Consumer secret** fields to provide the tokens obtained when creating the app.
6. Click **Connect**.

## NOTES

If you have created a new Connected App, consider the following:

- The Connected App must be assigned the *Full access (full)* and *Perform requests at any time (refresh\_token, offline\_access)* OAuth scopes. For more information on OAuth scopes in Salesforce, see [Salesforce Documentation](#).
- If you have configured Salesforce as an identity provider in Veeam Backup for Salesforce, the *access unique user identifiers (openid)* OAuth scope must be granted to the new Connected App. Otherwise, you will not be able to change the Connected App tokens.
- The callback URL specified in the Connected App settings must match the Veeam Backup for Salesforce server address. You can copy the address in the **Setting up Salesforce Connected App** section.
- It takes up to 10 minutes for newly created OAuth tokens to become active.

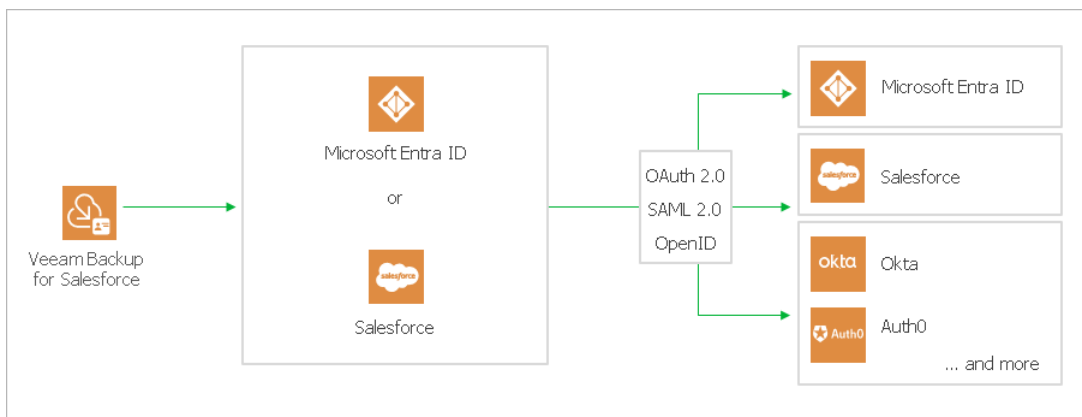
The screenshot shows the Veeam Backup for Salesforce configuration interface. The top navigation bar includes 'Backup', 'Restore', 'Browse', and 'Archive'. The user is logged in as 'Administrator' and the language is set to 'English'. The left sidebar shows the navigation menu with 'Security' selected. The main content area is titled 'Connected App' and includes tabs for 'Single Sign-On', 'Key Management Service', and 'Audit'. The 'Salesforce Connected App' section contains a warning message: 'Your Connected App is now configured, but connections to some Salesforce organizations need attention. Please go to the Salesforce tab and re-authorize the connected organizations with the backup users credentials.' Below this, there are fields for 'Verify with Salesforce domain' (set to 'Production'), 'Salesforce login domain' (https://login.salesforce.com/), 'Consumer key' (5MVG9DREgfgBqN9WksZK\_VJz5B1\_hLB2QP78nFvjphJLujxmVAFaE0hTehzI), and 'Consumer secret' (masked). A 'Connect' button is visible. The 'Setting up Salesforce Connected App' section provides instructions on the Callback URL and includes a field with the URL 'https://171.55.52.175' and a 'Copy to Clipboard' button. A link to 'Read KB on Salesforce Connected App' is also present.

# Configuring IdP and SSO Settings

Veeam Backup for Salesforce supports single sign-on (SSO) authentication using Microsoft Entra ID and Salesforce based on the OAuth 2.0 protocol. SSO authentication allows users to follow the corporate security policy and log in to Veeam Backup for Salesforce using the corporate identity provider (IdP).

## IMPORTANT

If you change IdP settings, all users added to Veeam Backup for Salesforce using these settings will become inactive. If you want to enable access for these users, choose the previously configured identity provider and save the settings.



## Configuring IdP Settings Using Microsoft Entra ID

To configure IdP settings using Microsoft Entra ID, you must first create an application for Veeam Backup for Salesforce on the Microsoft Identity Platform. To learn how to register an application with the Microsoft Identity Platform, see [Microsoft Docs](#).

When creating the application, consider the following:

- The following API permissions must be granted to the application:
  - *GroupMember.Read.All*
  - *User.Read*
  - *User.Read.All*
- The redirect URI added to the application must match the management server FQDN that you use to access the Veeam Backup for Salesforce Web UI. To make sure that you are adding the correct URI, switch to the **Configuration** page and navigate to **Security > Single Sign-On**. The address will be displayed in the **Callback URL** field.

## Configuring IdP Settings on Veeam Backup for Salesforce Side

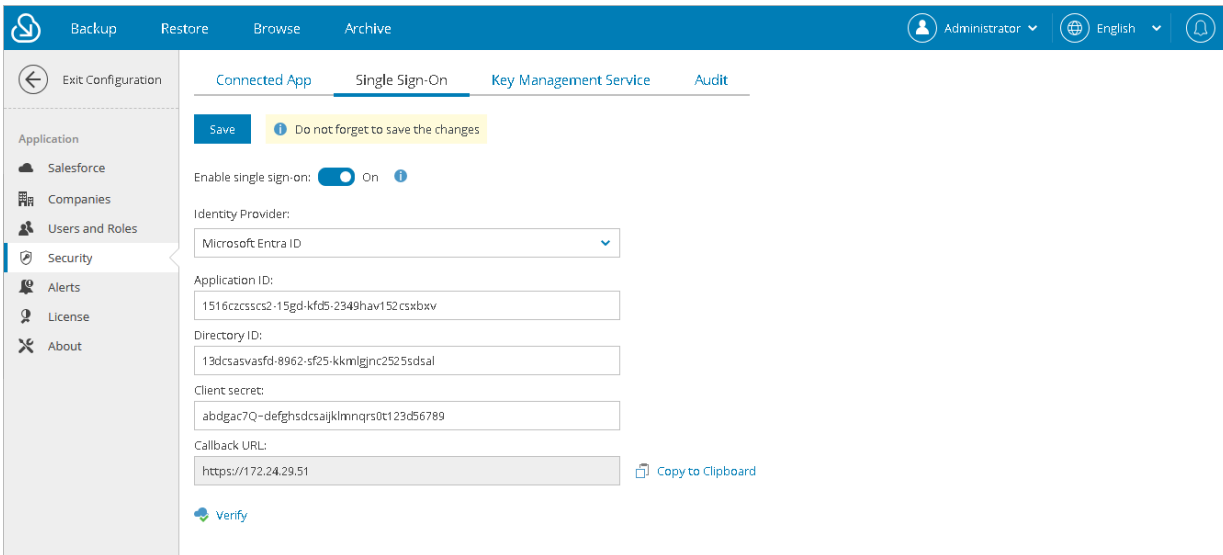
To configure the IdP settings on the Veeam Backup for Salesforce side, do the following:

1. Switch to the **Configuration** page.
2. Navigate to **Security > Single Sign-On**.
3. Set the **Enable single sign-on** toggle to *On*.
4. From the **Identity Provider** drop-down list, select *Microsoft Entra ID*.



5. In the **Application ID** field, provide the *Application ID* of the registered application. You can find the ID on the app registration **Overview** pane on the Microsoft Identify Platform.
6. In the **Directory ID** field, specify the *Directory ID* of the registered application. You can find the ID on the app registration **Overview** pane on the Microsoft Identify Platform.
7. In the **Client secret** field, enter the value of a client secret created in the specified application.  
Keep in mind that you can see and copy a client secret value only when creating it. Otherwise, you will not be able to retrieve the value. To learn how to create client secrets, see [Microsoft Docs](#).
8. Click **Save**. You will be redirected to the Microsoft authentication page. Enter the credentials of the Microsoft user and log in to the application. Grant admin consent to the application if required. To learn how to do that, see [Microsoft Docs](#).

As soon as the IdP settings are successfully configured, you can start [adding users](#) to Veeam Backup for Salesforce. Consider that the Veeam Backup for Salesforce session timeout is 60 minutes. If the session is expired, you must log in to Veeam Backup for Salesforce using the local administrator credentials once again, and continue adding users for the next 60 minutes.



# Configuring IdP Settings Using Salesforce

You can configure Salesforce as an OpenID Connect identity provider that will allow users of your Salesforce organizations to log in to Veeam Backup for Salesforce. For more information, see [Salesforce Documentation](#).

To be able to use Salesforce as an identity provider, you must grant the [access unique user identifiers \(openid\)](#) OAuth scope to the Connected App used to authorize access to all Salesforce organizations protected by this Veeam Backup for Salesforce installation. For more information on the Connected App, see [Changing Connected App Tokens](#).

## NOTE

If you have an allowlist for Connected Apps configured in Salesforce, make sure that the product is included in that list and users are granted access to the Veeam Backup for Salesforce Connected App. For more information, see [Salesforce Documentation](#).

## Configuring IdP Settings on Veeam Backup for Salesforce Side

To configure the IdP settings on the Veeam Backup for Salesforce side, do the following:

1. Switch to the **Configuration** page.
2. Navigate to **Security > Single Sign-On**.
3. Set the **Enable single sign-on** toggle to *On*.
4. From the **Identity Provider** drop-down list, select *Salesforce*.
5. From the **Login domain** field, choose one of the following:
  - If you want to authorize users of Salesforce production organizations only, select *Production*.
  - If you want to authorize users of Salesforce sandbox organizations only, select *Sandbox*.
  - If you want to authorize users of a specific Salesforce organization hosted on a custom domain, select *Custom*.

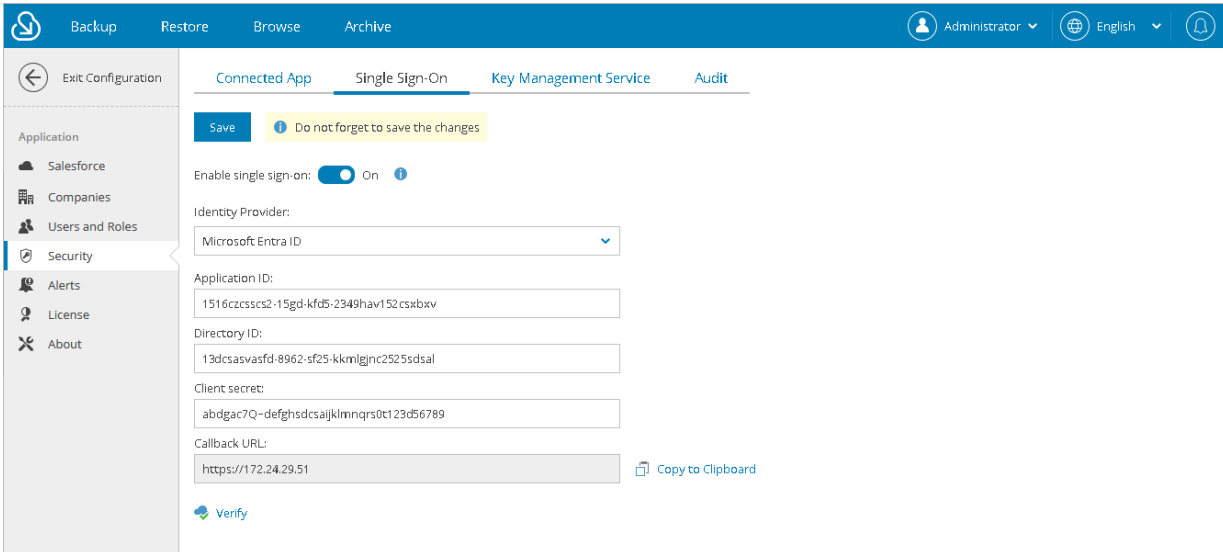
If you select the **Custom** option, you must also specify the organization domain name.
6. Click **Save**. You will be redirected to the Salesforce authentication webpage.

On the Salesforce authentication webpage, enter credentials of the Salesforce user and click **Log in**. The specified user must be granted permissions to read user data.

As soon as the IdP settings are successfully configured, you can start [adding users](#) to Veeam Backup for Salesforce. Consider that the Veeam Backup for Salesforce session time out is 60 minutes. If the session is expired, you must log in to Veeam Backup for Salesforce using the local administrator credentials once again, and continue adding users for the next 60 minutes.

## IMPORTANT

If you enabled a Salesforce organization as an identity provider, do not use the integration user account to sign in to Veeam Backup for Salesforce as it will cause the backup session token to expire after 5 login attempts. Backup jobs will fail with the expired Salesforce token message because the authorization token is revoked by Salesforce. You will have to reauthorize the connection to the Salesforce organization.



# Configuring Encryption Settings

Veeam Backup for Salesforce allows you to encrypt backed-up data stored in PostgreSQL databases and file repositories to protect your information from unauthorized access. To do that, the product leverages a cryptographic algorithm to transform data to an unreadable format using an organization-specific data key that is enciphered with one of the following master keys:

- An original (built-in) Veeam Backup for Salesforce master encryption key that is automatically generated by Veeam Backup for Salesforce upon installation.
- A native Amazon Web Services Key Management Service (AWS KMS) customer-managed master encryption key. Note that only symmetric keys are supported in Veeam Backup for Salesforce 3.0.

## NOTE

One master key can be used to encrypt data of multiple Salesforce organizations.

## In This Section

- [Managing AWS KMS Connections](#)
- [Managing Encryption Keys](#)

# Managing AWS KMS Connections

To encrypt data using an AWS KMS master key, you must first connect to an AWS account that manages this key. To learn how to do that, follow the instructions provided in section [Adding Connections](#).

Before you connect to an AWS account, check the following prerequisites:

- Make sure that the IAM user that will be used to perform data encryption have all the [required permissions](#).
- Make sure that you have created the AWS KMS master key in the AWS account. For more information, see [AWS Documentation](#).
- Make sure that you have created an access key ID and a secret access key that will be used to authenticate requests to the AWS account. Keep in mind that you can see and copy this ID and key only when creating an access key pair. For more information, see [AWS Documentation](#).

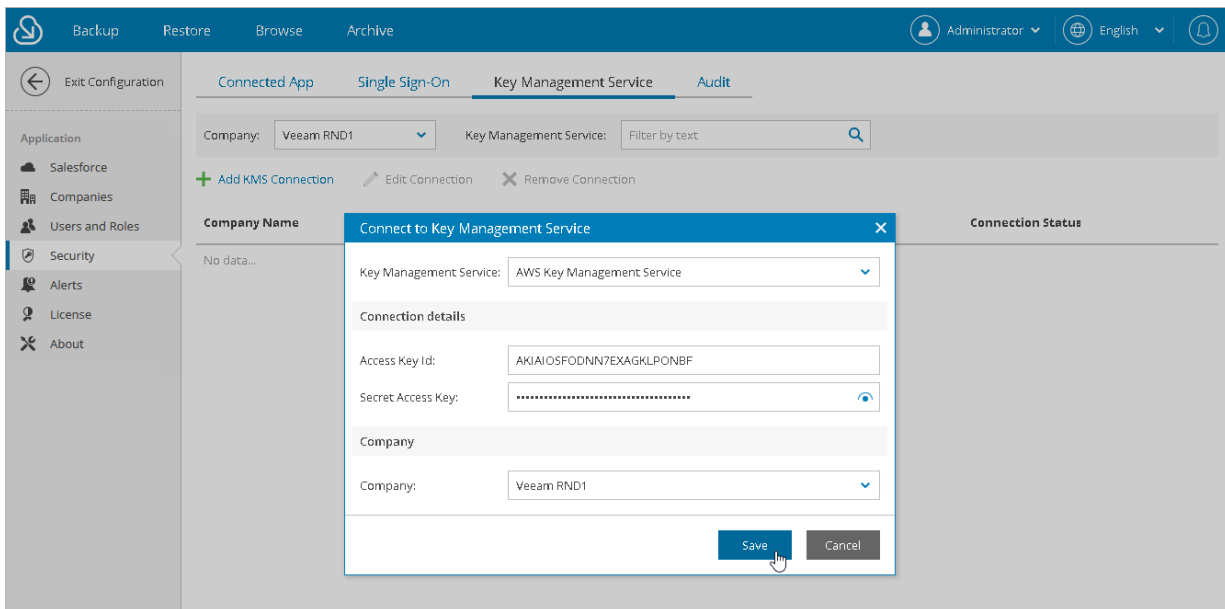
## Related Topics

[Removing Connections](#)

# Adding Connections

To connect to an AWS account, do the following:

1. Switch to the **Configuration** page.
2. Navigate to **Security > Key Management Service**.
3. Click **Add KMS Connection**.
4. In the **Connect to Key Management Service** window:
  - a. In the **Access Key Id** and **Secret Access Key** fields, specify an access key pair that will be used to authenticate requests to the AWS account managing this master key.
  - b. From the **Company** drop-down list, select a company to which you want to connect the AWS account.  
For a company to be displayed in the list of available companies, it must be created as described in section [Adding Companies](#).
  - c. Click **Save**.



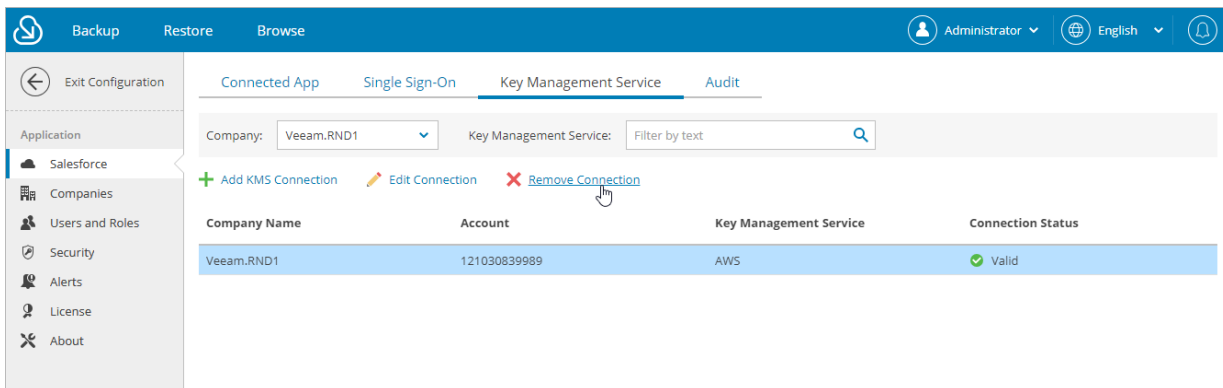
# Removing Connections

Veeam Backup for Salesforce allows you to remove a connection to an AWS account from Veeam Backup for Salesforce if you no longer need it. To do that:

1. Switch to the **Configuration** page.
2. Navigate to **Security > Encryption**.
3. Select the necessary connection in the **Key Management Service** section and click **Remove Connection**.
4. In the **Remove** window, acknowledge the operation and click **Remove**.

## NOTE

You cannot remove a connection to an AWS account whose key is currently used by any backup policy to encrypt data. [Edit the policy encryption settings](#) to choose another key – and then try removing the connection again.



# Managing Encryption Keys

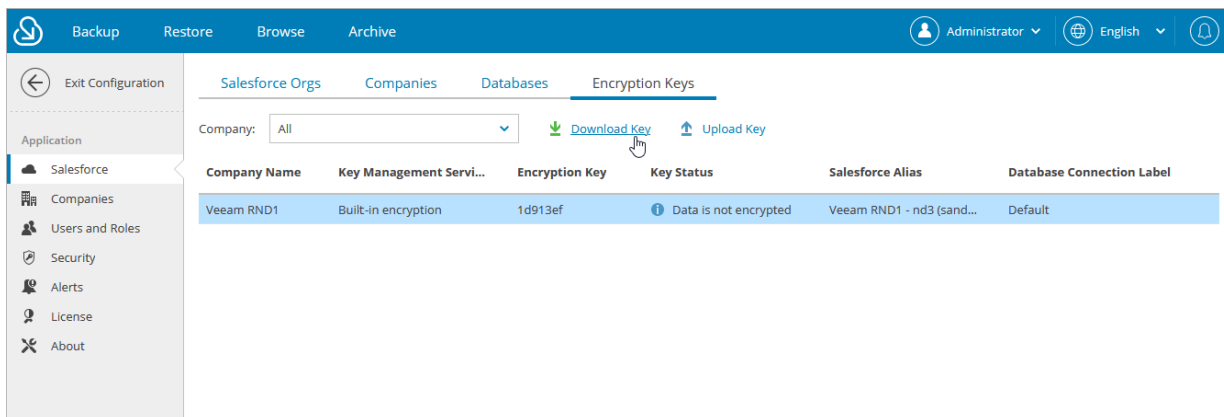
If your backed-up data is encrypted with a built-in encryption key, it is recommended that you download the key to your workstation. Otherwise, Veeam Backup for Salesforce will be not able to decrypt the data in case you migrate the product to another workstation.

To download the built-in encryption key, do the following:

1. Switch to the **Configuration** page
2. Navigate to **Salesforce > Encryption Keys**.
3. Choose the necessary key and click **Download Key**.

## TIP

After you download the built-in encryption key to your workstation, you will become able to decrypt data using this key in case of migration. To do that, click **Upload Key**. Keep in mind that you can decrypt only those records and files that were encrypted using the downloaded key.



The screenshot shows the Veeam Backup for Salesforce interface. The top navigation bar includes 'Backup', 'Restore', 'Browse', and 'Archive'. The user is logged in as 'Administrator' and the language is set to 'English'. The left sidebar shows the navigation menu with 'Salesforce' selected. The main content area is titled 'Encryption Keys' and includes a 'Company' dropdown menu set to 'All'. There are 'Download Key' and 'Upload Key' buttons. Below this is a table with the following data:

Company Name	Key Management Servi...	Encryption Key	Key Status	Salesforce Alias	Database Connection Label
Veeam RND1	Built-in encryption	1d913ef	Data is not encrypted	Veeam RND1 - nd3 (sand...	Default



# Viewing Audit Trail

The **Audit** tab displays a trail of all security-sensitive events such as logging in, database creation, connecting to Salesforce organizations, backup and restore operations, and so on. You can use this information for management and monitoring purposes.

To track Veeam Backup for Salesforce events, do the following:

1. Switch to the **Configuration** page.
2. Navigate to **Security > Audit**.

## NOTE

Dates in the **Event** column are always displayed in the following format: [yyyy-mm-dd].

Date ↓	Type	Event	User IP	User
6/19/24, 11:45:53 AM	User	User logout	172.25.164.23	admin
6/18/24, 4:11:20 PM	User	User logout	172.25.164.23	admin
6/18/24, 2:26:53 PM	User	User logout	172.25.164.23	admin
6/18/24, 1:11:34 PM	User	User logout	172.25.164.23	admin
6/17/24, 11:49:36 AM	User	User logout	172.25.164.23	admin
6/17/24, 10:49:30 AM	User	Query data. Organization: 1. Object: Account. Fields: Id,SystemModstamp,Nam...	172.25.164.23	admin
6/14/24, 1:01:11 PM	User	User logout	172.25.164.23	admin
6/14/24, 12:00:49 PM	User	Query data. Organization: 1. Object: Account. Fields: Id,SystemModstamp,Nam...	172.25.164.23	admin
6/14/24, 12:00:47 PM	User	Query data. Organization: 1. Object: Account. Fields: Id,SystemModstamp,Nam...	172.25.164.23	admin
6/12/24, 6:23:38 PM	User	User logout	172.25.164.23	admin
6/12/24, 4:08:56 PM	User	User logout	172.25.164.23	admin
6/12/24, 2:51:56 PM	User	Restore job created: #1 - Restore records [ID: 8]	172.25.164.23	admin
6/12/24, 2:41:00 PM	User	Restore job change: Options. Restore records [ID: 7]	172.25.164.23	admin
6/12/24, 2:40:58 PM	User	Restore job change: Files. Restore records [ID: 7]	172.25.164.23	admin
6/12/24, 2:40:57 PM	User	Restore job change: Hierarchy. Restore records [ID: 7]	172.25.164.23	admin
6/12/24, 2:40:57 PM	User	Restore job change: Data. Restore records [ID: 7]	172.25.164.23	admin
6/12/24, 2:40:54 PM	User	Query data. Organization: 1. Object: Account. Fields: Id,SystemModstamp,Nam...	172.25.164.23	admin

# Managing Alerts

Veeam Backup for Salesforce allows you to create alerts to notify you about important events, state changes and issues. Users assigned the *Administrator* role can manage alerts for all companies and Salesforce organizations in Veeam Backup for Salesforce, while users assigned the *Backup Operator* role can manage alerts only for companies and Salesforce organizations within their specified scope of permissions.

You can create alerts for the following types of events:

- **Backup policy** – an alert created for this type of events is triggered by a specific backup session status. You can choose whether you want to receive notifications in case any of the backup policies configured for your Salesforce organizations complete successfully, complete with warnings or complete with errors.
- **Restore job** – an alert created for this type of events is triggered by a specific restore session status. You can choose whether you want to receive notifications in case any of the restore jobs configured for your Salesforce organizations complete successfully, complete with warnings or complete with errors.
- **Database connection** – an alert created for this type of events is triggered when the connection to a PostgreSQL database is lost.
- **Salesforce connection** – an alert created for this type of events is triggered when the connection to Salesforce is lost.
- **License** – an alert created for this type of events is triggered when the license installed on the management server acquires a specific status. You can choose whether you want to receive notifications in case the license check completes successfully, completes with warnings or completes with errors.

By default, Veeam Backup for Salesforce automatically checks the license on a weekly basis. You can also do it manually as described in section [Viewing License Information](#).

- **File storage size** – an alert created for this type of events is triggered when the specified space usage threshold is breached. By default, Veeam Backup for Salesforce automatically checks the storage space usage on a daily basis at 9:00 UTC.
- **Archival policy** – an alert created for this type of events is triggered by a specific archival session status. You can choose whether you want to receive notifications in case any of the archival policies configured for your Salesforce organizations complete successfully, complete with warnings or complete with errors.
- **Encryption job** – an alert created for this type of events is triggered by a specific encryption session status. You can choose whether you want to receive notifications in case any of the encryption jobs configured for your Salesforce organizations complete successfully, complete with warnings or complete with errors.
- **Data change** – an alert created for this type of events is triggered when Veeam Backup for Salesforce detects any changes in protected data. You can choose whether you want to receive notifications in case new records are added to any of the backup policies configured for your Salesforce organizations, or any of the existing records are updated or deleted from Salesforce.

## NOTE

Administrators and Backup Operators can both create and view alerts for all types of events, while Restore Operators and Viewers can only view the created alerts. However, Administrators and Backup Operators can also limit this functionality by assigning specific user roles.

## In This Section

- [Configuring Notification Settings](#)
- [Creating Alerts](#)
- [Editing Alerts](#)

# Configuring Notification Settings

To receive notifications on created alerts, you must configure notification settings. You can instruct Veeam Backup for Salesforce to send notifications by email and to specific Slack channels and chats.

## Configuring Email Settings

To configure mail server settings, choose whether you want to employ basic or modern authentication for your mail server.

### Using Basic Authentication

To employ the basic authentication to connect to your mail server:

1. Switch to the **Configuration** page.
2. Navigate to **Alerts > Connection Settings**.
3. Set the **Email alerts** toggle to *On*.
4. From the **Connection settings** drop-down list, select *SMTP server (basic authentication)*.
5. In the **SMTP server** field, specify a DNS name or an IP address of the SMTP server. All email notifications (including test messages) will be sent by this SMTP server.
6. In the **Port** field, you can change a communication port for SMTP traffic. The default SMTP port is 25.
7. In the **Timeout** field, specify a timeout for the connection attempt to the SMTP server. The default timeout is 1,000 seconds.
8. In the **Sender** field, enter an email address of the notification sender. This email address will be displayed in the **From** field of the notifications.
9. If your SMTP server requires authentication, select the **Require authentication** check box and specify user credentials in the **Username** and **Password** fields.
10. To save the settings, click **Save**.

#### TIP

Veeam Backup for Salesforce allows you to send a test message to check whether you have configured all settings correctly. To do that, click **Send Test Email** and specify an email address to which the email will be sent.

### Using Modern Authentication

To employ the modern authentication to connect to the Microsoft 365 server, you must first create a Microsoft Entra ID application for Veeam Backup for Salesforce on the Microsoft Identity Platform. To learn how to register an application, see [Microsoft Docs](#).

When creating the application, consider the following:

- The following API permissions must be granted to the application:
  - *SMTP.Send*
  - *Mail.Send*

- The redirect URI added to the application must match the management server FQDN that you use to access the Veeam Backup for Salesforce Web UI. To make sure that you are adding the correct URI, switch to the **Configuration** page and navigate to **Security > Single Sign-On**. The address will be displayed in the **Callback URL** field.

To configure mail server settings, do the following:

1. From the **Connection settings** drop-down list, select *Microsoft 365 (modern authentication)*.
2. In the **Application ID** field, provide the *Application (client) ID* of the registered Microsoft Entra ID application. You can find the ID on the app registration **Overview** pane on the Microsoft Identity Platform.
3. In the **Directory ID** field, specify the *Directory (tenant) ID* of the registered Microsoft Entra ID application. You can find the ID on the app registration **Overview** pane on the Microsoft Identity Platform.
4. In the **Client secret** field, enter the value of a client secret created in the specified application.  
Keep in mind that you can see and copy a *Client Secret* value only when creating it. Otherwise, you will not be able to retrieve the value. To learn how to create client secrets, see [Microsoft Docs](#).
5. To save the settings, click **Save**.  
You will be redirected to the Microsoft Identity Platform. Navigate to the created application page, and grant admin consent to the application. To learn how to do that, see [Microsoft Docs](#).
6. Click **Configure Sender Email**.  
You will be redirected to the Microsoft Identity Platform. Sign in using a Microsoft Identity Platform account that will be used by Veeam Backup for Salesforce to send notification alerts. A user must be assigned a Microsoft 365 license to the Exchange Online service, and a mailbox must be created for this user.

#### TIP

Back to the Veeam Backup for Salesforce Web UI, you can send a test message to check whether you have configured all settings correctly. To do that, specify an email address to which the email will be sent in the **Send Test Email** window.

# Configuring Slack Settings

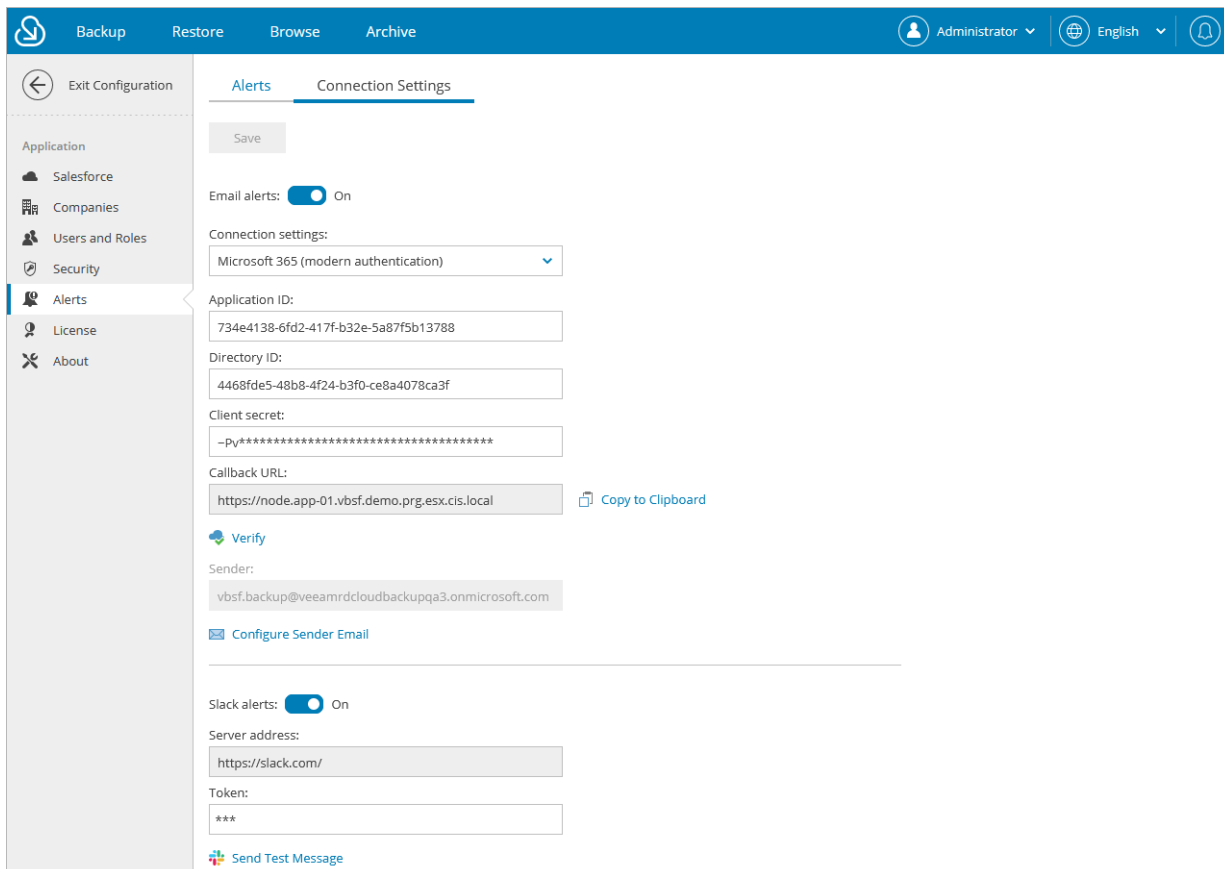
To send alert notifications to specific Slack channels and chats, you must create a Slack app. To learn how to create an app in Slack, see [Slack Documentation](#). Depending on how you want the Slack app to work, the Slack app must be assigned a scope of specific permissions, for example: the `chat:write` permission scope is required to send messages to chats.

To configure Veeam Backup for Salesforce to send alert notifications to Slack, do the following:

1. Switch to the **Configuration** page.
2. Navigate to **Alerts > Connection Settings**.
3. Set the **Slack alerts** toggle to *On*.
4. In the **Token** field, provide an access token generated by the created Slack app. The access token can be found on your Slack [app management page](#) in the **OAuth & Permissions** sidebar menu.
5. To save the settings, click **Save**.

## TIP

Veeam Backup for Salesforce allows you to send a test message to check whether you have configured all settings correctly. To do that, click **Send Test Message** and specify the name of a user or a channel to which the message will be sent.



The screenshot displays the Veeam Backup for Salesforce configuration interface. The top navigation bar includes 'Backup', 'Restore', 'Browse', and 'Archive'. The user is logged in as 'Administrator' and the language is set to 'English'. The left sidebar shows the navigation menu with 'Alerts' selected. The main content area is titled 'Alerts > Connection Settings' and contains the following fields and controls:

- Save** button
- Email alerts:**  On
- Connection settings:** Microsoft 365 (modern authentication) (dropdown menu)
- Application ID:** 734e4138-6fd2-417f-b32e-5a87f5b13788
- Directory ID:** 4468fde5-48b8-4f24-b3f0-ce8a4078ca3f
- Client secret:** -py\*\*\*\*\*
- Callback URL:** https://node.app-01.vbsf.demo.prg.esx.cis.local (with a 'Copy to Clipboard' icon)
- Verify** button
- Sender:** vbsf.backup@veeamrdcloudbackupqa3.onmicrosoft.com (with a 'Configure Sender Email' link)
- Slack alerts:**  On
- Server address:** https://slack.com/
- Token:** \*\*\*
- Send Test Message** button

# Creating Alerts

To create an alert, do the following:

1. Switch to the **Configuration** page.
2. Navigate to **Alerts**.
3. Click **Add**.
4. Complete the **Add Alert** wizard:
  - a. At the **Alert Type** step of the wizard, use the the **Event** drop-down list to select the type of events for which you want to create the alert, and specify the conditions under which Veeam Backup for Salesforce will trigger this alert.

If you select the *Data change* event type, you must also specify a Salesforce organization and choose objects that will be affected by the alert. For an object to be displayed in the list of available objects, it must be added to the backup policy that protects the specified Salesforce organization as described in section [Creating Backup Policies](#). Note that if the list does not contain the necessary object, this means that the object was excluded from the policy.

The screenshot shows the 'Add Alert' wizard in the Veeam Backup for Salesforce interface. The top navigation bar includes 'Backup', 'Restore', 'Browse', 'Archive', and a user profile 'Administ'. The wizard is titled 'Add Alert' and is currently on the 'Specify alert settings' step. On the left, there is a sidebar with 'Alert Type' and 'Recipients'. The main area contains the following settings:

- Event:** A dropdown menu set to 'Data change'.
- Select objects:** A message indicating '1 object(s) selected for Veeam RND1 - nd3 (sandbox)'.
- Alert on:** A dropdown menu set to 'Percentage of records' and a numeric input field set to '30'.
- Triggers:** Three checkboxes are checked: 'Inserted', 'Updated', and 'Deleted'.

At the bottom right, there are 'Next' and 'Cancel' buttons.

- b. At the **Recipients** step of the wizard, you can specify the following notification settings:
  - i. In the **Roles** section, you can limit the scope of users that will receive notifications triggered by the created alert.

If a selected role is assigned to a single user, this user will receive notifications in the Web UI and by email; if a selected role is assigned to a group of users, these users will receive notifications in the Web UI only. To instruct Veeam Backup for Salesforce to send notifications to the group by email, add the group email address to the group settings in Microsoft Azure Entra ID as described in [Microsoft Docs](#).

- ii. In the **Custom recipients** section, you can specify a list of additional email addresses and Slack channel names that will also receive notifications triggered by the created alert.

The addresses of email recipients must be specified in the following format: *email@domain.com*; the addresses of Slack recipients must be specified in either of the following formats: *@username*, *#channelname*, *@userid* or *channelid*. The items in the recipient lists must be separated by a semicolon and whitespace.

For Veeam Backup for Salesforce to be able to send notifications to email addresses and Slack channels, you must configure notifications settings beforehand as described in section [Configuring Notification Settings](#).

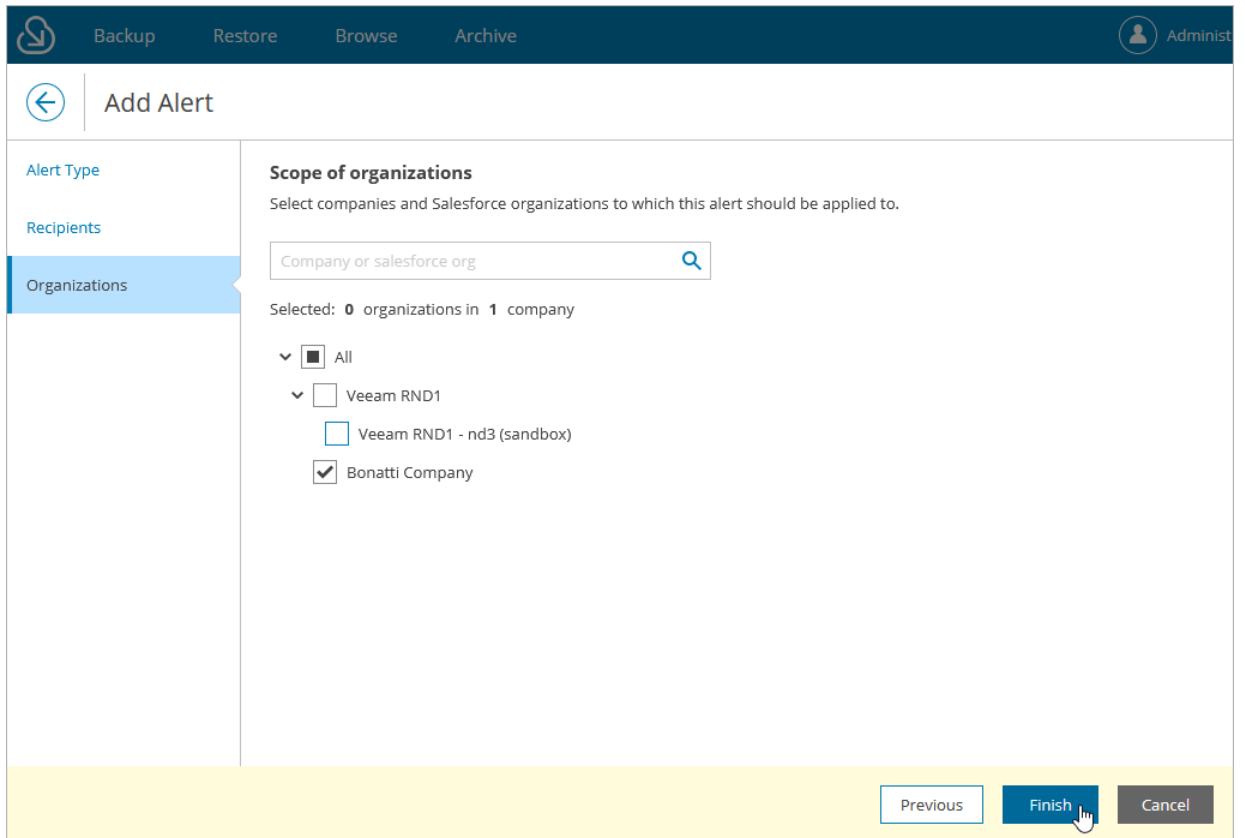
- iii. In the **Subject** and **Threshold** fields, you can provide a subject for notifications that will be triggered by the created alert, and specify the event recurrence threshold that must be breached for Veeam Backup for Salesforce to send the notifications (that is, if you set the threshold to *5*, the product will send a notification only upon the 6th event).

Veeam Backup for Salesforce allows you to pass runtime variables into the subject. For more information, see [Alert Variables](#).

The screenshot shows the 'Add Alert' configuration interface. At the top, there are navigation tabs: Backup, Restore, Browse, Archive, and a user profile icon labeled 'Administ'. Below the navigation is a breadcrumb trail: Add Alert. On the left, there is a sidebar with 'Alert Type' (selected), 'Recipients', and 'Organizations'. The main content area is titled 'Specify recipients and message options'. It includes a 'Roles' section with four checked checkboxes: Administrators, Backup operators, Restore operators, and Viewers. Below this is a 'Custom recipients' section with two unchecked checkboxes: Email (with a greyed-out input field 'Alert channel is not configured') and Slack (with a greyed-out input field 'Alert channel is not configured'). A note states: 'There are more variables you can use to compose a subject line. See the list of supported variables.' The 'Subject' field contains the text: '[%job\_status%]: [%job\_type%] backup for [%salesforce\_name%]'. The 'Threshold' is set to 50, with a dropdown arrow and the text: 'How many times the alert needs to trigger before the message is sent. 0 - send immediately.' At the bottom right, there are three buttons: 'Previous', 'Next', and 'Cancel'.



- c. [This step applies only if you have selected the *Archival policy*, *Backup policy*, *Database connection*, *Encryption job*, *Restore job* or *Salesforce connection* event type] At the **Organizations** step of the wizard, you can choose whether you want to limit the list of companies and Salesforce organizations that will be affected by the created alert.



# Alert Variables

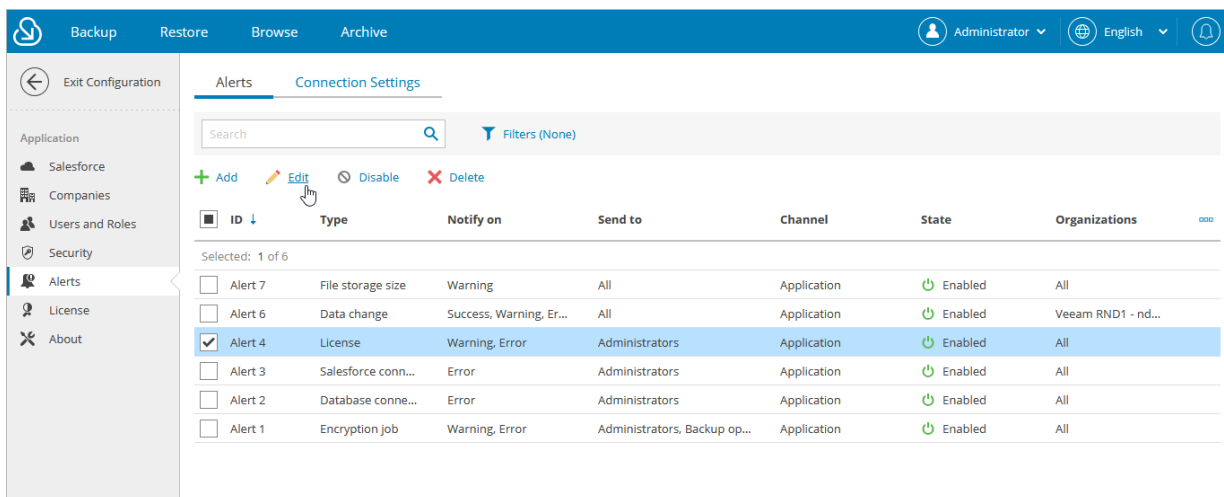
When you specify a subject for notifications, you can use the following runtime variables:

- *[%job\_name%]* – the name of a backup policy or restore job.
- *[%job\_status%]* – the current status of the backup policy or restore job.
- *[%job\_type%]* – the type of a backup job.
- *[%company\_name%]* – the name of a company to which a protected Salesforce organization belongs.
- *[%salesforce\_name%]* – the name of a Salesforce organization whose connection was lost.
- *[%api\_usage%]* – the total number of API requests that were sent to Salesforce.
- *[%deleted%]* – the total number of records that were deleted from Salesforce.
- *[%failed%]* – the total number of records that Veeam Backup for Salesforce failed to process.
- *[%changed%]* – the total number of records that were updated in Salesforce.
- *[%inserted%]* – the total number of new records that were added to the backup policy.
- *[%tip%]* – the total number of *[%changed%]*, *[%deleted%]* and *[%inserted%]* records.
- *[%object\_name%]* – the name of an object whose records are affected by the alert.

# Editing Alerts

For each alert, you can modify settings configured while creating the alert:

1. Switch to the **Configuration** page.
2. Navigate to **Alerts**.
3. Select the necessary alert from the list and click **Edit**.
4. Complete the **Edit Alert** wizard:
  - a. [This step applies only to the *Archival policy*, *Backup policy*, *Data change*, *Encryption job*, *File storage size*, *License* and *Restore job* event types] To modify the conditions under which Veeam Backup for Salesforce will trigger the alert, follow the instructions provided in section [Creating Alerts](#) (step 4a).
  - b. [This step applies only to the *Data change* event type] To modify the list of objects affected by the alert, follow the instructions provided in section [Creating Alerts](#) (step 4a).
  - c. To modify the notification settings configured for the alert, follow the instructions provided in section [Creating Alerts](#) (step 4b).
  - d. [This step applies only to the *Archival policy*, *Backup policy*, *Database connection*, *Encryption job*, *Restore job* or *Salesforce connection* event types] To modify the list of companies and organizations affected by the alert, follow the instructions provided in section [Creating Alerts](#) (step 4c).



# Configuring Advanced Settings

You can view and modify system limits and default settings configured in Veeam Backup for Salesforce. To do that, switch to the **Configuration** page, navigate to **About > Advanced Settings** and click **Confirm**. From the drop-down list, choose whether you want to view the restore or backend advanced settings. Note that only an Administrator can update the advanced settings.

## IMPORTANT

Changing the default advanced settings may result in unsupported or unusable product configuration. Do not change the settings unless it is advised in this document or by the Veeam Customer Support Team. If you change a setting accidentally, select this setting and click **Reset to Default**.

The **Backend service** list shows general settings of the management server and key settings that Veeam Backup for Salesforce uses for backend operations:

- `ui.restore.max.selected.records` – the maximum number of root records that can be restored in one restore job. This parameter applies to all types of restore jobs.
- `sf.api.version` – Salesforce API version of the Veeam backup and backend services.
- `restore.job.draft.lifetime.days` – the period of time (in days) during which the product keeps restore job drafts in the configuration database. If you set this parameter value to `0`, the product will keep job drafts for 1 day only.
- `restore.job.allow.parallel` – defines whether the product runs parallel restore jobs for the same organization.
- `proxy.settings` – the settings of a web proxy that the management server uses to connect to the internet.
- `logging.restore.file.retention` – the period of time (in days) during which the product keeps restore logs in the configuration database and log storage folder.
- `logging.backup.file.retention` – the period of time (in days) during which the product keeps backup logs in the configuration database and log storage folder.
- `logging.backend.file.retention` – the period of time (in days) during which the product keeps configuration logs in the log storage folder.
- `logging.archive.file.retention` – the period of time (in days) during which the product keeps archival session logs in the configuration database and log storage folder.
- `logging.add.domain.filename` – defines whether the product adds the [backend domain name](#) to the name of the downloaded log archive file.
- `encryption.data.object.max.field` – the maximum number of record fields that can be encrypted for one object. Note that if you increase this parameter value, the backup job may take significant time to complete.
- `data.storage.location` – the path to the folder where the product stores backups of Salesforce files and metadata. By default, the product stores backups in the `/opt/vbsf/data` folder. If you change this parameter value, you must move all your backups to a new location manually before enabling backup policies. Note that each Salesforce organization has its unique subfolder containing the organization ID that cannot be modified.
- `backup.metadata.retrieve.batchsize` – the number of metadata files retrieved in one request (batch) to Salesforce during a backup session. If you set this parameter value to `0`, the number of requests sent to Salesforce will depend on the amount of processed data.

- `backup.file.max.failure` – the maximum number of failed attempts to back up a file before the file is excluded from the backup policy. If you set this parameter value to `0`, the file will not be excluded from the backup policy regardless of the number of failed attempts.
- `backup.disk.cache.enabled` – the indication whether the product performs caching of data retrieved from Salesforce. It is recommended that you enable this setting in case a database that is used to store backed-up data is hosted on the same server as Veeam Backup for Salesforce, backed-up data is stored on hard disk drives (HDD), or timeout errors when trying to connect to Salesforce occur.
- `backup.describe.objects.in.batch` – the number of objects in one request sent to Salesforce during a metadata backup session.
- `backend.object.limit.rows` – the maximum number of backed-up records retrieved from the product database that are [displayed on the Browse tab](#). The minimum value is 1; the maximum value is 50,000.
- `backend.metadata.download.files` – the maximum number of metadata files that you can download at a time to the local machine during a [restore operation](#). The minimum value is 1; the maximum value is 500.
- `backend.domain` – the FQDN or IP address of the management server. Keep in mind that this parameter value match the [callback URL in the Connected App settings in Salesforce](#) and [redirect URI in Microsoft Entra ID](#).
- `aws.allowed.region` – the codes of AWS regions to which master keys of the connected AWS account belong. If these parameter values do not match the necessary AWS region codes, the product will not be able to access the keys of this region. For more information on codes, see the [AWS Documentation](#).

The **Restore service** list shows key settings that Veeam Backup for Salesforce uses for restore operations:

- `sf.composite.batch.size` – the number of records the product sends to Salesforce in one request (batch) during a restore session.
- `restore.thread.pool.size` – the number of worker threads processed during a restore session.
- `restore.fetch.size` – the maximum number of records the product retrieves from the product database in one request during a restore session.
- `restore.bulk.threshold` – the maximum number of records sent to Salesforce before the product switches to [Bulk API 2.0](#).
- `restore.bulk.exec.timeout.minutes` – the timeout (in minutes) used for a Bulk API restore job (maximum amount of time (in minutes) for a Bulk API restore job to execute). When the timeout is exceeded, Veeam Backup for Salesforce sends a new bulk request to Salesforce. The default parameter value is 60.
- `log.obfuscation.level` – the level of masking sensitive data in restore logs.
- `hierarchy.default.parent.depth` – the maximum level of the parent object hierarchy that is specified when configuring [hierarchy advanced settings](#). The default parameter value is 1.
- `hierarchy.default.child.depth` – the maximum level to which child records are automatically restored. This setting is applied only to those records that have not been reviewed (customized) [when configuring child hierarchy for restore](#). By default, this parameter is set to 2, that is, the product restores records that you selected at [step 4](#) of the **Restore Records** wizard and 2 levels of child records.
- `archive.thread.pool.size` – the number of worker threads processed during an archival session.
- `archive.fetch.size` – the maximum number of records the product retrieves from the product database in one request during an archival session.

- `archive.bulk.exec.timeout.minutes` – the timeout (in minutes) used for a Bulk API archival job (maximum amount of time (in minutes) for a Bulk API archival job to execute). When the timeout is exceeded, Veeam Backup for Salesforce sends a new bulk request to Salesforce. The default parameter value is 60.

# Performing Salesforce Backup

To perform backup of Salesforce organizations, Veeam Backup for Salesforce runs backup policies. A backup policy is a collection of settings that define the way backup operations are performed: what data to back up, where to store backups, when to start the backup process, and so on.

## NOTE

Only users assigned the *Administrator* or *Backup Operator* role can perform backup operations in Veeam Backup for Salesforce. However, these users can create and run backup policies within their permission scope only – that is, for companies and organizations whose data they can access.

## In This Section

- [Creating Backup Policies](#)
- [Starting and Stopping Backup Policies](#)
- [Disabling and Enabling Backup Policies](#)
- [Editing Backup Policies](#)
- [Removing Backup Policies](#)
- [Viewing Backup Policy Details](#)
- [Viewing Backed-Up Data](#)

# Creating Backup Policies

To create a backup policy, complete the following steps:

1. [Launch the Add Backup Policy wizard.](#)
2. [Configure connection to a Salesforce organization.](#)
3. [Configure policy schedule and backup options.](#)
4. [Enable backup of files and attachments.](#)
5. [Configure encryption settings](#)
6. [Configure retention settings.](#)
7. [Finish working with the wizard.](#)



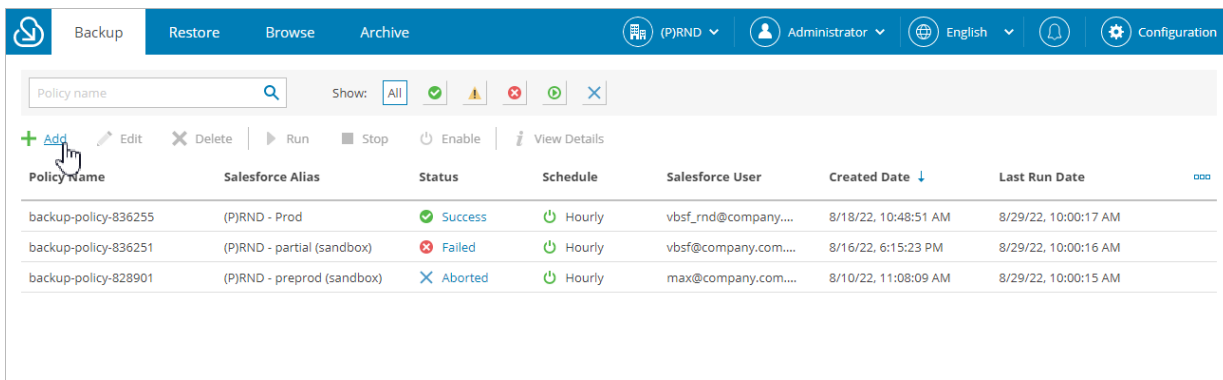
# Step 1. Launch Add Backup Policy Wizard

To launch the **Add Backup Policy** wizard, do the following:

1. Navigate to the **Backup** tab.
2. If you have added multiple companies to Veeam Backup for Salesforce, select a company to which the Salesforce organization whose data you want to protect belongs. To do that, select the company from the drop-down list at the top of the page.

For a company to be displayed in the list of available companies, it must be added to Veeam Backup for Salesforce as described in section [Adding Companies](#). Also, the user launching the **Add Backup Policy** wizard must be granted permissions to access the company as described in section [User Roles and Permissions](#).

3. Click **Add**.



The screenshot shows the Veeam Backup for Salesforce interface. The top navigation bar includes tabs for Backup, Restore, Browse, and Archive. The Backup tab is active. The interface displays a search bar for Policy name, a filter dropdown set to 'All', and a toolbar with icons for Add, Edit, Delete, Run, Stop, Enable, and View Details. Below the toolbar is a table with the following columns: Policy Name, Salesforce Alias, Status, Schedule, Salesforce User, Created Date, and Last Run Date. The table contains three rows of data.

Policy Name	Salesforce Alias	Status	Schedule	Salesforce User	Created Date ↓	Last Run Date
backup-policy-836255	(P)RND - Prod	Success	Hourly	vbsf_rnd@company....	8/18/22, 10:48:51 AM	8/29/22, 10:00:17 AM
backup-policy-836251	(P)RND - partial (sandbox)	Failed	Hourly	vbsf@company.com....	8/16/22, 6:15:23 PM	8/29/22, 10:00:16 AM
backup-policy-828901	(P)RND - preprod (sandbox)	Aborted	Hourly	max@company.com....	8/10/22, 11:08:09 AM	8/29/22, 10:00:15 AM

# Step 2. Configure Connection to Salesforce Organization

At the **Connection** step of the wizard, connect to a Salesforce organization and specify a database that will be used to store backed-up data:

1. In the **Log in with Salesforce account** section:

- a. Choose a Salesforce organization that you want to protect. You can choose an organization that is already connected to Veeam Backup for Salesforce or connect to a new organization. For an organization to be displayed in the list of available organizations, it must not be protected by any other backup policy on this management server.

If you choose an already connected organization, make sure that this organization belongs to the company selected at [step 1](#) of the wizard. Otherwise, it will not be displayed in the list of available organizations. If the organization belongs to a different company, choose the company to which this organization belongs or change the company of the selected organization as described in section [Editing Connections](#).

To connect to a new organization, do the following:

- i. Choose whether you want to use a Salesforce organization hosted on a production instance, sandbox instance or custom domain. If you select the **Custom domain** option, you must also specify the organization domain name.
- ii. Click **Log in with Salesforce account**. You will be redirected to the Salesforce authentication webpage.
- iii. On the Salesforce authentication webpage, enter credentials of a Salesforce user of the organization that you want to protect, and click **Log in**.

The specified Salesforce user must be assigned permissions required for Veeam Backup for Salesforce to be able to perform backup and restore operations. For information, see [Required Permissions](#).

## NOTE

Veeam Backup for Salesforce does not store Salesforce user credentials used to log in to Salesforce. To authorize in Salesforce and access Salesforce data, Veeam Backup for Salesforce uses the Connected App specified during the [initial configuration](#). You can change the Connected App as described in section [Changing Connected App Tokens](#), but keep in mind that after changing the Connected App, you will have to re-authorize all connections to Salesforce organizations added to Veeam Backup for Salesforce.

2. Back to the **Add Backup Policy** wizard, check whether any errors occurred during the authentication process and do the following:

## IMPORTANT

If an error occurs, check whether the Salesforce organization whose user you used to log in to Salesforce is not protected by another backup policy configured on this management server.

- a. In the **Verify permissions** section, verify whether the permissions assigned to the specified user are enough to perform backup and restore operations. To do that, click **Verify permissions** and wait for the check to complete. If any of the permissions are missing, you must grant them in the Salesforce console manually as described in [Salesforce documentation](#).

- b. In the **Connect to a database** section, choose a database that will be used to store backups of the protected Salesforce organization. To do that, click **Select a database**. The **Database connection** window will open.

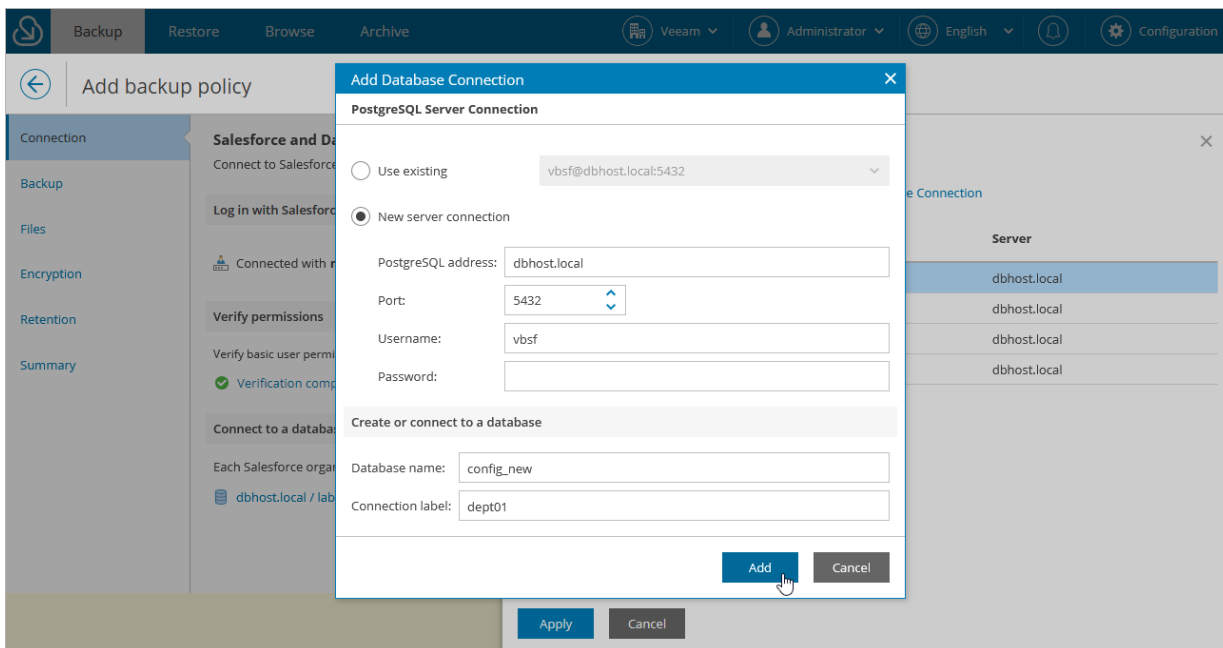
You can add a new database or select a database that has already been added to Veeam Backup for Salesforce:

- To add a database without closing the **Add Backup Policy** wizard, click **New Database Connection** and specify connection settings in the **Add Database Connection** window as described in section [Adding Databases](#).
- To specify an already added database, select the database from the list. For a database to be displayed in the list of available databases, it must be created as described in section [Adding Databases](#). You cannot choose a database that is used to protect any other Salesforce organization as one database can be used to protect one organization only.

## NOTES

When connecting to a database, consider the following:

- You can either connect to an empty database or a database with the same schema as the source database. In latter case, the organization IDs of the both databases must be the same.
- You can connect only to a database that belongs to the company that you selected at [step 1](#) of the wizard.



## Step 3. Configure Backup Settings

At the **Backup** step of the wizard, specify schedules according to which Veeam Backup for Salesforce will launch policy sessions, exclude objects and fields from the backup scope, automatically add new objects and fields to the policy, and limit API calls sent by Veeam Backup for Salesforce to Salesforce:

1. [Configure schedules for the backup policy.](#)
2. [Configure additional backup options.](#)

## Step 3a. Configure Backup Schedules

In the **Backup schedule** section of the **Backup** step of the wizard, configure default and custom schedules for the backup policy.

Veeam Backup for Salesforce has 3 built-in schedules:

- Hourly – this schedule launches a backup policy session at the beginning of every hour.
- Daily – this schedule launches a backup policy session every day at 00:00 UTC.
- Weekly – this schedule launches a backup policy session every Sunday at 00:00 UTC.

### NOTE

You cannot edit or remove the built-in schedules. If none of the built-in schedules meets your business needs, you can create a new schedule. To learn how to create schedules, see [Creating Schedules](#).

## Specifying Default Schedule for Backup Policy

From the **Default schedule for this policy** drop-down list, select a default schedule that will be used to back up data of all objects of the protected organization that have no [custom schedules assigned](#), to back up object metadata, to back up files and attachments if you enable this functionality at [step 4](#) of the wizard, and to back up new objects and fields if you select this option in the [Additional backup options](#) section. You can select one of the built-in schedules or create a new one as described in section [Creating Schedules](#).

## Specifying Custom Schedules for Protected Objects

If some objects are updated frequently and need to be backed up more or less often than other objects belonging to the protected Salesforce organization, you can assign custom schedules to these objects. Veeam Backup for Salesforce will launch a separate backup session to protect each group of objects according to the assigned schedule. It is recommended that you assign the same schedule to the related Salesforce objects to ensure that these objects can be restored properly.

To assign a schedule to an object, do the following:

1. Click the link in the **Custom schedules** field.
2. In the **Specify schedule per object** window, do the following:
  - a. In the **Object** list, select check boxes next to the objects that must be protected according to a specific schedule.
  - b. Click **Assign schedule**, choose the necessary schedule from the **Schedule** drop-down list in the **Assign schedule** window, and click **Assign**.

### TIP

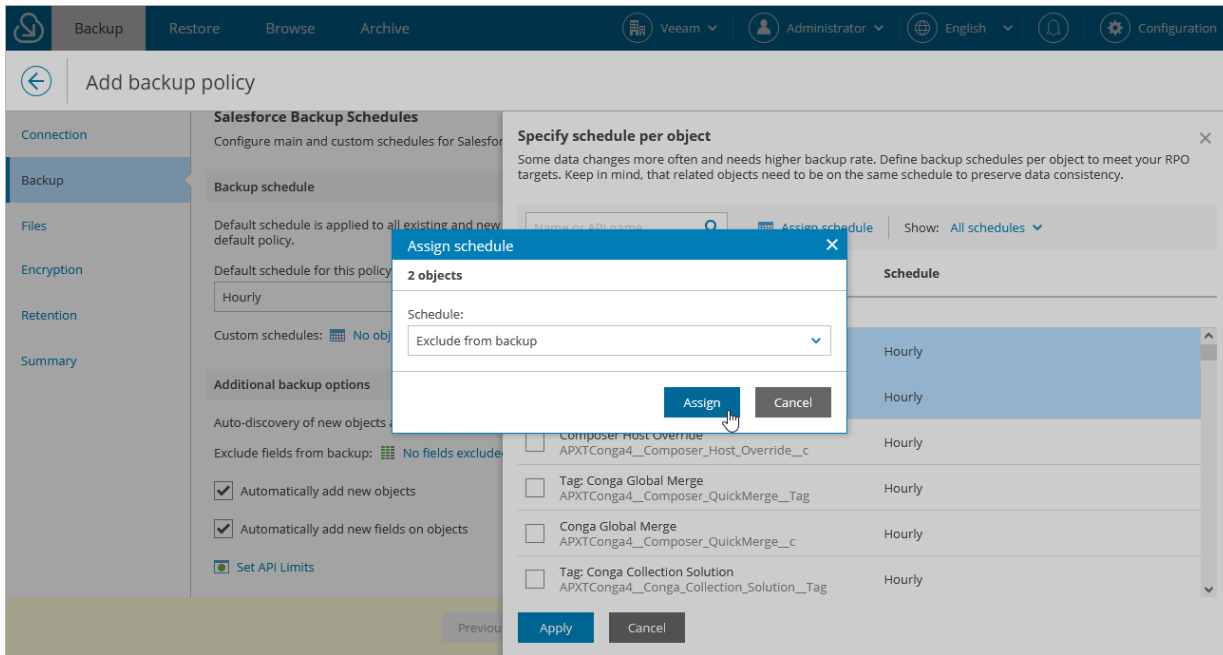
By default, Veeam Backup for Salesforce backs up all supported Salesforce objects of the protected organization. However, some Salesforce objects cannot be restored, such as history objects. If you do not want to back up these or any other objects of the organization, you can exclude them from the backup policy. To do that, select the **Exclude from backup** option from the **Schedule** drop-down list.

Salesforce objects that are not backed up by Veeam Backup for Salesforce are listed in [Appendix A. Unsupported Objects](#).

- c. Click **Apply** to save the changes.

## NOTE

By design, the user and organization objects are automatically added to every schedule configured for the backup policy. You cannot exclude these objects manually.



# Creating Schedules

## IMPORTANT

If you plan to run multiple backup policies at the same time, it is recommended that you add at least 256 MB of RAM per one backup schedule.

To create a new backup schedule for the policy at the **Backup** step of the wizard, do the following:

1. In the **Backup schedule** section, click **Manage Schedules**.
2. In the **Manage Schedules** window, click **Add New Schedule**.
3. In the **Add New Schedule** window, do the following:
  - a. In the **Schedule name** field, specify a name for the schedule. The name must be unique for the company selected at [step 1](#).
  - b. In the **Start policy** section, select the schedule type:
    - To run a backup policy once, select **Once at** and specify the time when the backup policy must run.

Note that you cannot combine one-time schedules with periodic schedules when configuring the [default schedule and custom schedules](#) for backup policy. If you select the *Once at* type of schedule as the default policy schedule, you must manually remove all periodic schedules configured for Salesforce objects, wait for the policy session to complete, and then re-configure periodic schedules for the policy.

- To run a backup policy periodically, select **Daily** and specify how often you want Veeam Backup for Salesforce to run the policy.

## NOTE

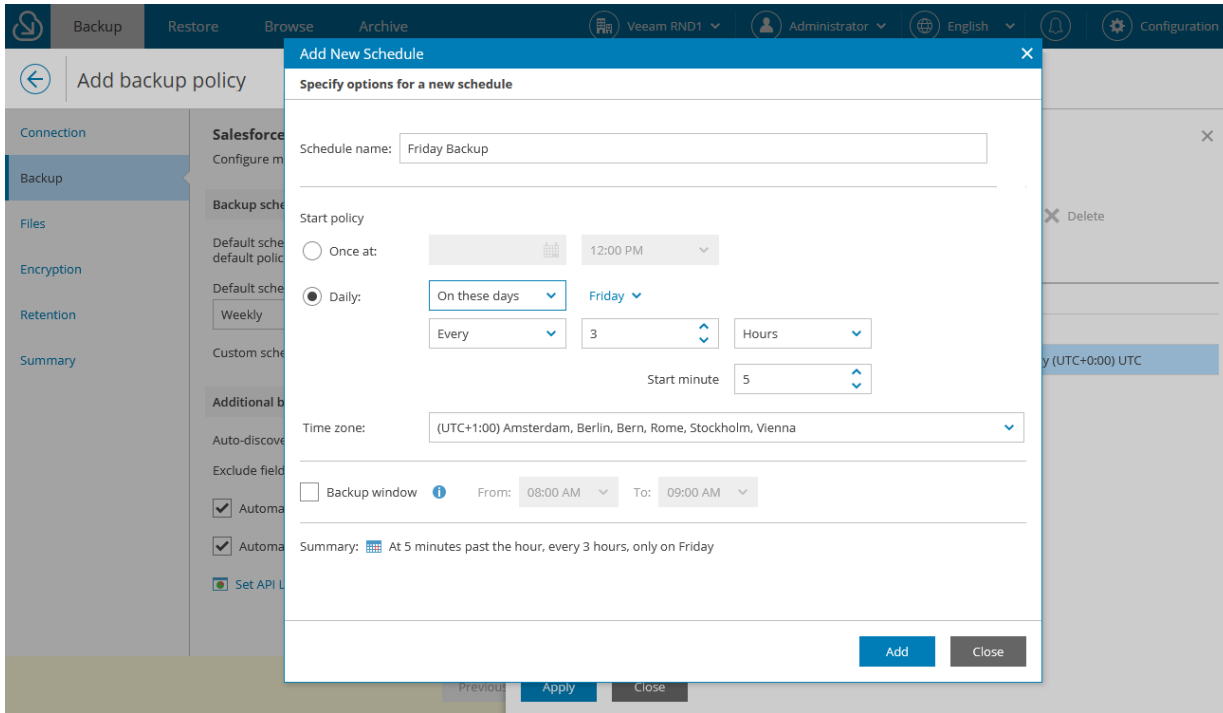
The configured schedules are stored in the CRON format and used to run policy sessions. If you specify to run a session every 9 hours, Veeam Backup for Salesforce will follow the following schedule (UTC): Mon 09:00, Mon 18:00, Tue 09:00, Tue 18:00 and so on.

- c. [Applies if you have selected the **Daily** option] If you want the backup policy to run only during the specific period of time, select the **Backup window** check box and specify the time interval.
- d. From the **Time zone** drop-down list, select a UTC time offset. By default, the time zone of your browser is selected.
- e. Review the settings and click **Add**.

The created schedule will be available in all backup policies created for Salesforce organizations within one company. You can further edit or delete these schedules.

## IMPORTANT

If you delete a schedule that is used to back up any objects in the current or in any other backup policy within the company, Veeam Backup for Salesforce will raise a warning. To eliminate the warning, specify a schedule that will replace the deleted one. Consider that the schedule will be replaced in all backup policies created for this company.





## Step 3b. Configure Additional Options

In the **Additional backup options** section of the **Backup** step of the wizard, you can specify data protection settings and limit the API requests.

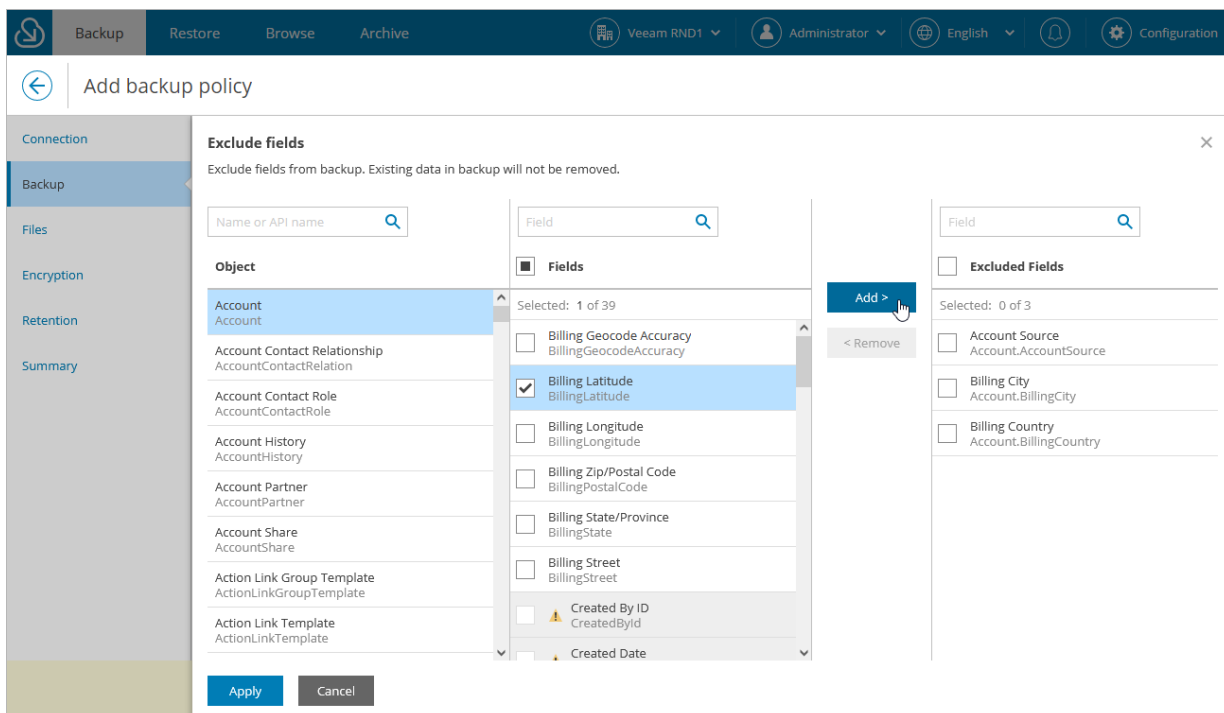
### Specifying Additional Options

To specify additional data protection options, do the following:

1. To exclude specific object fields from the backup policy, click the link in the **Exclude fields from backup** field.  
In the **Exclude fields** window:
  - a. From the **Object** list, select an object whose fields you want to exclude.
  - b. From the **Fields** list, select the necessary fields.
  - c. Click **Add**.
  - d. Repeat steps a-c for all fields that you want to exclude.
  - e. Click **Apply** to save the changes.
2. To automatically protect new objects added to the Salesforce organization, select the **Automatically add new objects** check box.
3. To automatically protect new object fields, select the **Automatically add new fields on objects** check box.

#### NOTE

While creating a backup, Veeam Backup for Salesforce can automatically process database schema changes such as adding or removing objects and fields. Keep in mind that if you change a field type in Salesforce, this may result in a backup failure.



# Setting API Request Limits

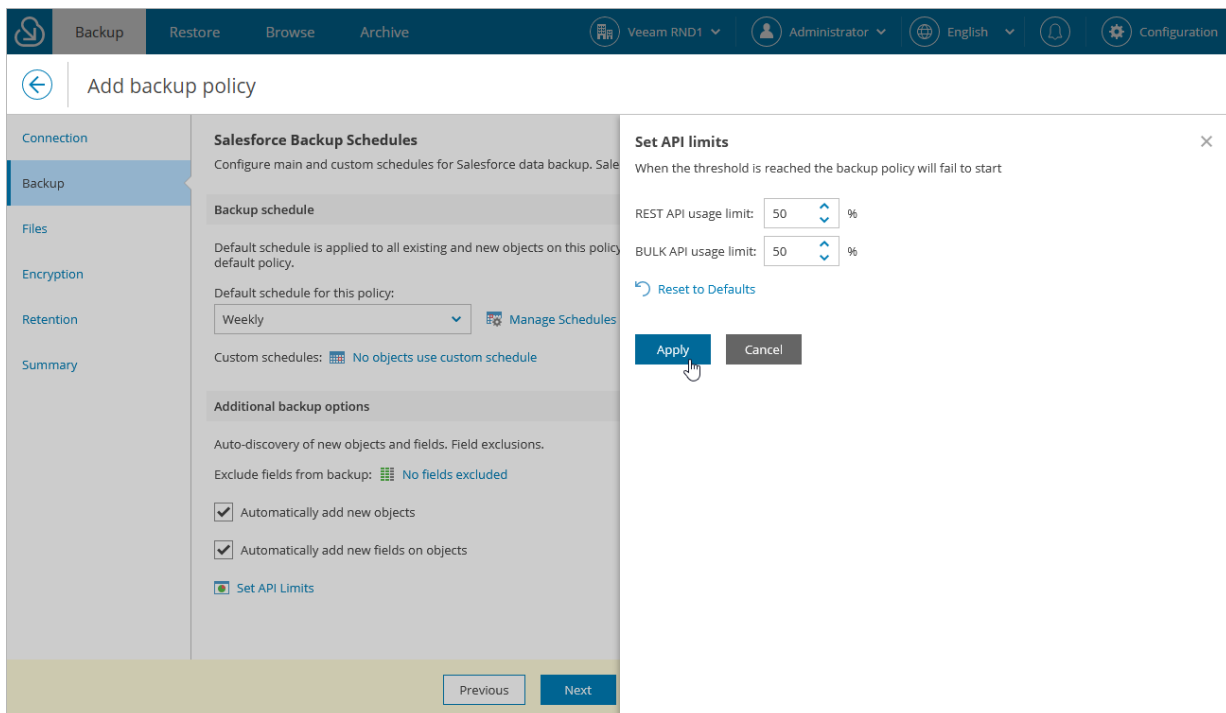
The total number of API requests that can be sent to Salesforce within 24 hours is limited for each Salesforce organization. To ensure that Veeam Backup for Salesforce does not conflict with other applications that use API requests for integration with Salesforce, it is strongly recommended that you specify thresholds for REST API and BULK API requests that must not be breached during backup operations. For more information on the API request limits, see [Salesforce Documentation](#).

By design, Veeam Backup for Salesforce checks the number of remaining API requests every time it starts a new policy session:

- If any of the specified thresholds is breached, the session fails with an error indicating that the API request limit has been exceeded.
- If none of the specified thresholds is breached, Veeam Backup for Salesforce starts processing objects added to the policy one by one.

Every time it processes a new object, it checks the number of remaining API requests – if any of the specified thresholds is breached, the session fails with an error indicating that the API request limit has been exceeded, and all objects that have not been processed yet remain unprotected. However, Veeam Backup for Salesforce continues sending requests to Salesforce to back up objects whose processing started before the session failed. The latter may cause Veeam Backup for Salesforce to accidentally exceed the maximum limit of API requests that you specified.

To specify the REST API and BULK API request thresholds, click **Set API Limits** and enter the necessary threshold values (in percentage) in the **Set API limits** window.



# Step 4. Enable Backup of Files and Attachments

[This step is available only if the Salesforce user that you have specified at step 2 of the wizard is assigned the [Query All Files](#) permission in Salesforce]

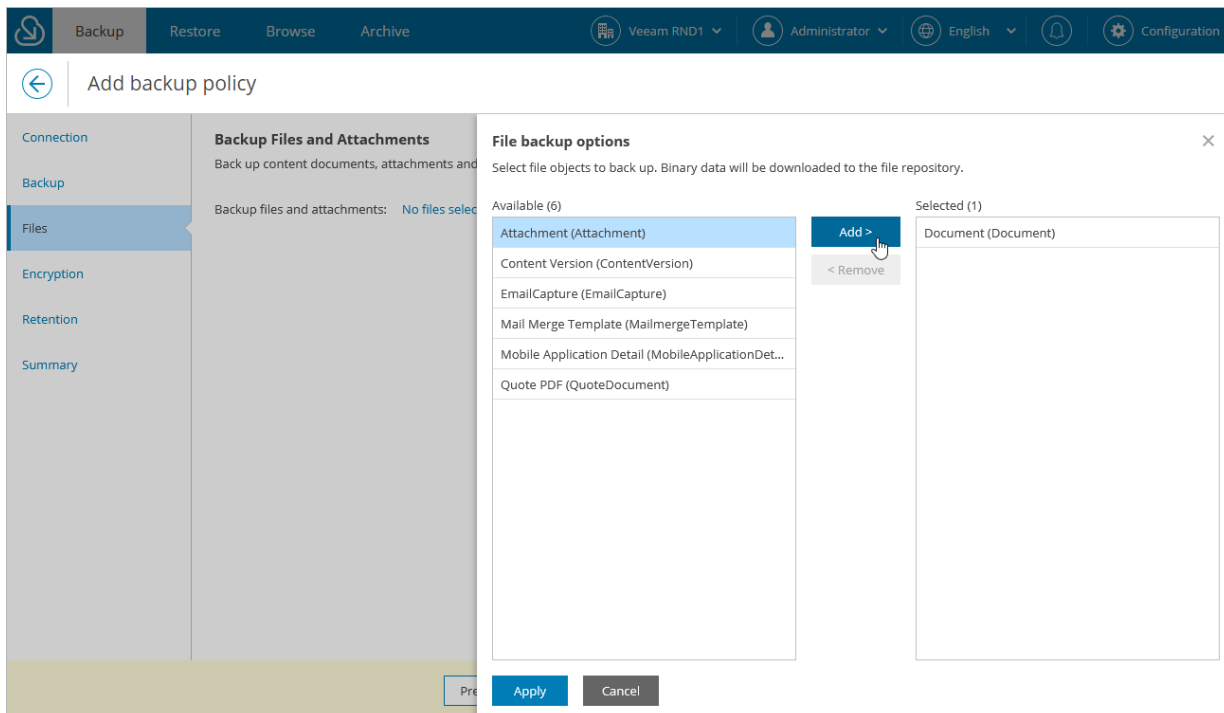
## IMPORTANT

Veeam Backup for Salesforce 3.0 allows you to back up the *MobileApplicationDetail* and *MailmergeTemplate* type of content. However, restore of this type of content is not supported.

At the **Files** step of the wizard, you can choose types of files that you want to back up. To do that, click the link in the **Backup files and attachments** field and select the necessary file types in the **File backup options** window. Veeam Backup for Salesforce will display in the **Repository location** field the local directory on the management server that will be used to store the backed-up files.

## NOTES

- For each protected organization, the product automatically creates a subfolder with a unique name containing the organization ID that cannot be modified. Therefore, if you remove a backup policy and then create a new policy for the same organization, Veeam Backup for Salesforce will use the same backup location for this organization.
- If you remove a backup policy, data stored in the specified location will not be removed automatically. If you do not need the backed-up files and attachments anymore, you must delete them manually.



# Step 5. Configure Encryption Settings

At the **Encryption** step of the wizard, you can configure the following encryption settings:

1. In the **Encryption settings** section, choose whether you want to encrypt specific object fields, file types or both. If you do not select any object fields or file types, this data will not be encrypted.

For a file type to be displayed in the list of available file types, it must be added to the backup policy at [step 3](#) of the wizard, and the **Backup files and attachments toggle** must be set to *On* at [step 4](#) of the wizard.

## NOTES

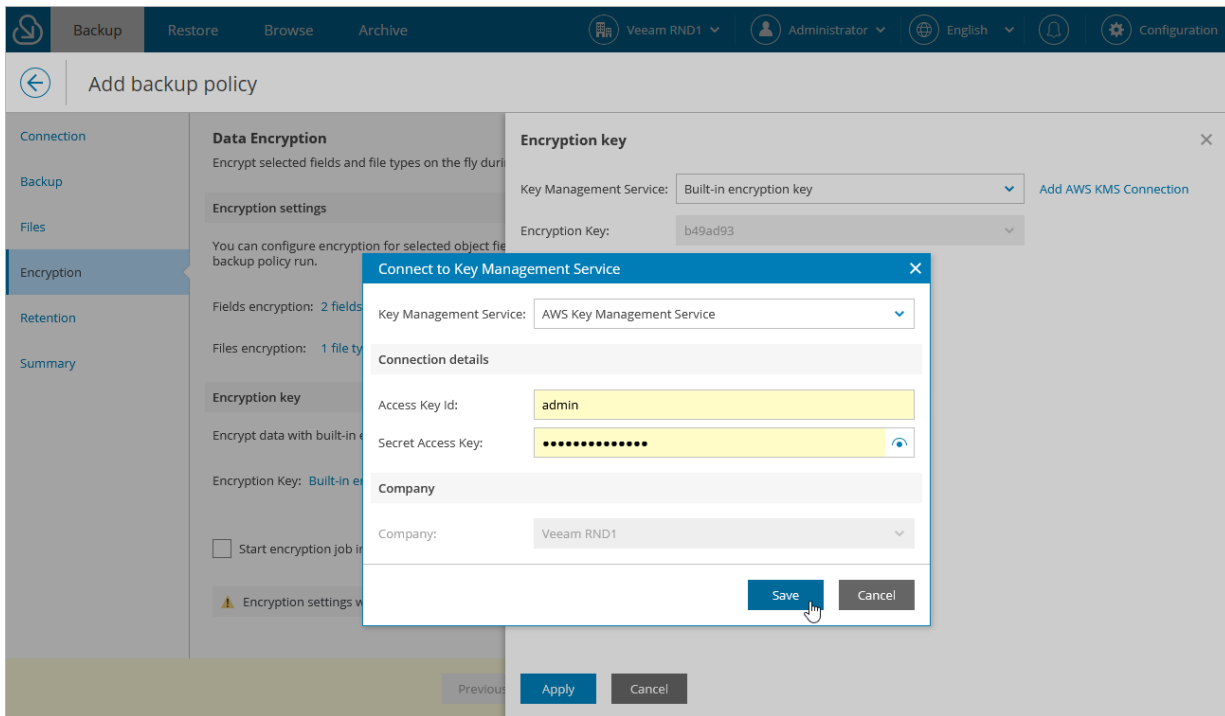
- If an object record that you want to back up contains fields that have been specified as filtering conditions in an archival policy, you will not be able to encrypt these fields. [Edit the filtering criteria settings](#) of the archival policy – and then modify the backup policy settings to encrypt these fields.
- By default, you can encrypt maximum 10 fields for one object. To be able to encrypt more object fields, modify the `encryption.data.object.max.field` parameter value as described in section [Configuring Advanced Settings](#).

2. In the **Encryption key** section, choose whether you want to encrypt backed-up data using an AWS master key or a built-in master key generated by Veeam Backup for Salesforce. If you want to use an AWS master key, you must also select the region to which the key belongs.

For an AWS master key to be displayed in the list of available keys, it must be added to the selected region in an AWS account as described in [AWS Documentation](#), and this account must be connected to Veeam Backup for Salesforce as described in section [Configuring Encryption Settings](#). If you have not connected the AWS account beforehand, you can do it without closing the **Add Backup Policy** window. To do that, click **Add AWS KMS Connection** and follow the instructions provided in section [Adding Connections](#).

## IMPORTANT

If you choose to encrypt backed-up data with a built-in encryption key, it is recommended that you download the data key to your workstation as described in section [Managing Encryption Keys](#). Otherwise, Veeam Backup for Salesforce will be not able to decrypt the data in case you migrate the product to another workstation.



# Step 6. Configure Retention Settings

At the **Retention** step of the wizard, you can configure retention settings for the backed-up data – a time period during which Veeam Backup for Salesforce keeps history records and attachments that were deleted from Salesforce. It allows you to consume less storage space by deleting history records and attachments that are older than the specified time period.

Consider the following:

- The time period is calculated since creation of a backup of a Salesforce record, not since creation of the record itself.
- Veeam Backup for Salesforce will always keep the latest version of a record in the backup even if the specified retention limit is reached and the record has been deleted from Salesforce.

To configure retention settings for the backup policy, do the following:

1. In the **Data and attachments retention policy** section:
  - a. In the **Keep versions for** field, specify the number of days (weeks, months, years) for which you want to keep Salesforce history records and deleted attachments.
  - b. If you want to configure specific retention settings for different objects protected by the backup policy, click the **Define custom retention policy** link.

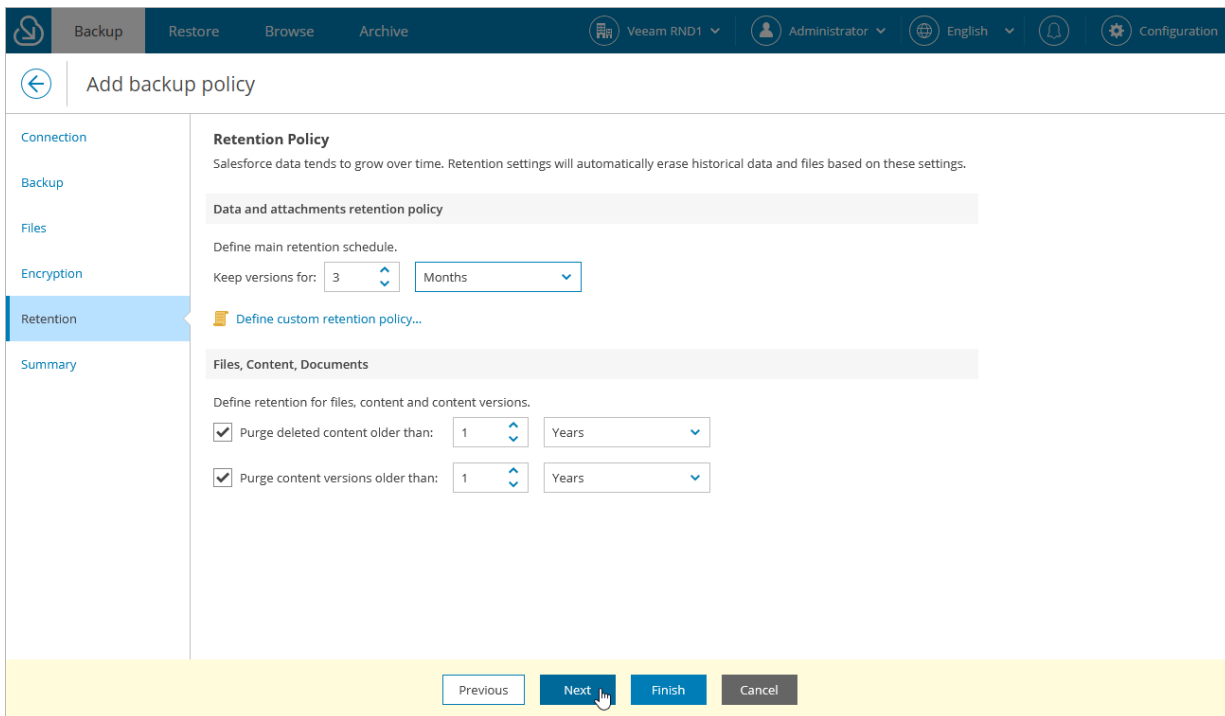
In the **Custom Retention Settings** window, click **Add Object**, select the necessary object from the **Object** drop-down list, and specify the retention period. Click **Apply**.

## IMPORTANT

Attachments associated with records to which custom retention settings are applied will still be removed according to the main data and attachments retention policy specified in the **Keep versions for** field.

2. The settings specified in the **Data and attachments retention policy** section do not apply to backups of Files, Content and Documents created by the policy. If you want Veeam Backup for Salesforce to automatically delete these backups according to the retention policy, you must configure their own retention settings in the **Files, Content, Documents** section:
  - To instruct Veeam Backup for Salesforce to remove backups of files that were permanently deleted from Salesforce according to the retention policy, select the **Purge deleted content older than** check box and specify the period after which these files will be removed.

- To instruct Veeam Backup for Salesforce to remove backups of file versions, select the **Purge content versions older than** check box and specify the period after which the outdated versions will be removed.



# Step 7. Finish Working with Wizard

At the **Summary** step of the wizard, review configured settings and click **Finish**.

The screenshot shows the 'Add backup policy' wizard in the Summary step. The interface includes a top navigation bar with 'Backup', 'Restore', 'Browse', and 'Archive' tabs. The main content area is divided into a left sidebar with navigation links (Connection, Backup, Files, Encryption, Retention, Summary) and a main panel displaying configuration details. At the bottom, there are three buttons: 'Previous', 'Finish', and 'Cancel'. A mouse cursor is pointing at the 'Finish' button.

Section	Property	Value
Objects	Main schedule:	Weekly
	Objects count:	353
	Excluded objects:	0
	Automatically add new objects:	Yes
Files	Automatically add new fields:	Yes
	Exclude fields:	0
Files	Document:	Yes
Encryption	Fields encryption:	2
	Files encryption:	1
Retention	Data and attachments:	3 months
	Custom data retention:	—
	Files, content, documents:	1 year
	File versions retention:	1 year



# Starting and Stopping Backup Policies

You can start a backup policy manually, for example, if you want to create an additional backup in the backup chain and do not want to modify the configured backup policy schedules. You can also stop a backup policy if processing of a session is about to take too long, and you do not want the policy to have an impact on the production environment during business hours.

To start or stop a backup policy:

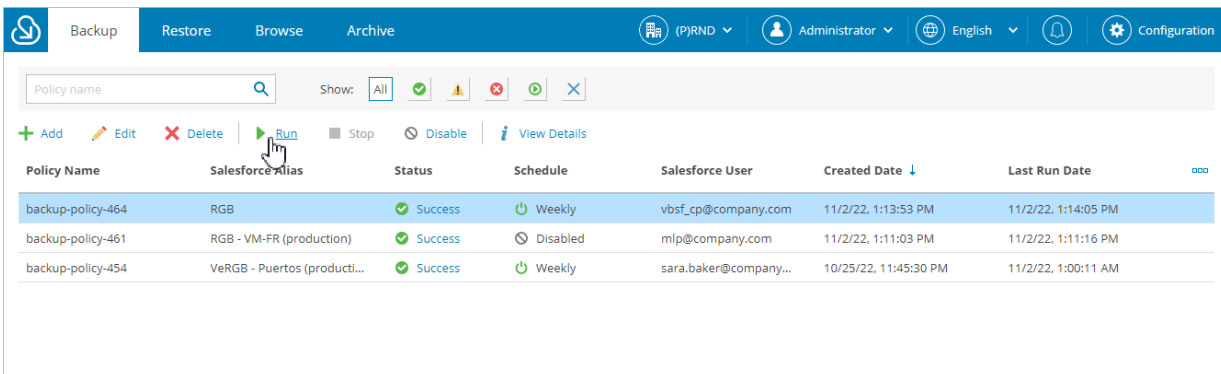
1. Navigate to the **Backup** tab.
2. From the **Organization** drop-down list, select a Salesforce organization for which the backup policy has been created.
3. Select the necessary backup policy.

You can filter backup policies displayed on the **Backup** tab by using the icons in the **Show** field at the top of the list. If you select a filter, the settings will apply to all companies and will not change during the current user session. That is why if you do not see the necessary policy in the list, make sure that the **All** filter is selected.

4. Click **Run** or **Stop**. Keep in mind that if you run a backup policy, it will automatically launch all backup schedules configured for this policy.

If you stop the running backup policy, in the **Confirm Policy Stop** window, do the following:

- Click **Hard Stop** to immediately stop the backup policy. In this case, Veeam Backup for Salesforce will interrupt the currently running backup session, and the backup policy will acquire the *Aborted* status.
- Click **Graceful Stop** to complete backup for Salesforce objects that are already being processed by the backup session. Veeam Backup for Salesforce will stop the policy execution when backup of the processed objects is finished, and the backup policy will acquire the *Stopped* status.



# Disabling and Enabling Backup Policies

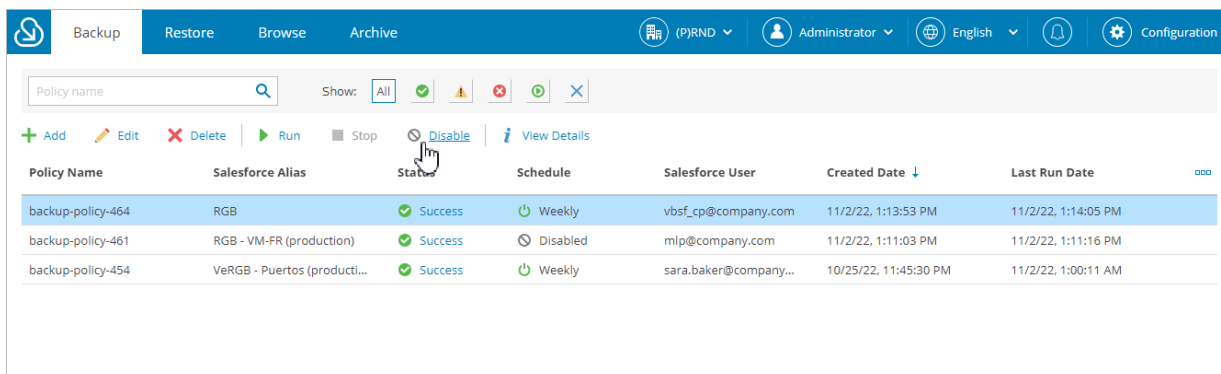
By default, Veeam Backup for Salesforce runs all created backup policies according to the specified schedules. However, you can temporarily disable a backup policy so that Veeam Backup for Salesforce does not run the backup policy automatically. You will still be able to manually start or enable the disabled backup policy at any time you need.

To disable or enable a backup policy, do the following:

1. Navigate to the **Backup** tab.
2. From the **Organization** drop-down list, select a Salesforce organization for which the backup policy has been created.
3. Select the necessary backup policy.

You can filter backup policies displayed on the **Backup** tab by using the icons in the **Show** field at the top of the list. If you select a filter, the settings will apply to all companies and will not change during the current user session. That is why if you do not see the necessary policy in the list, make sure that the **All** filter is selected.

4. Click **Disable** or **Enable**.



Policy Name	Salesforce Alias	Status	Schedule	Salesforce User	Created Date ↓	Last Run Date
backup-policy-464	RGB	Success	Weekly	vbsf_cp@company.com	11/2/22, 1:13:53 PM	11/2/22, 1:14:05 PM
backup-policy-461	RGB - VM-FR (production)	Success	Disabled	mlp@company.com	11/2/22, 1:11:03 PM	11/2/22, 1:11:16 PM
backup-policy-454	VeRGB - Puertos (producti...	Success	Weekly	sara.baker@company...	10/25/22, 11:45:30 PM	11/2/22, 1:00:11 AM

# Editing Backup Policies

For each backup policy, you can modify settings configured while creating the policy:

1. Navigate to the **Backup** tab.
2. From the **Organization** drop-down list, select a Salesforce organization for which the backup policy has been created.
3. Select the necessary backup policy.

You can filter backup policies displayed on the **Backup** tab by using the icons in the **Show** field at the top of the list. If you select a filter, the settings will apply to all companies and will not change during the current user session. That is why if you do not see the necessary policy in the list, make sure that the **All** filter is selected.

4. Click **Edit**.

## IMPORTANT

If you encounter an error while trying to reconnect to the Salesforce organization, check whether the specified credentials belong to a user from the same Salesforce organization.

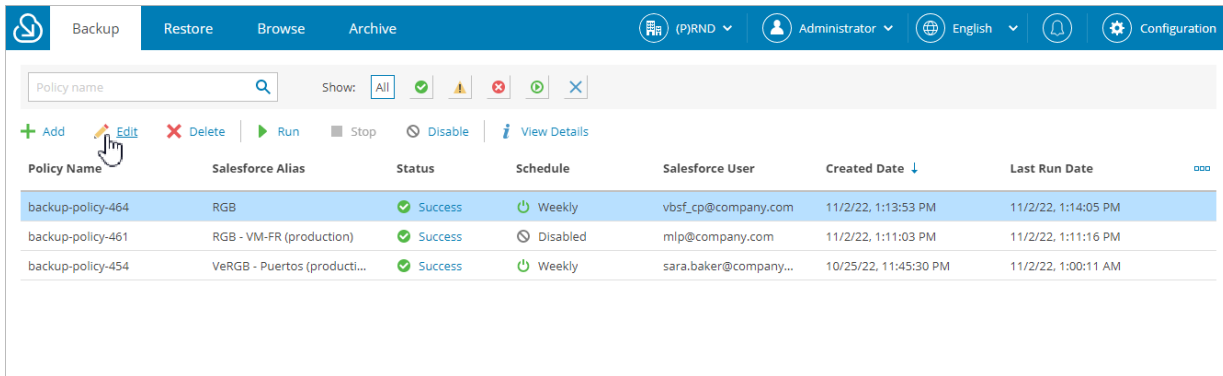
5. Complete the **Edit Backup Policy** wizard:
  - a. To choose another database that will be used to protect your Salesforce organization, follow the instructions provided in section [Creating Backup Policies](#) (step 2).
  - b. To change the schedule configured for the policy, follow the instructions provided in section [Creating Backup Policies](#) (step 3.1).
  - c. To modify the excluded fields and change the specified API limits, follow the instructions provided in section [Creating Backup Policies](#) (step 3.2).

## TIP

If an object record that you want to back up contains fields that were specified as filtering conditions in an archival policy, you will not be able to exclude these fields from the backup policy. [Edit the filtering criteria settings](#) of the archival policy – and then modify the backup policy settings to exclude these fields from the backup scope.

- d. To modify the list of files and attachments that you want to back up, follow the instructions provided in section [Creating Backup Policies](#) (step 4).
- e. To change the encryption settings configured for the policy, follow the instructions provided in section [Creating Backup Policies](#) (step 5). You can also instruct Veeam Backup for Salesforce to run an encryption job immediately after completing the wizard. To do that, select the **Start now. Encryption change is applied immediately after saving policy** check box. If you clear this check box, the product will run the encryption job an hour after you complete the wizard.
- f. To change the retention settings configured for the policy, follow the instructions provided in section [Creating Backup Policies](#) (step 6).

g. At the **Summary** step of the wizard, review configuration information and click **Finish** to confirm the changes.



The screenshot displays the 'Summary' step of the Veeam Backup for Salesforce wizard. The interface includes a top navigation bar with tabs for 'Backup', 'Restore', 'Browse', and 'Archive'. The user is logged in as 'Administrator' and the language is set to 'English'. Below the navigation bar is a search field for 'Policy name' and a 'Show:' filter set to 'All'. A toolbar contains icons for '+ Add', 'Edit' (highlighted with a mouse cursor), 'Delete', 'Run', 'Stop', 'Disable', and 'View Details'. The main area features a table with the following columns: Policy Name, Salesforce Alias, Status, Schedule, Salesforce User, Created Date, and Last Run Date. Three policies are listed:

Policy Name	Salesforce Alias	Status	Schedule	Salesforce User	Created Date	Last Run Date
backup-policy-464	RGB	Success	Weekly	vbsf_cp@company.com	11/2/22, 1:13:53 PM	11/2/22, 1:14:05 PM
backup-policy-461	RGB - VM-FR (production)	Success	Disabled	mlp@company.com	11/2/22, 1:11:03 PM	11/2/22, 1:11:16 PM
backup-policy-454	VeRGB - Puertos (producti...	Success	Weekly	sara.baker@company...	10/25/22, 11:45:30 PM	11/2/22, 1:00:11 AM

# Removing Backup Policies

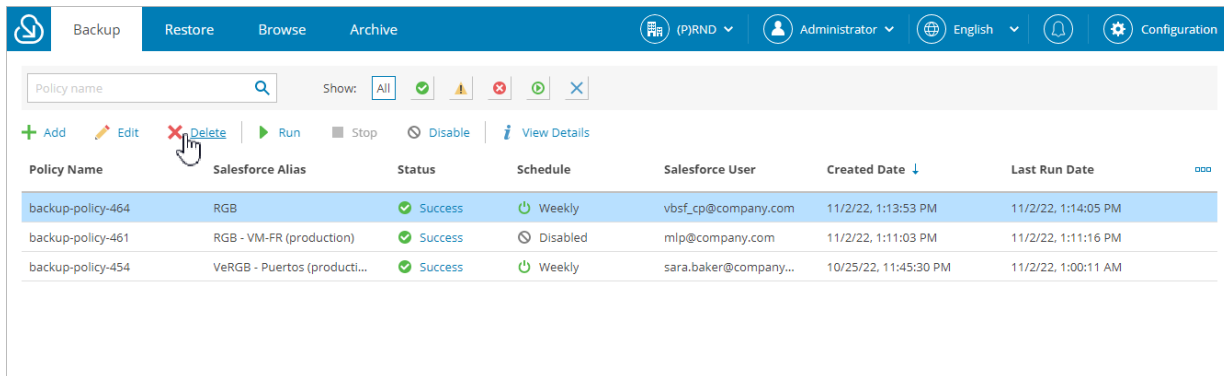
Veeam Backup for Salesforce allows you to permanently remove a backup policy from the configuration database if you no longer need it. Note that the backed-up data will not be automatically deleted from the product database when you remove the policy.

To remove a backup policy, do the following:

1. Navigate to the **Backup** tab.
2. From the **Organization** drop-down list, select a Salesforce organization for which the backup policy has been created.
3. Select the necessary backup policy.

You can filter backup policies displayed on the **Backup** tab by using the icons in the **Show** field at the top of the list. If you select a filter, the settings will apply to all companies and will not change during the current user session. That is why if you do not see the necessary policy in the list, make sure that the **All** filter is selected.

4. In the **Delete Confirmation** window, click **Remove** to acknowledge the operation.



# Viewing Backup Policy Details

After you create backup policies, Veeam Backup for Salesforce displays the policies on the **Backup** tab. Users assigned any role can see information on backup policies created for Salesforce organizations to which data they have access.

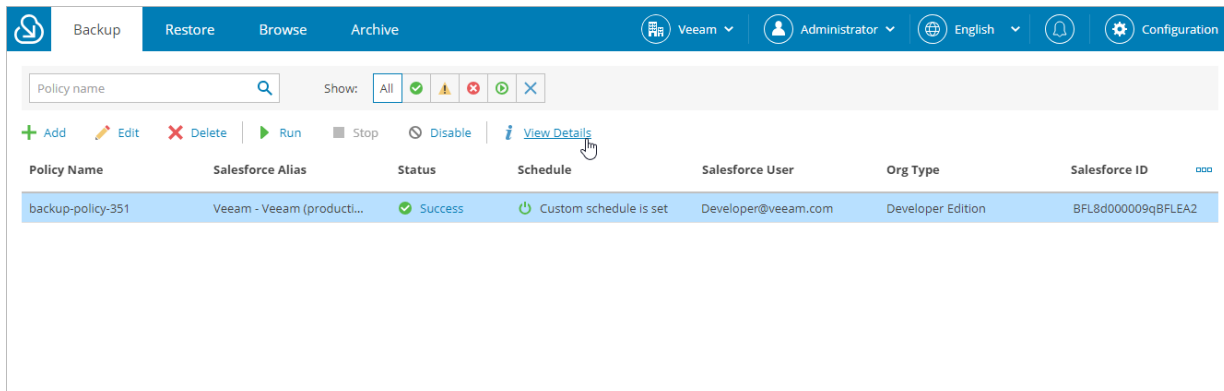
You can filter backup policies displayed on the **Backup** tab by using the icons in the **Show** field at the top of the list. If you select a filter, the settings will apply to all companies and will not change during the current user session. That is why if you do not see the necessary job in the list, make sure that the **All** filter is selected.

Each policy in the list is described with the following set of properties:

- **Policy Name** – the name of the backup policy.
- **Salesforce Alias** – the name of the protected Salesforce organization displayed in the Veeam Backup for Salesforce Web UI. To change the Salesforce alias, follow the instructions provided in section [Editing Organizations](#).
- **Status** – the status of the latest backup policy session.  
To see all policy sessions, click the link in the **Status** column. For more information, see [Viewing Backup Policy Sessions](#).
- **Schedule** – the name or status of the schedule configured for the backup policy.
- **Salesforce User** – the name of a Salesforce account specified during the policy configuration.
- **Org Type** – the type of the Salesforce protected organization.
- **Salesforce ID** – the ID assigned to the organization in Salesforce.
- **Salesforce URL** – the URL of the protected Salesforce organization.
- **Company** – the name of a company to which the protected Salesforce organization belongs.
- **Created Date** – the date and time when the backup policy was created.
- **Last Run Date** – the date and time when the latest backup policy session started.

## TIP

You can view settings configured for a specific backup policy. To do that, select the necessary backup policy and click **View Details**.



# Viewing Backup Policy Sessions

For each performed data protection operation, Veeam Backup for Salesforce starts a new session according to the created backup jobs, and stores the session details in the product database. You can track real-time statistics of all running and completed operations on the **Backup** tab. To view the full list of tasks executed during an operation, click the link in the **Status** column.

The **Backup Sessions** section of the **Backup** tab displays information on all sessions of the backup policy. Each session is described with the following set of properties:

- **Session ID** – the ID assigned to the session.
- **Type** – the type of a [backup job](#) launched during the session.
- **Start** – the date and time when the session started.
- **Finish** – the date and time when the session ended.
- **Status** – the current status of the session.
- **Message** – the explanation why Veeam Backup for Salesforce failed to process the records (applies only to sessions with the *Warning* and *Error* statuses).
- **Processed Objects** – the total number of objects processed during the session.
- **API Usage** – the total number of API calls sent during the session.
- **Inserted** – the total number of new Salesforce records added to the backup scope during the session.
- **Updated** – the total number of Salesforce records updated in Salesforce during the session.
- **Deleted** – the total number of Salesforce records deleted from Salesforce during the session.
- **Failed** – the total number of Salesforce records that Veeam Backup for Salesforce failed to process.
- **Total** – the total number of Salesforce records processed during the session.
- **Run Type** – the type of the job run (defines whether the policy has been launched manually or automatically by schedule).
- **Schedule** – the name of the schedule according to which the backup job has been launched.

The **Session Details** section of the **Backup** tab displays information on all objects included in a specific policy session. Each object is described with the following set of properties:

- **Object / Event** – the name of the backed-up object.
- **Status** – the current status of the task.
- **Start** – the date and time when Veeam Backup for Salesforce started a new task to process the object.
- **Finish** – the date and time when Veeam Backup for Salesforce completed the task.
- **Duration** – the duration of the task.
- **Message** – the explanation why Veeam Backup for Salesforce failed to process the records (applies only to sessions with the *Warning* and *Error* statuses).
- **API Usage** – the total number of API calls sent during the task.
- **Inserted** – the total number of new Salesforce records added to the backup scope during the task.
- **Updated** – the total number of Salesforce records updated in Salesforce during the task.

- **Downloaded** – the total number of Salesforce files added to the Veeam Backup for Salesforce file repository during the task.
- **Deleted** – the total number of records deleted from Salesforce during the task.
- **Failed** – the total number of Salesforce records that Veeam Backup for Salesforce failed to process.
- **Total** – the total number of Salesforce records processed during the task.

## TIP

If you want to view logs of a specific backup session, select the session and click **Download Logs**. Veeam Backup for Salesforce will collect the session logs and save them as a single .ZIP archive to the default download folder on the local machine.

The screenshot displays the Veeam Backup for Salesforce web interface. At the top, there are navigation tabs: Backup, Restore, Browse, and Archive. The current view is for a backup policy named 'backup-policy-1' (nd3 (USA6705)).

The main section is titled 'Backup Sessions'. It includes a filter dropdown set to 'All', a 'Show:' menu with icons for All, Success, Warning, Error, Paused, and Cancel, and action buttons for Stop, Restart, View Details, Download Logs, and Refresh.

Session ID	Type	Start ↓	Finish	Status	Message	API Usage	Inserted	Updated	Deleted ∞
12	Validate	6/15/24, 10:42:11 PM	6/15/24, 10:42:43 PM	Success	—	207	0	0	0
10	Data	6/15/24, 10:00:21 PM	6/15/24, 10:02:11 PM	Warning	—	75	0	1	1
11	File	6/15/24, 10:00:20 PM	6/15/24, 10:00:43 PM	Success	—	22	11	1	0
9	Metadata	6/15/24, 10:00:20 PM	6/15/24, 10:01:12 PM	Success	—	178	0	0	0

Below the sessions table is the 'Session Details' section. It has a search box for 'Object / Event' and a 'Show:' menu with the same icons as the sessions table. A 'View Details' link is highlighted with a mouse cursor.

Object / Event	Status	Start	Duration	Message	Inserted	Updated	Downloaded	Deleted ∞
UserRole	Success	6/15/24, 10:42:41 PM	00:00:01	—	0	0	—	0
xkffmkke_c	Success	6/15/24, 10:42:41 PM	00:00:00	—	0	0	—	0
zqqlhqzc_c	Success	6/15/24, 10:42:41 PM	00:00:00	—	0	0	—	0
WorkThanks	Success	6/15/24, 10:42:41 PM	00:00:00	—	0	0	—	0
WorkOrderLineItem	Success	6/15/24, 10:42:41 PM	00:00:00	—	0	0	—	0
WorkBadgeDefinition	Success	6/15/24, 10:42:41 PM	00:00:00	—	0	0	—	0
WorkOrder	Success	6/15/24, 10:42:41 PM	00:00:00	—	0	0	—	0
WorkBadge	Success	6/15/24, 10:42:41 PM	00:00:00	—	0	0	—	0



# Backup Job Types

When creating a backup policy, you configure the default backup schedule according to which Veeam Backup for Salesforce will back up the Salesforce organization. You can also enable custom schedules in the backup policy settings to additionally protect specific groups of objects. The configured schedules are further used by the product to create backup jobs of 5 different types:

- **Data job** – this job type is used to back up object data of the protected Salesforce organization. Data jobs run according to each configured backup schedule (both custom and default). To learn how to configure backup schedules, see [Creating Backup Policies](#).
- **Metadata job** – this job type is used to back up metadata of the protected Salesforce organization. Metadata jobs run according to default backup schedules only.
- **File job** – this job type is used to back up files and attachments of the protected Salesforce organization. File jobs run according to default backup schedules and only if you enable backup of files and attachments in backup policy settings. To learn how to enable this functionality, see [Creating Backup Policies](#).
- **Validate job** – this job type is used to compare backed-up data in the product database with data currently stored in Salesforce, that is, to detect hard-deleted items and mark them as deleted in the product database. Validate jobs automatically run weekly at the same time for each enabled backup policy. To learn how to enable backup policies, see [Disabling and Enabling Backup Policies](#).
- **Encryption job** – this job type is used to encrypt records and files of the protected Salesforce organization. Encryption jobs run according to the [configured encryption settings](#) – but only for those backup policies that have already been used to protect data and previously had the encryption functionality disabled.

If you disable encryption for a backup policy, the next run of the encryption job will decrypt data that has been previously encrypted. To learn how to enable and disable encryption, see [Creating Backup Policies](#).

## NOTES

- For each object specified while [configuring encryption settings](#), Veeam Backup for Salesforce runs a separate encryption job.
- If you enable encryption when creating a backup policy, or if you add new records and files to a policy that previously had the encryption functionality enabled, Veeam Backup for Salesforce will encrypt data by running data and file jobs instead of encryption jobs.

# Viewing Backed-Up Data

On the **Browse** tab, you can look through the backed-up data and check whether restore is needed. This tab is available for the *Administrator*, *Backup Operator* and *Restore Operator* user roles that have access to the Salesforce organization.

Keep in mind that search results are limited to 1,000 records. You can choose the displayed information and apply additional search conditions using specific filters. To do that:

1. Navigate to the **Browse** tab.
2. Select a Salesforce organization whose records you want to restore.
3. Select a Salesforce root object whose records you want to restore.

For a Salesforce object to be displayed in the list of available root objects, it must have a backup. If the list does not contain the necessary object, the object either does not have a backup or cannot be restored. The object may not have a backup for the following reasons:

- The object was excluded from the backup policy that protects the Salesforce organization to which this object belongs.
  - The Salesforce user whose permissions are used for backup operations does not have access to the object.
  - Backup of the object is not supported in the current product version. For more information, see [Appendix A. Unsupported Objects](#).
4. Choose one of the following search options:
    - **Latest** – allows you to search only through the latest record versions.
    - **Modified Date** – allows you to search through all record versions for the time period you specify.
  5. Click the **Customize** link to apply specific search conditions and reduce the number of search results. Veeam Backup for Salesforce provides a number of built-in conditional operators (such as *contains*, *equals*, *starts with*, *is null* and so on) that can be used to send requests to databases. Note that the time required to process a request depends on the operator you use – for example, processing a request with the *equals* operator will take less time than processing a request with the *contains* operator.

## TIPS

When adding conditions, consider the following:

- If you want to search for records with null field values, use the *is null* operator. Using the *equals* operator in this case is not supported.
- If you want to search for a list of records, you can use the *in* operator and specify the IDs of the necessary records using a comma-separated list.
- If you want to search for a record but you do not have any information on this record except for the fact that it is linked to a specific object, you can use the lookup relationship field to filter all records linked to this object. To do that, specify the ID of the necessary object in the **Value** field.

Note that the **Value** field is case sensitive for the following operators: *starts with*, *ends with*, *equals*, *in*.

By default, filters are combined by the AND logical operator. That is, a record is displayed in the search results only if all the specified conditions are met. You can change this behavior by combining filters using different operators. To do that, set the **Use filter logic** toggle to *On*, and specify the filter logic expression using condition ordinal numbers, brackets and logical operators – for example, *1 AND (2 OR 3) AND NOT 4*.

## IMPORTANT

If an object record that you want to restore contains encrypted fields, you will not be able to specify filters for these fields.

You can also specify what Salesforce fields you want to be displayed for the found records. To do that, navigate to the **Display Fields** tab and add the necessary fields.

6. Click **Search**. If you apply any filtering conditions, the search results will be displayed on the same pages where the records were originally shown. To make sure that you have seen all the results, look through all the pages.

Note that only users assigned the *Administrator* and *Backup Operator* roles can view values of the encrypted fields.

7. Select records that you want to restore. You can also choose the version of a record that will be restored. To do that, click the link in the **Version** column, compare the latest version of the backed-up record both with previous backed-up record versions and with the version of the record currently stored in the Salesforce database, and select the necessary version from the **Restore** point drop-down list. If you want Veeam Backup for Salesforce to show only field values that differ between the selected versions, set the **Compare changes toggle** to On.

The screenshot shows the Veeam Backup for Salesforce interface with the 'Select Version To Restore' dialog box open. The dialog box has a title bar with a close button (X) and a subtitle: 'Compare record versions between backups and live data. Select the version you want to restore.' Below the subtitle, there is a 'Restore point:' dropdown menu showing '8/1/24, 5:01:55 PM'. To the right of the dropdown are navigation buttons: '← Previous', 'Next →', and 'Latest →'. Below the dropdown is a 'Filter by text' input field. To the right of the input field is a 'Compare changes:' toggle switch, which is currently set to 'Off'. Below the input field and toggle is a table with three columns: 'Field', 'Restore Point', and 'Production Data'. The 'Restore Point' column is highlighted in yellow. The table contains the following data:

Field	Restore Point	Production Data
Account Number AccountNumber	8/1/24, 5:01:55 PM null	8/16/24, 3:27:22 PM null
Account Source AccountSource	8/1/24, 5:01:55 PM null	8/16/24, 3:27:22 PM null
Annual Revenue AnnualRevenue	8/1/24, 5:01:55 PM 123,123	8/16/24, 3:27:22 PM 123,123
Billing City BillingCity	8/1/24, 5:01:55 PM Berlin	8/16/24, 3:27:22 PM Berlin
Billing Country BillingCountry	8/1/24, 5:01:55 PM Germany	8/16/24, 3:27:22 PM Germany
Billing Geocode Accuracy BillingGeocodeAccuracy	8/1/24, 5:01:55 PM null	8/16/24, 3:27:22 PM null
Billing Latitude BillingLatitude	8/1/24, 5:01:55 PM null	8/16/24, 3:27:22 PM null
Billing Longitude BillingLongitude	8/1/24, 5:01:55 PM null	8/16/24, 3:27:22 PM null
Billing Zip/Postal Code BillingPostalCode	8/1/24, 5:01:55 PM 10000	8/16/24, 3:27:22 PM 10000

At the bottom of the dialog box are two buttons: 'Apply' and 'Cancel'.

# Performing Salesforce Restore

To recover backed-up data, Veeam Backup for Salesforce runs restore jobs. When you create a restore job, it is created as a draft that you can further edit, remove, start and clone. Once the restore job is started, it can be only stopped or cloned.

## NOTE

Only users assigned the *Administrator*, *Backup Operator* or *Restore Operator* role can perform restore operations in Veeam Backup for Salesforce. However, users assigned the *Backup Operator* or *Restore Operator* role can create and run restore jobs within their permission scope only – that is, for companies and organizations whose data they can access.

## In This Section

- [Creating Restore Jobs](#)
- [Starting and Stopping Restore Jobs](#)
- [Cloning Restore Jobs](#)
- [Editing Restore Jobs](#)
- [Removing Restore Job Drafts](#)
- [Configuring Restore Mapping Settings](#)
- [Viewing Restore Job Details](#)

# Creating Restore Jobs

You can create drafts of restore jobs that you want Veeam Backup for Salesforce to perform. After you create a draft, you can start the job right after you finish the restore job configuration wizard or later as described in section [Starting and Stopping Restore Jobs](#).

## NOTE

Restore job drafts older than 7 days are automatically removed by Veeam Backup for Salesforce.

Veeam Backup for Salesforce offers the following restore options:

- [Restore records](#)
- [Restore field values](#)
- [Restore files](#)
- [Restore metadata](#)

# Restoring Records

Record restore jobs allow you to restore earlier versions of modified or corrupted records and linked objects.

To create a record restore job, perform the following steps:

1. [Launch the Restore Records wizard.](#)
2. [Specify a name and description for the restore job.](#)
3. [Select Salesforce organizations.](#)
4. [Choose the data that will be restored.](#)
5. [Choose what attachments associated with the specified records will be restored.](#)
6. [Enable restore of object hierarchy.](#)
7. [Configure additional restore settings.](#)
8. [Check permissions.](#)
9. [Finish working with the wizard.](#)

# Step 1. Launch Restore Records Wizard

To launch the **Restore Records** wizard:

1. Navigate to the **Restore** tab.
2. If you have added multiple companies to Veeam Backup for Salesforce, select a company to which the Salesforce organization whose data you want to restore belongs. To do that, select the company from the drop-down list at the top of the page.

For a company to be displayed in the list of available companies, it must be added to Veeam Backup for Salesforce as described in section [Adding Companies](#). Also, the user launching the **Restore Records** wizard must be granted permissions to access the company as described in section [User Roles and Permissions](#).

3. Click **New Restore > Records**.

The screenshot shows the Veeam Backup for Salesforce interface. The top navigation bar includes 'Backup', 'Restore', 'Browse', and 'Archive'. The 'Restore' tab is active. The interface displays a table of restore jobs with columns for 'Type', 'Status', 'Created Date', 'Start Date', 'Finish Date', 'Created By', 'Modified By', and 'Started By'. A dropdown menu is open under 'New Restore', with 'Records' selected. The table contains several rows of jobs, including 'restore-job-159058' through 'restore-job-126917', with various statuses like 'Draft', 'Stopped', and 'Failed'.

Type	Status	Created Date	Start Date	Finish Date	Created By	Modified By	Started By
Records	Draft	5/18/23, 9:46:23 ...	—	—	admin	admin	—
Metadata	Draft	5/18/23, 9:35:51 ...	—	—	admin	admin	—
Metadata	Draft	5/18/23, 8:29:52 ...	—	—	admin	admin	—
Records	Draft	5/18/23, 4:42:02 ...	—	—	admin	admin	—
Records	Draft	5/18/23, 3:18:14 ...	—	—	admin	admin	—
Records	Draft	5/17/23, 2:01:18 ...	—	—	admin	admin	—
Fields	Draft	5/17/23, 1:47:43 ...	—	—	admin	admin	—
Files	Draft	5/17/23, 12:29:58...	—	—	admin	admin	—
Fields	Stopped	5/16/23, 11:42:19...	5/16/23, 1:54:35 ...	5/16/23, 1:54:42 ...	admin	admin	admin
Records	Draft	5/15/23, 11:34:20...	—	—	admin	admin	—
Records	Draft	5/15/23, 9:55:06 ...	—	—	admin	admin	—
Fields	Failed	5/12/23, 7:35:18 ...	5/12/23, 7:35:32 ...	5/12/23, 7:35:59 ...	admin	admin	admin

## Step 2. Specify Restore Job Info

At the **Name** step of the wizard, use the **Job name** and **Job details or reason for restore** fields to specify a name for the new restore job and to provide a description for future reference. The maximum length of the job name is 100 characters.

The screenshot shows the 'Restore Job Name' step in the Veeam Backup for Salesforce wizard. The interface includes a top navigation bar with tabs for Backup, Restore, Browse, and Archive. The 'Restore' tab is active. The breadcrumb trail shows 'Restore Records' with the ID 'restore-job-159061'. A left-hand sidebar lists the wizard steps: Name, Organization, Data, Files, Hierarchy, Options, Verification, and Summary. The 'Name' step is currently selected. The main content area is titled 'Restore Job Name' and contains the following text: 'This information will be included in the audit log of the restore. It may be helpful to reference the incoming ticket or work item.' Below this text are two input fields: 'Job name:' with the value 'restore-job-159061' and 'Job details or reason for restore:' with the value 'restoring org records'. At the bottom of the form, there are two buttons: 'Next' and 'Cancel'.



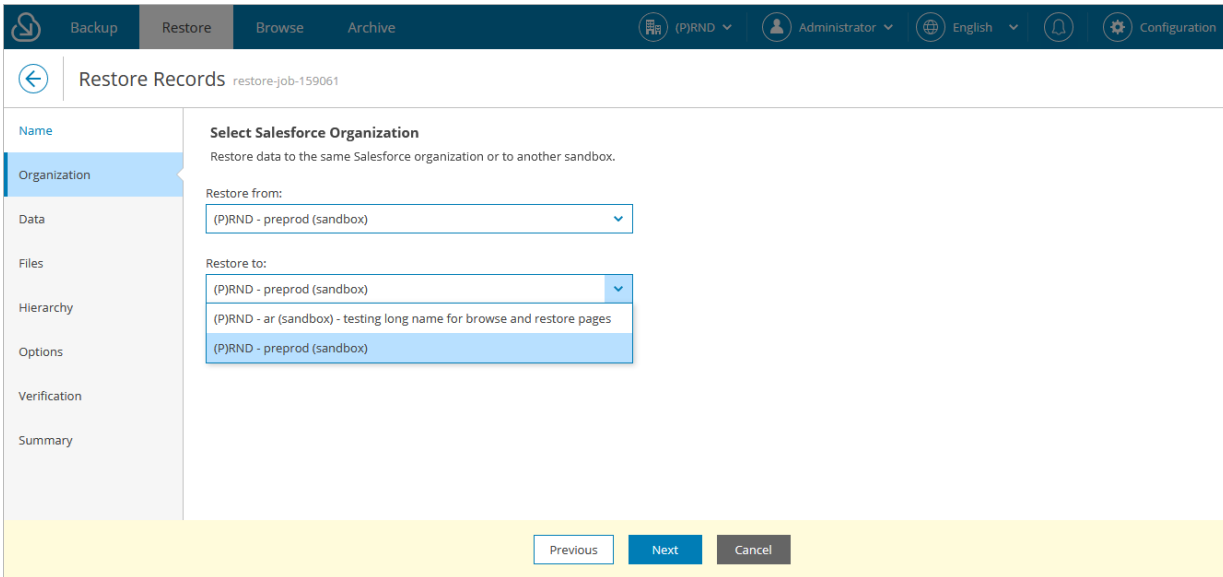
# Step 3. Select Organization

At the **Organization** step of the wizard, use the **Restore from** drop-down list to select a Salesforce organization whose records you want to restore. For a Salesforce organization to be displayed in the list of available organizations, it must belong to the company specified at [step 1](#) of the wizard.

By default, the records are restored to the same Salesforce organization. However, you can choose to restore records to another organization (for example, if you want to seed a sandbox organization with backed-up data of another organization) – to do that, use the **Restore to** drop-down list. For a Salesforce organization to be displayed in the list of available organizations, it must belong to the company specified at [step 1](#) and be compatible with the organization whose records you want to restore. This means that you can restore from a production or sandbox organization only to its sandbox copies.

### IMPORTANT

- When you restore an object record to another organization, make sure that metadata of the object that you want to restore match metadata of the object in the target organization. If metadata is missing or does not match, you must first create a dedicated [metadata restore job](#).
- When you restore an object record that contains encrypted fields to the same production organization, Veeam Backup for Salesforce decrypts and restores the fields. However, if you restore this record to a sandbox organization, the product does not restore the encrypted fields – unless you provide [override values for these fields](#).



## Step 4. Choose Data to Restore

At the **Data** step of the wizard, do the following:

1. Select a Salesforce root object whose records you want to restore.

For a Salesforce object to be displayed in the list of available root objects, it must have a backup. If the list does not contain the necessary object, the object either does not have a backup or cannot be restored. The object may not have a backup for the following reasons:

- The object was excluded from the backup policy that protects the Salesforce organization to which this object belongs.
  - The Salesforce user whose permissions are used for backup operations does not have access to the object.
  - Backup of the object is not supported in the current product version. For more information, see [Appendix A. Unsupported Objects](#).
2. Choose one of the following search options:
    - **Latest** – allows you to search only through the latest record versions.
    - **Backup Date** – allows you to search search only through the latest record versions before the time period you specify.
    - **Modified Date** – allows you to search through all record versions for the time period you specify.
  3. Click the **Customize** link to apply specific search conditions and reduce the number of search results. Veeam Backup for Salesforce provides a number of built-in conditional operators (such as *contains*, *equals*, *starts with*, *is null* and so on) that can be used to send requests to databases. Note that the time required to process a request depends on the operator you use – for example, processing a request with the *equals* operator will take less time than processing a request with the *contains* operator.

### TIPS

When adding conditions, consider the following:

- If you want to search for records with null field values, use the *is null* operator. Using the *equals* operator in this case is not supported.
- If you want to search for a list of records, you can use the *in* operator and specify the IDs of the necessary records using a comma-separated list.
- If you want to search for a record but you do not have any information on this record except for the fact that it is linked to a specific object, you can use the lookup relationship field to filter all records linked to this object. To do that, specify the ID of the necessary object in the **Value** field.

Note that the **Value** field is case sensitive for the following operators: *starts with*, *ends with*, *equals*, *in*.

By default, filters are combined by the AND logical operator. That is, a record is displayed in the search results only if all the specified conditions are met. You can change this behavior by combining filters using different operators. To do that, set the **Use filter logic** toggle to *On*, and specify the filter logic expression using condition ordinal numbers, brackets and logical operators – for example, *1 AND (2 OR 3) AND NOT 4*.

### IMPORTANT

If an object record that you want to restore contains encrypted fields, you will not be able to specify filters for these fields.

You can also specify what Salesforce fields you want to be displayed for the found records. To do that, navigate to the **Display Fields** tab and add the necessary fields.

3. Click **Search**. If you apply any filtering conditions, the search results will be displayed on the same pages where the records were originally shown. To make sure that you have seen all the results, look through all the pages.
4. Select records that you want to restore.

You can also choose the version of a record that will be restored. To do that, click the link in the **Version** column, compare the latest version of the backed-up record both with previous backed-up record versions and with the version of the record currently stored in the Salesforce database, and select the necessary version from the **Restore point** drop-down list. If you want Veeam Backup for Salesforce to show only field values that differ between the selected versions, set the **Compare changes** toggle to *On*.

## NOTE

Only users assigned the *Administrator* and *Backup Operator* roles can view and compare values of the encrypted fields.

The screenshot shows the 'Restore Records' interface with the 'Select Version To Restore' dialog open. The dialog title is 'Select Version To Restore' and it contains the instruction: 'Compare record versions between backups and live data. Select the version you want to restore.' The 'Restore point' dropdown menu is open, showing three options: '8/1/24, 5:01:55 PM' (selected), '8/1/24, 5:01:55 PM', and '7/31/24, 5:10:43 PM'. The 'Compare changes' toggle is currently set to 'Off'. Below the dropdown is a table comparing the selected restore point with the production data.

Field	Restore Point 8/1/24, 5:01:55 PM	Production Data 8/16/24, 3:25:38 PM
Account Number AccountNumber	null	null
Account Source AccountSource	null	null
Annual Revenue AnnualRevenue	123,123	123,123
Billing City BillingCity	Berlin	Berlin
Billing Country BillingCountry	Germany	Germany
Billing Geocode Accuracy BillingGeocodeAccuracy	null	null
Billing Latitude BillingLatitude	null	null
Billing Longitude BillingLongitude	null	null
Billing Zip/Postal Code BillingPostalCode	10000	10000

At the bottom of the dialog, there are 'Apply' and 'Cancel' buttons.

## Step 5. Choose Attachments to Restore

At the **Files** step of the wizard, you can instruct Veeam Backup for Salesforce to restore files associated with the records selected at [step 4](#). To do that, set the **Restore attachments** toggle to *On* and apply filters to choose files that you want to restore. If you do not specify any filtering conditions, Veeam Backup for Salesforce will restore all files associated with the selected record.

Veeam Backup for Salesforce provides a number of built-in conditional operators (such as *contains*, *equals*, *starts with*, *is null* and so on) that can be used to send requests to databases. Note that the time required to process a request depends on the operator you use – for example, processing a request with the *equals* operator will take less time than processing a request with the *contains* operator.

For a file to be displayed in the list of available files, it must be associated with the selected record and have a backup.

### IMPORTANT

If you choose to restore an encrypted file to a production organization, Veeam Backup for Salesforce will decrypt the file and fully restore its content. However, if you choose to restore an encrypted file to a sandbox organization, Veeam Backup for Salesforce will create only an empty copy of this file.

The screenshot displays the 'Restore Records' wizard for job 'restore-job-271403'. The 'Files' step is selected in the sidebar. The 'Restore Attachments' section is active, showing a toggle set to 'On'. A filter rule is applied: 'Id (File ID) starts with 0688'. The '1 file will be restored' section shows a table with the following data:

File ID	Is Deleted	File Extension	Created
0688d0000Th...	False	png	3/26/24, 9:17:58

Navigation buttons at the bottom include 'Previous', 'Next', and 'Cancel'.

## Step 6. Enable Hierarchy Restore

At the **Hierarchy** step of the wizard, Veeam Backup for Salesforce allows you to restore parent and child records linked to the records selected at [step 4](#). While restoring hierarchy, the product analyzes all lookup relationship fields of the records and compares backed-up data with the current Salesforce data. For more information, see [How Veeam Backup for Salesforce Restores Object Hierarchy](#).

### IMPORTANT

If you have enabled restore of files and attachments at [step 5](#), keep in mind that the product will not restore files and attachments of child and parent records. To restore them, create a dedicated [file restore job](#).

To restore lookup relationships, set the **Restore records hierarchy** toggle to *On* and do the following:

1. In the **Parent hierarchy** section, select the maximum level of the parent object hierarchy that will be restored for all records. By default, Veeam Backup for Salesforce restores the 1st level parent records only.

The restore parent hierarchy settings are applied to every record in the session and not only to the records selected at [step 4](#). It means that Veeam Backup for Salesforce will restore the record and then will verify lookup links to its parent records. This process will repeat for all the selected child records.

2. In the **Child hierarchy** section, configure the following settings:
  - a. In the **Child hierarchy levels** field, select the minimum level of the child object hierarchy that will be restored for all records.
  - b. Click the link in the **Exclude objects** field to choose whether you want to exclude specific child objects from restore. Note that Veeam Backup for Salesforce will also exclude all child objects associated with the objects that you specified.
  - c. Click the link in the **Customize records** field to customize child hierarchy settings for individual records. To configure settings for a record, click **Customize** and select check boxes next to the objects whose records you want to restore in the **Customize Hierarchy Restore** window.
3. In the **Hierarchy data consistency** section, configure the following settings:
  - a. From the **Validation rule** drop-down list, choose when to stop updating the child records:
    - To stop proceeding to deeper levels of the hierarchy if a child record exists in Salesforce, select *Record exists in Salesforce*. This child record will be the last updated record. Keep in mind that it will be updated according to the selected **Records restore rule** option.
    - To stop proceeding to deeper levels of the hierarchy if a child record exists in Salesforce and the lookup field value matches the backed-up value, select *Record exists in Salesforce and parent lookup matches backup data*. This child record will be the last updated record. Keep in mind that it will be updated according to the selected **Records restore rule** option.
    - To stop proceeding to deeper levels of the hierarchy if a child record exists in Salesforce and the values of all fields of the record match the backed-up values, select *Record exists in Salesforce and all fields match backup data*.
    - To proceed with hierarchy restore until the specified child hierarchy restore level is reached and all the child records with the configured custom hierarchy settings are updated, select *Always check entire hierarchy tree*.
  - b. From the **Records restore rule** drop-down list, choose what fields will be updated for existing child records:

- Not to update fields of the existing child records, select *Restore deleted records. Do not update existing records.*
- To update only the parent lookup fields of the existing child records, select *Update lookup relationships and restore deleted records.*
- To update fields of the existing child records and replace empty field values with null, select *Update all filed values, including empty values, and restore deleted records.*
- To update all fields of the existing child records without replacing empty field values with null, select *Update all field values, ignoring empty values, and restore deleted records.*

## NOTE

The product restores child and parent records of the versions that you selected at [step 4](#).

The screenshot shows the 'Restore Records' configuration interface for a restore job named 'restore-job-1'. The 'Hierarchy' tab is active in the left-hand navigation pane. The main configuration area is titled 'Restore Records Hierarchy' and includes the following settings:

- Restore records hierarchy:** A toggle switch is turned 'On'.
- Parent hierarchy:** A section for updating or restoring records on higher levels of the hierarchy.
  - Parent hierarchy levels:** A dropdown menu is set to '1'.
- Child hierarchy:** A section for updating or restoring records on lower levels of the hierarchy.
  - Child hierarchy levels:** A dropdown menu is set to '2'.
  - Exclude objects:** '1 object excluded'.
  - Customize records:** 'No records customized'.
- Hierarchy data consistency:** A section for resolving discrepancies.
  - Validation rule:** 'Record exists in Salesforce and parent lookup matches backup data'.
  - Records restore rule:** 'Update lookup relationships and restore deleted records'.

At the bottom of the configuration area, there are three buttons: 'Previous', 'Next' (which is highlighted with a mouse cursor), and 'Cancel'.

## Step 7. Configure Additional Restore Settings

At the **Options** step of the wizard, you can instruct Veeam Backup for Salesforce to automatically replace empty field values with *null*, overwrite field values manually, map fields of backed-up records to specific fields in Salesforce, and choose how you want to deactivate blocking automation in Salesforce.

### Automatic Field Overriding Settings

In the **Data consistency** section, you can choose whether you want Veeam Backup for Salesforce to update all existing records and overwrite field values, or restore only those records that have been deleted from Salesforce without updating the existing records. If you select the **Restore records and field values** option, you can also decide whether you want to replace non-empty field values of the existing object records in Salesforce with empty (*null*) values of the backed-up records.

### Manual Field Overriding Settings

In the **Field customization options** section, you can choose whether you want to override specific field values in the restored records (for example, in case of sandbox seeding when you need to mask sensitive data). To do that, click the link in the **Override field values** field, choose a field whose value you want to override and provide a new value.

For a record field to be displayed in the list of available fields, this record must be added to the restore job as described at [step 4](#) of the wizard. Keep in mind that if you restore an object record that contains encrypted fields to the same organization, these fields will be grayed out.

#### TIPS

- When overriding time values, keep in mind that even though the management server and databases use the UTC time zone for all operations, Salesforce adjusts the time set for every Salesforce user according to the time zone settings defined for this user. To learn how to change default time zones in Salesforce, see [Salesforce Documentation](#).
- When entering field values, you can add comments to these values in the following format: *<comment> {value}*. For example, if the backed-up values of the **Name** field are *Account1*, *Account2* and *Account3*, and you specify the *New {value}* comment, the restored values of the field will be *New Account1*, *New Account2* and *New Account3*.

### Field Mapping Settings

In the **Field customization options** section, you can also choose whether you want Veeam Backup for Salesforce to populate fields of the record in Salesforce with values of a specific record from the backup. To do that, click the link in the **Map old fields to new fields** field, choose a field from the backup whose values you want to use and a Salesforce field that you want to be updated. For a field to be displayed in the list of available fields, it must have a backup.

#### IMPORTANT

Mapping of encrypted fields is not supported.

# Blocking Automation Settings

Business logic and automated rules configured in Salesforce can block Veeam Backup for Salesforce restore operations or trigger undesirable side processes. You can choose either to manually deactivate Flows, Validation Rules and Apex Triggers in Salesforce or to instruct the product to bypass all blocking automation while performing a restore operation. To do that, select one of the options in the Turn off automation section:

- Select the **I will manually turn off all blocking automation** option, if you are a Salesforce Administrator and want to deactivate Flows, Validation Rules and Apex Triggers in Salesforce manually.
- Select the **Automatically turn off all automation** option to automatically update Flows, Validation Rules and Apex Triggers so that they are bypassed while the product performs the restore operation without impacting the Salesforce functionality. When you choose this option for a restore job for the first time, updating Flows, Validation Rules and Apex Triggers will take significant time to complete. However, as the updates will be kept in Salesforce, all further restore operations will run faster.
- Select the **Temporarily turn off all automation** option to automatically update Flows, Validation Rules and Apex Triggers so that they are bypassed while the product performs the current restore operation only without impacting the Salesforce functionality. All changes made by the product will be reverted after the restore operation is over. Note that updating Flows, Validation Rules and Apex Triggers and reverting the changes may take significant time to complete.

The screenshot shows the 'Restore Records' configuration page for a restore job (ID: restore-job-271404). The 'Options' tab is active in the left sidebar. The main content area is titled 'Additional Restore Options' and includes the following sections:

- Data consistency:** Existing records in Salesforce may differ from backup. Choose how resolve such discrepancies. Records restore rule: Restore records and field values.
- Field customization options:** Override field values: 1 field will be overridden. Map old fields to new fields: Not specified...
- Turn off automation (workflows, flows, apex triggers and validation rules):** Three radio button options are present:
  - I will manually turn off all blocking automation
  - Automatically turn off all automation
  - Temporarily turn off all automation

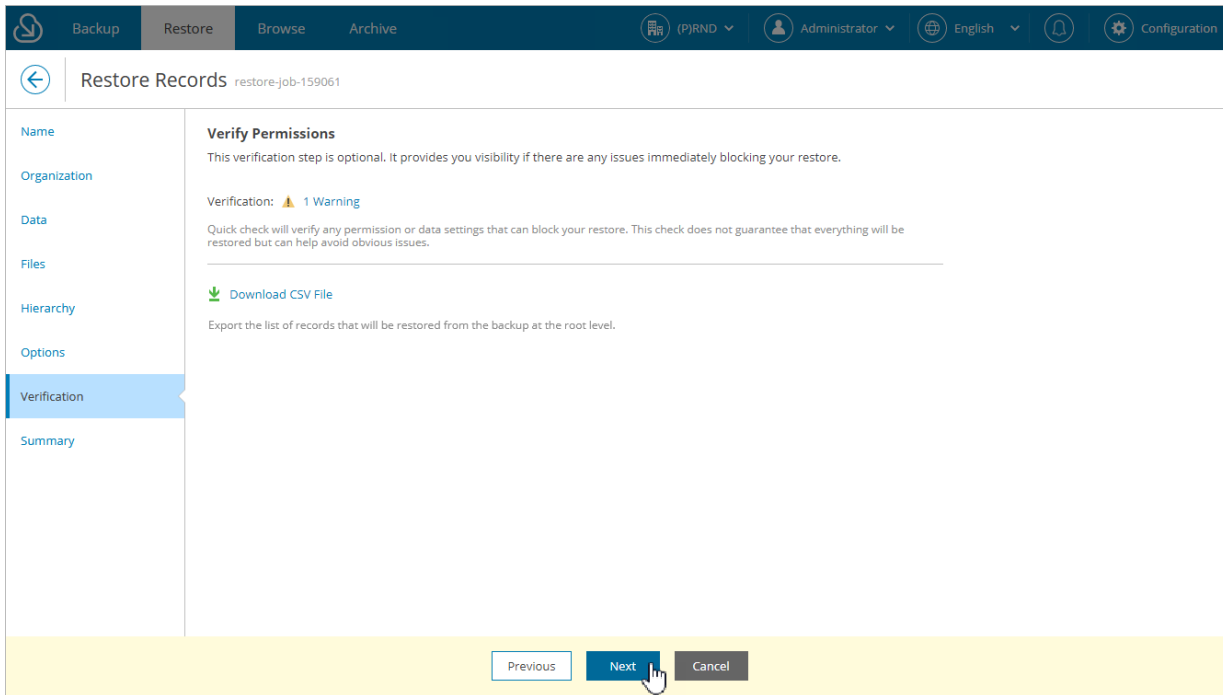
At the bottom of the page, there are three buttons: 'Previous', 'Next', and 'Cancel'. The 'Next' button is highlighted with a mouse cursor.



## Step 8. Check Permissions

At the **Verification** step of the wizard, verify whether the user that is used to perform the restore operation is assigned the permissions required to restore the selected Salesforce object. To do that, click the **Not verified yet** link and wait for the check to complete. If any of the permissions are missing, you must grant them in the Salesforce console manually as described in [Salesforce documentation](#).

To export the list that contains all records selected at [step 4](#) as a single .CSV file, click **Download CSV File**. Veeam Backup for Salesforce will save the file with the exported data to the default download folder on the local machine.



# Step 9. Finish Working with Wizard

At the **Summary** step of the wizard, review configured settings and click **Finish**.

If you want Veeam Backup for Salesforce to start restore automatically after you complete the wizard, select the **Start the job after clicking the Finish button** check box. Otherwise, the job draft will be created, and you will have to manually run the job as described in section [Starting and Stopping Restore Jobs](#).

## TIP

To view all objects added to the restore session, click the link in the **Object** field.

The screenshot shows the 'Restore Records' wizard in the 'Summary' step. The interface includes a top navigation bar with 'Backup', 'Restore', 'Browse', and 'Archive' tabs. The 'Restore' tab is active, and the user is logged in as 'Administrator'. The main content area is divided into a left sidebar with navigation links (Name, Organization, Data, Files, Hierarchy, Options, Verification, Summary) and a main panel. The 'Summary' step is highlighted in the sidebar. The main panel displays the following settings:

- Hierarchy**
  - Parent hierarchy levels: 2
  - Child hierarchy levels: 2
  - Excluded objects: 1
  - Customized records: —
  - Records restore rule: Update lookup relationships and restore deleted records
  - Finish restore when: Record exists in Salesforce and parent lookup matches backup data
- Mapping**

Fields mapping:	Backup field	Salesforce field
	Sic	AccountNumber

Fields override: —
- Options**
  - Overwrite records: Yes
  - Restore empty values: No
  - Disable automation: No
  - Roll-back disable automation: No

An information message states: "Permanently deleted objects are restored with different IDs. Auto-number fields will get next sequential value." Below this, there is a checkbox labeled "Start the job after clicking the Finish button" which is currently unchecked. At the bottom of the wizard, there are three buttons: "Previous", "Finish" (highlighted with a mouse cursor), and "Cancel".

# Restoring Field Values

Field value restore jobs allow you to recover earlier versions of changed or deleted field values.

## IMPORTANT

Using this type of restore, you can restore field values only. If you want to restore the field itself, you must perform the [metadata restore](#) first.

To create a field value restore job, perform the following steps:

1. [Launch the Restore Field Values wizard.](#)
2. [Specify a name and description for the restore job.](#)
3. [Select Salesforce organizations.](#)
4. [Select records whose field values you want to restore.](#)
5. [Select fields whose values will be restored.](#)
6. [Configure additional restore settings.](#)
7. [Check permissions.](#)
8. [Finish working with the wizard.](#)

# Step 1. Launch Restore Field Values Wizard

To launch the **Restore Field Values** wizard:

1. Navigate to the **Restore** tab.
2. If you have added multiple companies to Veeam Backup for Salesforce, select a company to which the Salesforce organization whose data you want to restore belongs. To do that, select the company from the drop-down list at the top of the page.

For a company to be displayed in the list of available companies, it must be added to Veeam Backup for Salesforce as described in section [Adding Companies](#). Also, the user launching the **Restore Field Values** wizard must be granted permissions to access the company as described in section [User Roles and Permissions](#).

3. Click **New Restore > Fields**.

The screenshot shows the Veeam Backup for Salesforce interface. The top navigation bar includes 'Backup', 'Restore', 'Browse', and 'Archive'. The 'Restore' tab is active. The interface displays a table of restore jobs with columns for Type, Status, Created Date, Start Date, Finish Date, Created By, Modified By, and Started By. A dropdown menu is open under 'New Restore', showing options for 'Records', 'Fields', 'Files', and 'Metadata'. The 'Fields' option is highlighted. The table below shows various restore jobs, including one that is 'Failed'.

Type	Status	Created Date	Start Date	Finish Date	Created By	Modified By	Started By
Records	Draft	5/18/23, 9:46:23 ...	—	—	admin	admin	—
Metadata	Draft	5/18/23, 9:35:51 ...	—	—	admin	admin	—
Metadata	Draft	5/18/23, 8:29:52 ...	—	—	admin	admin	—
Records	Draft	5/18/23, 4:42:02 ...	—	—	admin	admin	—
Records	Draft	5/18/23, 3:18:14 ...	—	—	admin	admin	—
Records	Draft	5/17/23, 2:01:18 ...	—	—	admin	admin	—
Fields	Draft	5/17/23, 1:47:43 ...	—	—	admin	admin	—
Files	Draft	5/17/23, 12:29:58...	—	—	admin	admin	—
Fields	Stopped	5/16/23, 11:42:19...	5/16/23, 1:54:35 ...	5/16/23, 1:54:42 ...	admin	admin	admin
Records	Draft	5/15/23, 11:34:20...	—	—	admin	admin	—
Records	Draft	5/15/23, 9:55:06 ...	—	—	admin	admin	—
Fields	Failed	5/12/23, 7:35:18 ...	5/12/23, 7:35:32 ...	5/12/23, 7:35:59 ...	admin	admin	admin

## Step 2. Specify Restore Job Info

At the **Name** step of the wizard, use the **Job name** and **Job details or reason for restore** fields to specify a name for the new restore job and to provide a description for future reference. The maximum length of the job name is 100 characters.

The screenshot shows the 'Restore Field Values' wizard in the 'Name' step. The breadcrumb trail is 'Backup > Restore > Browse > Archive'. The user is logged in as 'Administrator' and the language is 'English'. The wizard title is 'Restore Field Values restore-job-2'. On the left, a sidebar lists the steps: Name (selected), Organization, Data, Fields, Options, Verification, and Summary. The main content area is titled 'Restore Job Name' and includes the following text: 'This information will be included in the audit log of the restore. It may be helpful to reference the incoming ticket or work item.' Below this, there are two text input fields. The first is labeled 'Job name:' and contains the text 'Restore Fields'. The second is labeled 'Job details or reason for restore:' and contains the text 'Restoring field values 01'. At the bottom of the wizard, there are two buttons: 'Next' (highlighted in blue) and 'Cancel'.

## Step 3. Select Organization

At the **Organization** step of the wizard, use the **Restore from** drop-down list to select a Salesforce organization whose field values you want to restore. For a Salesforce organization to be displayed in the list, it must belong to the company specified at [step 1](#).

By default, the field values are restored to the same Salesforce organization. However, you can choose to restore field values to another organization – to do that, use the **Restore to** drop-down list. For a Salesforce organization to be displayed in the list of available organizations, it must belong to the company specified at [step 1](#) and be compatible with the organization whose field values you want to restore. This means that you can restore from a production or sandbox organization only to its sandbox copies.

### IMPORTANT

When you restore an object record that contains encrypted fields to the same production organization, Veeam Backup for Salesforce decrypts and restores the fields. However, if you restore this record to a sandbox organization, the product does not restore the encrypted fields – unless you provide [override values for these fields](#).

The screenshot shows the 'Restore Field Values' wizard in the Veeam Backup for Salesforce interface. The top navigation bar includes 'Backup', 'Restore', 'Browse', and 'Archive'. The current step is 'Restore Field Values', with a sub-tab 'Restore Fields'. The interface is divided into a left sidebar and a main content area. The sidebar contains a list of steps: Name, Organization (highlighted), Data, Fields, Options, Verification, and Summary. The main content area is titled 'Select Salesforce Organizations' and contains the instruction: 'Restore data to the same Salesforce organization or to another sandbox.' Below this, there are two dropdown menus: 'Restore from:' and 'Restore to:'. Both dropdown menus currently show 'Veeam RND1 - nd3 (sandbox)'. At the bottom of the wizard, there are three buttons: 'Previous', 'Next' (which is highlighted and has a mouse cursor over it), and 'Cancel'.

## Step 4. Choose Data to Restore

At the **Data** step of the wizard, do the following:

1. Select a Salesforce root object whose record fields you want to restore.

For a Salesforce object to be displayed in the list of available root objects, it must have a backup. If the list does not contain the necessary object, the object either does not have a backup or cannot be restored. The object may not have a backup for the following reasons:

- The object was excluded from the backup policy that protects the Salesforce organization to which this object belongs.
  - The Salesforce user whose permissions are used for backup operations does not have access to the object.
  - Backup of the object is not supported in the current product version. For more information, see [Appendix A. Unsupported Objects](#).
2. Choose one of the following search options:
    - **Latest** – allows you to search only through the latest record versions.
    - **Backup Date** – allows you to search search only through the latest record versions before the time period you specify.
    - **Modified Date** – allows you to search through all record versions for the time period you specify.
  3. Click the **Customize** link to apply specific search conditions and reduce the number of search results. Veeam Backup for Salesforce provides a number of built-in conditional operators (such as *contains*, *equals*, *starts with*, *is null* and so on) that can be used to send requests to databases. Note that the time required to process a request depends on the operator you use – for example, processing a request with the *equals* operator will take less time than processing a request with the *contains* operator.

### TIPS

When adding conditions, consider the following:

- Veeam Backup for Salesforce automatically adds a condition that filters the records to show only existing Salesforce fields. If you want to restore value of a field that was removed from Salesforce, you must perform the [metadata restore](#) first.
- If you want to search for records with null field values, use the *is null* operator. Using the *equals* operator in this case is not supported.
- If you want to search for a list of records, you can use the *in* operator and specify the IDs of the necessary records using a comma-separated list.
- If you want to search for a record but you do not have any information on this record except for the fact that it is linked to a specific object, you can use the lookup relationship field to filter all records linked to this object. To do that, specify the ID of the necessary object in the **Value** field.

Note that the **Value** field is case sensitive for the following operators: *starts with*, *ends with*, *equals*, *in*.

By default, filters are combined by the AND logical operator. That is, a record is displayed in the search results only if all the specified conditions are met. You can change this behavior by combining filters using different operators. To do that, set the **Use filter logic** toggle to *On*, and specify the filter logic expression using condition ordinal numbers, brackets and logical operators – for example, *1 AND (2 OR 3) AND NOT 4*.

## IMPORTANT

If an object record that you want to restore contains encrypted fields, you will not be able to specify filters for these fields.

You can also specify what Salesforce fields you want to be displayed for the found records. To do that, navigate to the **Display Fields** tab and add the necessary fields.

3. Click **Search**. If you apply any filtering conditions, the search results will be displayed on the same pages where the records were originally shown. To make sure that you have seen all the results, look through all the pages.
4. Select records that you want to restore. By default, you can select up to 500,000 of records for one field value restore session. To change this limit, modify the `fields.restore.max.input.records` parameter value as described in section [Configuring Advanced Settings](#).

You can also choose the version of a record that will be restored. To do that, click the link in the **Version** column, compare the latest version of the backed-up record both with previous backed-up record versions and with the version of the record currently stored in the Salesforce database, and select the necessary version from the **Restore point** drop-down list. If you want Veeam Backup for Salesforce to show only field values that differ between the selected versions, set the **Compare changes** toggle to *On*.

## NOTE

Only users assigned the *Administrator* and *Backup Operator* roles can view and compare values of the encrypted fields.

**Select Version To Restore**

Compare record versions between backups and live data. Select the version you want to restore.

Restore point: **8/1/24, 5:01:55 PM** | Previous | Next | Latest

Filter by text:  | Compare changes:  Off

Field	Restore Point	Production Data
Account Number AccountNumber	8/1/24, 5:01:55 PM null	8/16/24, 3:27:22 PM null
Account Source AccountSource	null	null
Annual Revenue AnnualRevenue	123,123	123,123
Billing City BillingCity	Berlin	Berlin
Billing Country BillingCountry	Germany	Germany
Billing Geocode Accuracy BillingGeocodeAccuracy	null	null
Billing Latitude BillingLatitude	null	null
Billing Longitude BillingLongitude	null	null
Billing Zip/Postal Code BillingPostalCode	10000	10000

Apply Cancel

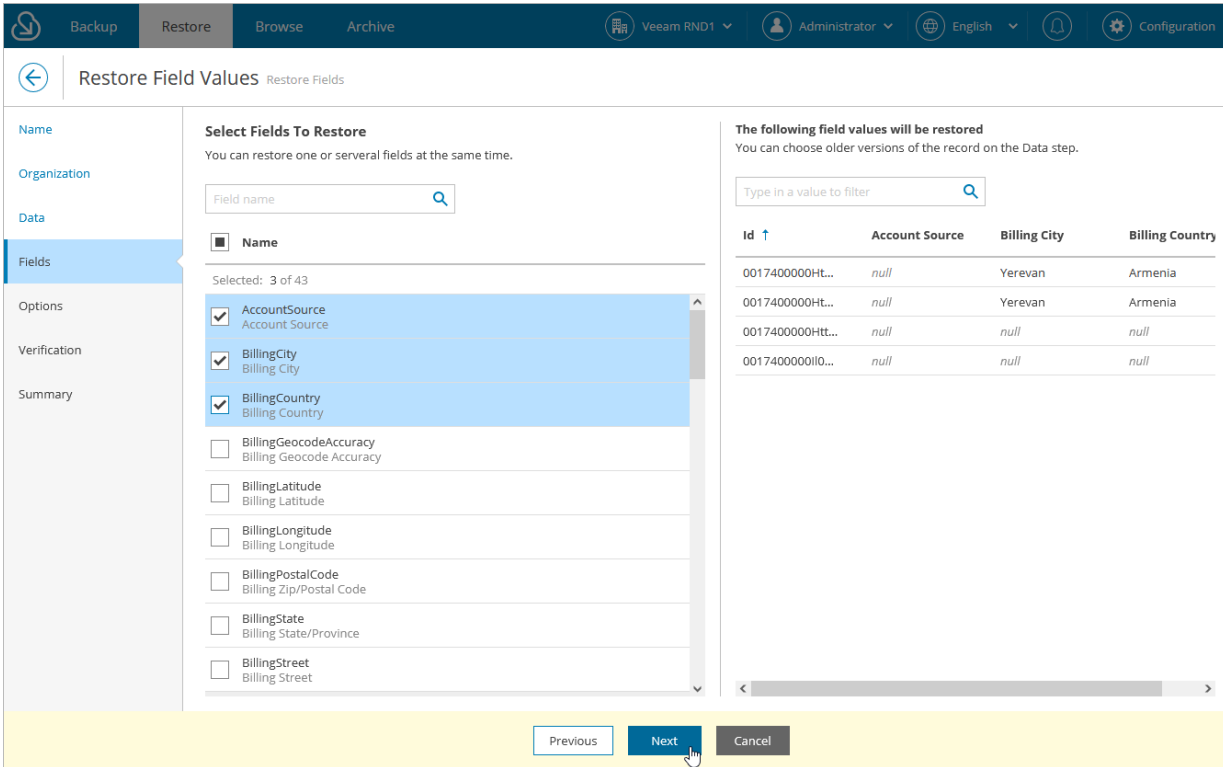


# Step 5. Select Fields to Restore

At the **Fields** step of the wizard, choose fields whose values you want to restore for the selected records. Consider that only values of the fields that are defined by Salesforce as *updatable* can be restored. For example, you cannot restore values of the *read-only* or *formula* fields. These fields will be grayed out.

### TIP

To restore a *formula* field, perform the [metadata restore](#) job.



## Step 6. Configure Additional Restore Settings

At the **Options** step of the wizard, you can instruct Veeam Backup for Salesforce to automatically replace empty field values with *null*, overwrite field values manually, map fields of backed-up records to specific fields in Salesforce, and choose how you want to deactivate blocking automation in Salesforce.

### Automatic Field Overriding Settings

In the **Data consistency** section, you can choose whether you want Veeam Backup for Salesforce to update all existing records and overwrite field values, or restore only those records that have been deleted from Salesforce without updating the existing records. If you select the **Restore records and field values** option, you can also decide whether you want to replace non-empty field values of the existing object records in Salesforce with empty (*null*) values of the backed-up records.

### Manual Field Overriding Settings

In the **Field customization options** section, you can choose whether you want to override specific field values in the restored layouts and new labels (for example, in case of sandbox seeding when you need to mask sensitive data). To do that, click the link in the **Override field values** field, choose a field whose value you want to override and provide a new value.

For a record field to be displayed in the list of available fields, this record must be added to the restore job as described at [step 4](#) of the wizard. Keep in mind that if you restore an object record that contains encrypted fields to the same organization, these fields will be grayed out.

#### TIPS

- When overriding time values, keep in mind that even though the management server and databases use the UTC time zone for all operations, Salesforce adjusts the time set for every Salesforce user according to the time zone settings defined for this user. To learn how to change default time zones in Salesforce, see [Salesforce Documentation](#).
- When entering field values, you can add comments to these values in the following format: *<comment> {value}*. For example, if the backed-up values of the **Name** field are *Account1*, *Account2* and *Account3*, and you specify the *New {value}* comment, the restored values of the field will be *New Account1*, *New Account2* and *New Account3*.

### Field Mapping Settings

In the **Field customization options** section, you can also choose whether you want Veeam Backup for Salesforce to populate fields of the record in Salesforce with values of a specific record from the backup. To do that, click the link in the **Map old fields to new fields** field, choose a field from the backup whose values you want to use and a Salesforce field for which you want to configure mapping. For a field to be displayed in the list of available fields, it must have a backup.

#### IMPORTANT

Mapping of encrypted fields is not supported.

# Blocking Automation Settings

Business logic and automated rules configured in Salesforce can block Veeam Backup for Salesforce restore operations or trigger undesirable side processes. You can choose either to manually deactivate Flows, Validation Rules and Apex Triggers in Salesforce or to instruct the product to bypass all blocking automation while performing a restore operation. To do that, select one of the options in the Turn off automation section:

- Select the **I will manually turn off all blocking automation** option, if you are a Salesforce Administrator and want to deactivate Flows, Validation Rules and Apex Triggers in Salesforce manually.
- Select the **Automatically turn off all automation** option to automatically update Flows, Validation Rules and Apex Triggers so that they are bypassed while the product performs the restore operation without impacting the Salesforce functionality. When you choose this option for a restore job for the first time, updating Flows, Validation Rules and Apex Triggers will take significant time to complete. However, as the updates will be kept in Salesforce, all further restore operations will run faster.
- Select the **Temporarily turn off all automation** option to automatically update Flows, Validation Rules and Apex Triggers so that they are bypassed while the product performs the current restore operation only without impacting the Salesforce functionality. All changes made by the product will be reverted after the restore operation is over. Note that updating Flows, Validation Rules and Apex Triggers and reverting the changes may take significant time to complete.

The screenshot shows the 'Restore Field Values' configuration page for a restore job (ID: restore-job-271429). The page is divided into a left sidebar with navigation tabs (Name, Organization, Data, Fields, Options, Verification, Summary) and a main content area. The 'Options' tab is active. The main content area is titled 'Additional Restore Options' and includes sections for 'Data consistency', 'Field customization options', and 'Turn off automation (workflows, flows, apex triggers and validation rules)'. In the 'Turn off automation' section, the radio button for 'I will manually turn off all blocking automation' is selected. At the bottom of the page, there are three buttons: 'Previous', 'Next', and 'Cancel'.

## Step 7. Check Permissions

At the **Verification** step of the wizard, verify whether the user that is used to perform the restore operation is assigned the permissions required to restore the selected Salesforce object. To do that, click the **Not verified yet** link and wait for the check to complete. If any of the permissions are missing, you must grant them in the Salesforce console manually as described in [Salesforce documentation](#).

To export the list that contains all fields of the records selected at [step 4](#) as a single .CSV file, click **Download CSV File**. Veeam Backup for Salesforce will save the file with the exported data to the default download folder on the local machine.

The screenshot displays the Veeam Backup for Salesforce interface during the 'Restore Field Values' wizard. The top navigation bar includes 'Backup', 'Restore', 'Browse', and 'Archive' tabs, along with user and system information. The left sidebar shows a navigation menu with 'Verification' selected. The main content area is divided into two sections: 'Verify Permissions' and 'Download CSV File'. The 'Verify Permissions' section indicates that the verification step is optional and shows a successful status: 'Verification: No errors or warnings'. The 'Download CSV File' section provides an option to export the list of records. A 'Verification' dialog box is open on the right, displaying a table with the following content:

Status	Operation
Success	No errors or warnings

A 'Close' button is visible at the bottom right of the dialog box.

## Step 8. Finish Working with Wizard

At the **Summary** step of the wizard, review configured settings and click **Finish**.

If you want Veeam Backup for Salesforce to start restore automatically after you complete the wizard, select the **Start the job after clicking the Finish button** check box. Otherwise, the job draft will be created, and you will have to manually run the job as described in section [Starting and Stopping Restore Jobs](#).

### TIP

To view all objects added to the restore session, click the link in the **Object** field.

The screenshot shows the 'Restore Field Values' wizard in the 'Summary' step. The interface includes a top navigation bar with 'Backup', 'Restore', 'Browse', and 'Archive' tabs. The main content area is divided into sections: Connection, Data, Mapping, and Options. The 'Summary' section is highlighted in the left sidebar. At the bottom, there are three buttons: 'Previous', 'Finish', and 'Cancel'. A checkbox labeled 'Start the job after clicking the Finish button' is located above the buttons.

Connection		
Source:	Veeam RND1 - nd3 (sandbox)	
Source database:	vbsf_backup	
Target:	Veeam RND1 - nd3 (sandbox)	

Data		
Restore type:	Fields	
Object:	<a href="#">Account (4)</a>	

Mapping		
Fields mapping:	<b>Backup field</b>	<b>Live org field</b>
	BillingCity	BillingCountry
Fields override:	<b>Field</b>	<b>Value</b>
	AccountSource	Webinar

Options	
Overwrite records:	Yes
Write null values:	Yes
Disable automation:	No
Roll-back disable automation:	No

**Info:** Permanently deleted objects are restored with different IDs. Auto-number fields will get next sequential value.

Start the job after clicking the Finish button

Previous **Finish** Cancel

# Restoring Files

File restore jobs allow you to recover changed and deleted content and attachments.

## IMPORTANT

- When you restore a content version of an existing Salesforce document, Salesforce creates a new version of this Content Document.
- When you restore an attachment, Veeam Backup for Salesforce creates a new file with the same file name and new ID. If the source file still exists, the file content is updated.
- Restore of the *MobileApplicationDetail* and *MailmergeTemplate* types of content is not supported in Veeam Backup for Salesforce.
- Restore of embedded images in rich text area fields is not supported in Veeam Backup for Salesforce, except for images that are stored as content versions in *FeedAttachment* objects.
- To be able to restore an attachment of an email message, the user whose credentials are used to authorize the connection to Salesforce must be assigned the *Update Email Messages* permission. For more information, see [Required Permissions](#).

To create a file restore job, perform the following steps:

1. [Launch the Restore Files wizard.](#)
2. [Specify a name and description for the restore job.](#)
3. [Select Salesforce organizations.](#)
4. [Select files and attachments to restore.](#)
5. [Finish working with the wizard.](#)

# Step 1. Launch Restore Files Wizard

To launch the **Restore Files** wizard:

1. Navigate to the **Restore** tab.
2. If you have added multiple companies to Veeam Backup for Salesforce, select a company to which the Salesforce organization whose data you want to restore belongs. To do that, select the company from the drop-down list at the top of the page.

For a company to be displayed in the list of available companies, it must be added to Veeam Backup for Salesforce as described in section [Adding Companies](#). Also, the user launching the **Restore Files** wizard must be granted permissions to access the company as described in section [User Roles and Permissions](#).

3. Click **New Restore > Files**.

The screenshot shows the Veeam Backup for Salesforce interface. The top navigation bar includes 'Backup', 'Restore', 'Browse', and 'Archive'. The 'Restore' tab is active. Below the navigation bar, there is a search bar for 'Filter by restore job name' and a 'Show:' dropdown set to 'All'. A 'New Restore' dropdown menu is open, showing options for 'Records', 'Fields', 'Files', and 'Metadata'. The 'Files' option is highlighted. Below the menu is a table of restore jobs with columns for 'Type', 'Status', 'Created Date', 'Start Date', 'Finish Date', 'Created By', 'Modified By', and 'Started By'. The table contains 14 rows of data, including jobs with statuses like 'Draft', 'Stopped', and 'Failed'.

	Type	Status	Created Date ↓	Start Date	Finish Date	Created By	Modified By	Started By
<input type="checkbox"/>	Records	Draft	5/18/23, 9:46:23 ...	—	—	admin	admin	—
<input type="checkbox"/>	Metadata	Draft	5/18/23, 9:35:51 ...	—	—	admin	admin	—
<input type="checkbox"/>	Metadata	Draft	5/18/23, 8:29:52 ...	—	—	admin	admin	—
<input type="checkbox"/>	Records	Draft	5/18/23, 4:42:02 ...	—	—	admin	admin	—
<input type="checkbox"/>	Records	Draft	5/18/23, 3:18:14 ...	—	—	admin	admin	—
<input type="checkbox"/>	Records	Draft	5/17/23, 2:01:18 ...	—	—	admin	admin	—
<input type="checkbox"/>	Fields	Draft	5/17/23, 1:47:43 ...	—	—	admin	admin	—
<input type="checkbox"/>	Files	Draft	5/17/23, 12:29:58...	—	—	admin	admin	—
<input type="checkbox"/>	Fields	Stopped	5/16/23, 11:42:19...	5/16/23, 1:54:35 ...	5/16/23, 1:54:42 ...	admin	admin	admin
<input type="checkbox"/>	Records	Draft	5/15/23, 11:34:20...	—	—	admin	admin	—
<input type="checkbox"/>	Records	Draft	5/15/23, 9:55:06 ...	—	—	admin	admin	—
<input type="checkbox"/>	Fields	Failed	5/12/23, 7:35:18 ...	5/12/23, 7:35:32 ...	5/12/23, 7:35:59 ...	admin	admin	admin

## Step 2. Specify Restore Job Info

At the **Name** step of the wizard, use the **Job name** and **Job details or reason for restore** fields to specify a name for the new restore job and to provide a description for future reference. The maximum length of the job name is 100 characters.

The screenshot shows the 'Restore Files' wizard interface. The top navigation bar includes 'Backup', 'Restore', 'Browse', and 'Archive'. The current step is 'Restore Files' (restore-job-4). The left sidebar shows 'Name' as the active step, with other options like 'Organization', 'Data', and 'Summary'. The main content area is titled 'Restore Job Name' and contains the following text: 'This information will be included in the audit log of the restore. It may be helpful to reference the incoming ticket or work item.' Below this, there are two input fields: 'Job name:' with the value 'Restore Files' and 'Job details or reason for restore:' with the value 'Restoring object files'. At the bottom right, there are 'Next' and 'Cancel' buttons.



## Step 3. Select Organization

At the **Organization** step of the wizard, use the **Restore from** drop-down list to select a Salesforce organization whose files and attachments you want to restore. For a Salesforce organization to be displayed in the list, it must belong to the company specified at [step 1](#).

By default, files and attachments are restored to the same Salesforce organization. However, you can choose to restore files and attachments to another organization – to do that, use the **Restore to** drop-down list. For a Salesforce organization to be displayed in the list of available organizations, it must belong to the company specified at [step 1](#) and be compatible with the organization whose files and attachments you want to restore. This means that you can restore from a production or sandbox organization only to its sandbox copies.

### IMPORTANT

If you choose to restore an encrypted file to a production organization, Veeam Backup for Salesforce will decrypt the file and fully restore its content. However, if you choose to restore an encrypted file to a sandbox organization, Veeam Backup for Salesforce will fail to decrypt the file and therefore will create only an empty copy of this file.

The screenshot shows the 'Restore Files' wizard in Veeam Backup for Salesforce. The interface is in the 'Restore' tab, with a navigation bar at the top containing 'Backup', 'Restore', 'Browse', and 'Archive'. The user is logged in as 'Administrator' and the language is set to 'English'. The main content area is titled 'Restore Files' and contains a section for 'Select Salesforce Organizations'. Below this title, there is a sub-header 'Select Salesforce Organizations' and a note: 'Restore data to the same Salesforce organization or to another sandbox.' There are two dropdown menus: 'Restore from:' and 'Restore to:'. Both dropdown menus currently show 'Veeam RND1 - nd3 (sandbox)'. At the bottom of the wizard, there are three buttons: 'Previous', 'Next', and 'Cancel'. The 'Next' button is highlighted with a mouse cursor.

## Step 4. Select Files to Restore

At the **Data** step of the wizard:

1. Select the type of files that you want to restore. For a file type to be displayed in the list of available file types, it must have a backup.

Note that if you select the *Attachment* or *Content Version* file type, you can also specify a Salesforce object associated with these files.

2. Click the **Customize** link to apply specific search conditions and reduce the number of search results. Veeam Backup for Salesforce provides a number of built-in conditional operators (such as *contains*, *equals*, *starts with*, *is null* and so on) that can be used to send requests to databases. Note that the time required to process a request depends on the operator you use – for example, processing a request with the equals operator will take less time than processing a request with the contains operator.

By default, filters are combined by the AND logical operator. That is, a record is displayed in the search results only if all the specified conditions are met. You can change this behavior by combining filters using different operators. To do that, set the **Use filter logic** toggle to *On*, and specify the filter logic expression using condition ordinal numbers, brackets and logical operators – for example, *1 AND (2 OR 3) AND NOT 4*.

You can also specify what Salesforce fields you want to be displayed for the found records. To do that, navigate to the **Display Fields** tab and add the necessary fields.

3. Click **Search**. If you apply any filtering conditions, the search results will be displayed on the same pages where the records were originally shown. To make sure that you have seen all the results, look through all the pages.
4. Select files that you want to restore.

For the *Content Version* file type, you can also choose the version of a file that will be restored. To do that, click the link in the **Version** column, compare the latest version of the backed-up file both with previous backed-up file versions and with the version of the file currently stored in the Salesforce database, and select the necessary version from the **Restore point** drop-down list. If you want Veeam Backup for Salesforce to show only files that differ between selected versions, set the **Compare changes** toggle to *On*.

## TIP

You can download up to 10 files to the local machine. To do that, select the necessary items, and click **Download**. Note that only users assigned the *Administrator* and *Backup Operator* roles can download encrypted files.

The screenshot shows the 'Restore Files' interface in Veeam Backup for Salesforce. The 'Data Filters and Display Fields' dialog is open, allowing users to customize the display of search results. The dialog is divided into two tabs: 'Data Filters' and 'Display Fields'. The 'Display Fields' tab is active, showing a list of available fields and a 'Selected' list.

**Data Filters and Display Fields**

Specify any filters to narrow down your search. Customize a display fields set on the second tab.

**Display Fields**

Available (52)

- Selected: 1 of 52
- Account.AccountSource (Account Source)
- Account.BillingCity (Billing City)
- Account.BillingCountry (Billing Country)
- Account.BillingGeocodeAccuracy (Billing Geoco...
- Account.BillingLatitude (Billing Latitude)
- Account.BillingLongitude (Billing Longitude)
- Account.BillingPostalCode (Billing Zip/Postal Co...
- Account.BillingState (Billing State/Province)
- Account.BillingStreet (Billing Street)
- Account.CreatedById (Created By ID)
- Account.CreatedDate (Created Date)
- Account.Description (Account Description)

Selected (2)

- Selected: 0 of 2
- Name (File Name)
- CreatedDate (Created Date)

Buttons: Add >, < Remove, Search, Cancel

## Step 5. Finish Working with Wizard

At the **Summary** step of the wizard, review configured settings and click **Finish**.

If you want Veeam Backup for Salesforce to start restore automatically after you complete the wizard, select the **Start the job after clicking the Finish button** check box. Otherwise, the job draft will be created, and you will have to manually run the job as described in section [Starting and Stopping Restore Jobs](#).

### TIP

To view all objects added to the restore session, click the link in the **Object** field.

The screenshot shows the 'Restore Files' wizard summary step for job ID 159064. The interface includes a top navigation bar with 'Backup', 'Restore', and 'Browse' tabs, and a user menu for 'Administrator'. The left sidebar has tabs for 'Name', 'Organization', 'Data', and 'Summary', with 'Summary' selected. The main content area displays job details: Job Id: 159064, Job name: restore-job-159064, and Job details: restoring files. It is divided into sections: 'Connection' (Source: (P)RND - preprod (sandbox), Source database: preprod, Target: (P)RND - preprod (sandbox)), 'Data' (Restore type: Files, Object: [Total Objects: 2](#)), and 'Files' (Attachment: 2). An information icon indicates that permanently deleted objects are restored with different IDs and auto-number fields will get the next sequential value. A checkbox labeled 'Start the job after clicking the Finish button' is checked. At the bottom, there are 'Previous', 'Finish', and 'Cancel' buttons.

Name	Job Id: 159064
	Job name: restore-job-159064
	Job details: restoring files
Organization	
Data	
Summary	

**Connection**

Source: (P)RND - preprod (sandbox)  
Source database: preprod  
Target: (P)RND - preprod (sandbox)

**Data**

Restore type: Files  
Object: [Total Objects: 2](#)

**Files**

Attachment: 2

*Permanently deleted objects are restored with different IDs. Auto-number fields will get next sequential value.*

Start the job after clicking the Finish button

Previous Finish Cancel

# Restoring Metadata

Metadata restore jobs allow you to recover metadata of deleted objects as well as to restore metadata to another organization so that metadata of the object you want to restore matches metadata of the object in the target organization. For example:

- If you want to restore the connected app configuration, restore the *ConnectedApp* metadata file first. For more information, see [Salesforce Documentation](#).
- If you want to restore the session settings, restore the *ProfileSessionSetting* metadata file first. For more information, see [Salesforce Documentation](#).
- If you want to restore the password policies, restore the *ProfilePasswordPolicy* metadata file first. For more information, see [Salesforce Documentation](#).
- Reports and dashboards are also types of metadata that can be restored using this type of restore job.

## IMPORTANT

After you restore the metadata of a deleted Salesforce object, you must perform backup of this object before you start a record restore operation. The backup is required for the object to be displayed at [step 4](#) of the **Restore Records** wizard.

To create a metadata restore job, perform the following steps:

1. [Launch the Restore Metadata wizard](#).
2. [Specify a name and description for the restore job](#).
3. [Select Salesforce organizations](#).
4. [Select objects whose metadata will be restored](#).
5. [Review the restore list](#).
6. [Finish working with the wizard](#).

# Step 1. Launch Restore Metadata Wizard

To launch the **Restore Metadata** wizard:

1. Navigate to the **Restore** tab.
2. If you have added multiple companies to Veeam Backup for Salesforce, select a company to which the Salesforce organization whose data you want to restore belongs. To do that, select the company from the drop-down list at the top of the page.

For a company to be displayed in the list of available companies, it must be added to Veeam Backup for Salesforce as described in section [Adding Companies](#). Also, the user launching the **Restore Metadata** wizard must be granted permissions to access the company as described in section [User Roles and Permissions](#).

3. Click **New Restore > Metadata**.

The screenshot shows the Veeam Backup for Salesforce interface. The top navigation bar includes 'Backup', 'Restore', 'Browse', and 'Archive'. The 'Restore' tab is active. Below the navigation bar, there is a search bar for 'Filter by restore job name' and a 'Show:' dropdown set to 'All'. A 'New Restore' dropdown menu is open, showing options for 'Records', 'Fields', 'Files', and 'Metadata'. The 'Metadata' option is highlighted. Below the menu is a table of restore jobs with columns: Type, Status, Created Date, Start Date, Finish Date, Created By, Modified By, and Started By.

Type	Status	Created Date ↓	Start Date	Finish Date	Created By	Modified By	Started By
Records	Draft	5/18/23, 9:46:23 ...	—	—	admin	admin	—
Metadata	Draft	5/18/23, 9:35:51 ...	—	—	admin	admin	—
Metadata	Draft	5/18/23, 8:29:52 ...	—	—	admin	admin	—
Records	Draft	5/18/23, 4:42:02 ...	—	—	admin	admin	—
Records	Draft	5/18/23, 3:18:14 ...	—	—	admin	admin	—
Records	Draft	5/17/23, 2:01:18 ...	—	—	admin	admin	—
Fields	Draft	5/17/23, 1:47:43 ...	—	—	admin	admin	—
Files	Draft	5/17/23, 12:29:58...	—	—	admin	admin	—
Fields	Stopped	5/16/23, 11:42:19...	5/16/23, 1:54:35 ...	5/16/23, 1:54:42 ...	admin	admin	admin
Records	Draft	5/15/23, 11:34:20...	—	—	admin	admin	—
Records	Draft	5/15/23, 9:55:06 ...	—	—	admin	admin	—
Fields	Failed	5/12/23, 7:35:18 ...	5/12/23, 7:35:32 ...	5/12/23, 7:35:59 ...	admin	admin	admin

## Step 2. Specify Restore Job Info

At the **Name** step of the wizard, use the **Job name** and **Job details or reason for restore** fields to specify a name for the new restore job and to provide a description for future reference. The maximum length of the job name is 100 characters.

The screenshot shows the 'Restore Metadata' wizard interface. The top navigation bar includes 'Backup', 'Restore', 'Browse', and 'Archive' tabs. The current step is 'Restore Metadata' for 'restore-job-6'. The left sidebar contains a navigation menu with 'Name' (selected), 'Organization', 'Data', 'Restore List', and 'Summary'. The main content area is titled 'Restore Job Name' and includes a note: 'This information will be included in the audit log of the restore. It may be helpful to reference the incoming ticket or work item.' Below this note are two text input fields: 'Job name:' with the value 'Metadata' and 'Job details or reason for restore:' with the value 'Restoring object metadata'. At the bottom of the form are 'Next' and 'Cancel' buttons.

## Step 3. Select Organization

At the **Organization** step of the wizard, use the **Restore from** drop-down list to select a Salesforce organization whose metadata you want to restore. For a Salesforce organization to be displayed in the list, it must belong to the company specified at [step 1](#).

By default, metadata is restored to the same Salesforce organization. However, you can choose to restore metadata to another organization – to do that, use the **Restore to** drop-down list. For a Salesforce organization to be displayed in the list of available organizations, it must belong to the company specified at [step 1](#) and be compatible with the organization whose metadata you want to restore. This means that you can restore from a production or sandbox organization only to its sandbox copies.

### IMPORTANT

If you plan to restore user profiles to another organization, keep in mind that the same set of objects and fields must exist in the target organization.

The screenshot shows the 'Restore Metadata' wizard in the Veeam Backup for Salesforce interface. The top navigation bar includes 'Backup', 'Restore', 'Browse', and 'Archive'. The current step is 'Restore Metadata', with a sub-tab for 'Metadata'. The left sidebar shows a navigation menu with 'Name', 'Organization' (selected), 'Data', 'Restore List', and 'Summary'. The main content area is titled 'Select Salesforce Organizations' and contains the instruction: 'Restore data to the same Salesforce organization or to another sandbox.' Below this, there are two dropdown menus: 'Restore from:' and 'Restore to:', both currently set to 'Veeam RND1 - nd3 (sandbox)'. At the bottom of the wizard, there are three buttons: 'Previous', 'Next' (highlighted with a mouse cursor), and 'Cancel'.



## Step 4. Select Metadata to Restore

At the **Data** step of the wizard:

1. Use the **Metadata type** drop-down list to select the type of metadata that you want to restore.
2. Click the **Customize** link to apply specific search conditions and reduce the number of search results. Veeam Backup for Salesforce provides a number of built-in conditional operators (such as *contains*, *equals*, *starts with*, *is null* and so on) that can be used to send requests to databases. Note that the time required to process a request depends on the operator you use – for example, processing a request with the *equals* operator will take less time than processing a request with the *contains* operator.

### TIPS

When adding conditions, consider the following:

- If you want to search for records with null field values, use the *is null* operator. Using the *equals* operator in this case is not supported.
- If you want to search for a list of records, you can use the *in* operator and specify the IDs of the necessary records using a comma-separated list.
- If you want to search for a record but you do not have any information on this record except for the fact that it is linked to a specific object, you can use the lookup relationship field to filter all records linked to this object. To do that, specify the ID of the necessary object in the **Value** field.

Note that the **Value** field is case sensitive for the following operators: *starts with*, *ends with*, *equals*, *in*.

By default, filters are combined by the AND logical operator. That is, a record is displayed in the search results only if all the specified conditions are met. You can change this behavior by combining filters using different operators. To do that, set the **Use filter logic** toggle to *On*, and specify the filter logic expression using condition ordinal numbers, brackets and logical operators – for example, *1 AND (2 OR 3) AND NOT 4*.

3. Click **Search**. If you apply any filtering conditions, the search results will be displayed on the same pages where the records were originally shown. To make sure that you have seen all the results, look through all the pages.

- Select metadata files that you want to restore. You can also choose the version of a metadata file that will be restored. To do that, click the link in the **Version** column, compare the latest version of the backed-up metadata file both with previous backed-up file versions and with the version of the file currently stored in the Salesforce database, and select the necessary version from the **Version to restore** drop-down list.

## IMPORTANT

If you are restoring a removed metadata object, make sure that you choose the previous correct version of the file. By default, files are restored to the latest version.

## TIPS

- By default, you can download up to 100 metadata files to the local machine. To do that, select the necessary objects, and click **Download**.
- For metadata of custom objects that was permanently deleted from Salesforce, you must restore metadata of the following types: *CustomObject*, *CustomTab*, *Layout* and *Profile*. While selecting user profiles, you can choose only those profiles that had access to this object.

The screenshot displays the 'Restore Metadata' interface in Veeam Backup for Salesforce. The top navigation bar includes 'Backup', 'Restore', 'Browse', and 'Archive'. The main header shows 'Restore Metadata Metadata'. On the left, a sidebar contains 'Name', 'Organization', 'Data', 'Restore List', and 'Summary'. The main content area is titled 'Select Metadata To Restore' and includes a search bar and a 'Download' button. Below the search bar, a table lists 911 objects found. The table has the following columns: Type, Version, API Name, Name, Last Modified D..., Created Date, and Deleted Date. Two objects are selected, indicated by checkmarks in the first column:

Type	Version	API Name	Name	Last Modified D...	Created Date	Deleted Date
<input checked="" type="checkbox"/>	Workflow	Latest	TestBackupResto...	null	6/3/24, 2:59:38 PM	6/3/24, 2:59:38 PM
<input checked="" type="checkbox"/>	TopicsForObj...	Latest	zqoihqzc_c	null	6/3/24, 2:59:38 PM	6/3/24, 2:59:38 PM
<input type="checkbox"/>	TopicsForObj...	Latest	xkffmkke_c	null	6/3/24, 2:59:38 PM	6/3/24, 2:59:38 PM
<input type="checkbox"/>	TopicsForObj...	Latest	WorkOrderLinelt...	null	6/3/24, 2:59:38 PM	6/3/24, 2:59:38 PM
<input type="checkbox"/>	TopicsForObj...	Latest	WorkOrder	null	6/3/24, 2:59:38 PM	6/3/24, 2:59:38 PM
<input type="checkbox"/>	TopicsForObj...	Latest	usjrznqx_c	null	6/3/24, 2:59:38 PM	6/3/24, 2:59:38 PM

At the bottom of the interface, there are 'Previous', 'Next', and 'Cancel' buttons. The 'Next' button is highlighted with a mouse cursor.

## Step 5. Review Restore List

At the **Restore List** step, review the list of items that you want to restore and proceed with the wizard.

### TIP

You can download up to 100 metadata files to the local machine. To do that, select the necessary objects and click **Download**.

The screenshot shows the 'Restore Metadata' wizard in the Veeam Backup for Salesforce interface. The 'Restore List' step is selected in the left-hand navigation pane. The main area displays a table titled 'Restore list (2 items)' with the following data:

<input checked="" type="checkbox"/>	Type	Version	API Name	Name	Last Modified D...	Created Date	Deleted Date
<input checked="" type="checkbox"/>	Workflow	Latest	TestBackupRestor...	null	6/3/24, 2:59:38 PM	6/3/24, 2:59:38 PM	null
<input checked="" type="checkbox"/>	TopicsForObj...	Latest	zqoihqzc_c	null	6/3/24, 2:59:38 PM	6/3/24, 2:59:38 PM	null

At the bottom of the wizard, there are three buttons: 'Previous', 'Next' (which is highlighted with a mouse cursor), and 'Cancel'.

## Step 6. Finish Working with Wizard

At the **Summary** step of the wizard, review configured settings and click **Finish**.

If you want Veeam Backup for Salesforce to start restore automatically after you complete the wizard, select the **Start the job after clicking the Finish button** check box. Otherwise, the job draft will be created, and you will have to manually run the job as described in section [Starting and Stopping Restore Jobs](#).

### TIP

To view all objects added to the restore session, click the link in the **Object** field.

As soon as you start the restore job, you can see the status of the job both in the Veeam Backup for Salesforce Web UI and in Salesforce. Consider that if you have any other running deploy sessions in Salesforce, the restore job may fail with an error indicating that another deploy is in progress. Wait until other sessions complete, and start the restore job again.

The screenshot shows the 'Restore Metadata' wizard in the 'Summary' step. The interface includes a top navigation bar with 'Backup', 'Restore', 'Browse', and 'Archive' tabs. The main content area is divided into a left sidebar with navigation links (Name, Organization, Data, Restore List, Summary) and a main panel. The main panel displays the following information:

- Summary:** Restore job configuration is complete. You can browse back to adjust the scope and parameters of restore.
- Summary:**
  - Job id: 6
  - Job name: Metadata
  - Job details: Restoring object metadata
- Connection:**
  - Source: Veeam RND1 - nd3 (sandbox)
  - Source database: vbsf\_backup
  - Target: Veeam RND1 - nd3 (sandbox)
- Data:**
  - Restore type: Metadata
  - Object: [2](#)

An information message states: "Permanently deleted objects are restored with different IDs. Auto-number fields will get next sequential value." Below this is a checkbox labeled "Start the job after clicking the Finish button", which is currently unchecked. At the bottom of the wizard, there are three buttons: "Previous", "Finish" (highlighted with a mouse cursor), and "Cancel".

# Starting and Stopping Restore Jobs

You can start a restore job automatically right after you finish the restore job configuration wizard or manually on the **Restore** tab. Consider that after you start the restore job, it cannot be edited or removed anymore. You can only [view the job details](#). However, you can clone this job after the job completes, and then edit it, for example, to create a new draft or to see the list of the restored objects. To learn how to clone and edit restore jobs, see [Cloning and Editing Restore Jobs](#).

To start a restore job:

1. Navigate to the **Restore** tab.
2. From the **Organization** drop-down list, select a Salesforce organization for which the restore job has been created.
3. Select the necessary job.

You can filter restore jobs displayed on the **Restore** tab by using the icons in the **Show** field at the top of the list. If you select a filter, the settings will apply to all companies and will not change during the current user session. That is why if you do not see the necessary job in the list, make sure that the **All** filter is selected.

4. Click **Run**.

## Stopping Restore Jobs

You can stop a running restore job. However, it is not recommended that you do that, as it may result in data inconsistency. Consider that you cannot further edit, start or remove the stopped job.

Job Name	Type	Status	Created Date	Start Date	Finish Date	Created By	Modified By	Started By
<input checked="" type="checkbox"/> Restore records	Records	Draft	6/12/24, 2:40:4...	—	—	admin	admin	—
<input type="checkbox"/> Metadata	Metadata	Draft	6/12/24, 1:56:0...	—	—	admin	admin	—

# Cloning Restore Jobs

You can clone a restore job if you want to launch it again or to create a new job based on the settings of the existing one.

## IMPORTANT

You cannot clone a running restore job.

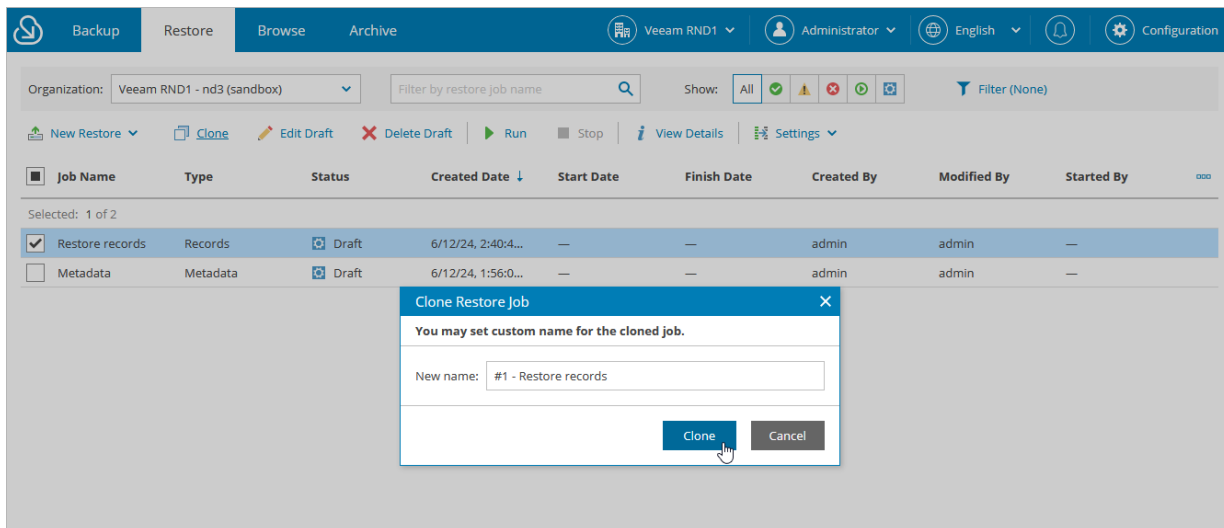
To clone a restore job:

1. Navigate to the **Restore** tab.
2. From the **Organization** drop-down list, select a Salesforce organization for which the restore job has been created.
3. Select the necessary restore job.

You can filter restore jobs displayed on the **Restore** tab by using the icons in the **Show** field at the top of the list. If you select a filter, the settings will apply to all companies and will not change during the current user session. That is why if you do not see the necessary job in the list, make sure that the **All** filter is selected.

4. Click **Clone**.
5. In the **Clone Restore Job** window, specify a name for the new job, and click **Clone**.

After you clone the restore job, you can edit settings of the new draft.



The screenshot displays the Veeam Backup for Salesforce interface. The top navigation bar includes tabs for Backup, Restore, Browse, and Archive. The main area shows a list of restore jobs with columns for Job Name, Type, Status, Created Date, Start Date, Finish Date, Created By, Modified By, and Started By. A dialog box titled "Clone Restore Job" is open, prompting the user to set a custom name for the cloned job. The "New name" field contains "#1 - Restore records". The dialog box has "Clone" and "Cancel" buttons.

Job Name	Type	Status	Created Date	Start Date	Finish Date	Created By	Modified By	Started By
Restore records	Records	Draft	6/12/24, 2:40:4...	—	—	admin	admin	—
Metadata	Metadata	Draft	6/12/24, 1:56:0...	—	—	admin	admin	—

# Editing Restore Jobs

For each restore job that has the *Draft* status, you can edit settings configured while creating the job:

1. Navigate to the **Restore** tab.
2. From the **Organization** drop-down list, select a Salesforce organization for which the restore job has been created.
3. Select the necessary restore job.

You can filter restore jobs displayed on the **Restore** tab by using the icons in the **Show** field at the top of the list. If you select a filter, the settings will apply to all companies and will not change during the current user session. That is why if you do not see the necessary job in the list, make sure that the **All** filter is selected.

4. Click **Edit Draft**.
5. Complete the restore job wizard:
  - a. To provide a new name and description, follow the instructions provided in sections [Restoring Records](#) (step 2), [Restoring Field Values](#) (step 2), [Restoring Files](#) (step 2) or [Restoring Metadata](#) (step 2).
  - b. To change the Salesforce organizations specified for the job, follow the instructions provided in sections [Restoring Records](#) (step 3), [Restoring Field Values](#) (step 3), [Restoring Files](#) (step 3) or [Restoring Metadata](#) (step 3).
  - c. [This step applies to record and field restore only] To modify the list of records that you want to restore, follow the instructions provided in section [Restoring Records](#) (step 4) or [Restoring Field Values](#) (step 4).
  - d. [This step applies to record field restore only] To modify the list of fields whose values you want to restore, follow the instructions provided in section [Restoring Field Values](#) (step 5).
  - e. [This step applies to metadata restore only] To modify the list of metadata objects that you want to restore, follow the instructions provided in section [Restoring Metadata](#) (step 4).
  - f. [This step applies to metadata restore only] To modify the list of metadata records that you want to restore, follow the instructions provided in section [Restoring Metadata](#) (step 5).
  - g. [This step applies to record and file restore only] To modify the list of files that you want to restore, follow the instructions provided in section [Restoring Records](#) (step 5) or [Restoring Files](#) (step 4).
  - h. [This step applies to record restore only] To change the hierarchy restore settings configured for the job, follow the instructions provided in section [Restoring Records](#) (step 6).
  - i. [This step applies to record and field restore only] To change the additional restore options configured for the job, follow the instructions provided in sections [Restoring Records](#) (step 7) or [Restoring Field Values](#) (step 6).
  - j. [This step applies only to record and field restore] To verify the permissions required for the restore job, follow the instructions provided in sections [Restoring Records](#) (step 8) or [Restoring Field Values](#) (step 8).

k. At the **Summary** step of the wizard, review configuration information and click **Finish** to confirm the changes.

Organization: Veeam RND1 - nd3 (sandbox) Filter by restore job name Show: All Filter (None)

New Restore Clone Edit Draft Delete Draft Run Stop View Details Settings

Job Name	Type	Status	Created Date	Start Date	Finish Date	Created By	Modified By	Started By
#1 - Restore rec...	Records	Draft	6/12/24, 2:51:5...	—	—	admin	admin	—
Restore records	Records	Draft	6/12/24, 2:40:4...	—	—	admin	admin	—
Metadata	Metadata	Draft	6/12/24, 1:56:0...	—	—	admin	admin	—



# Removing Restore Job Drafts

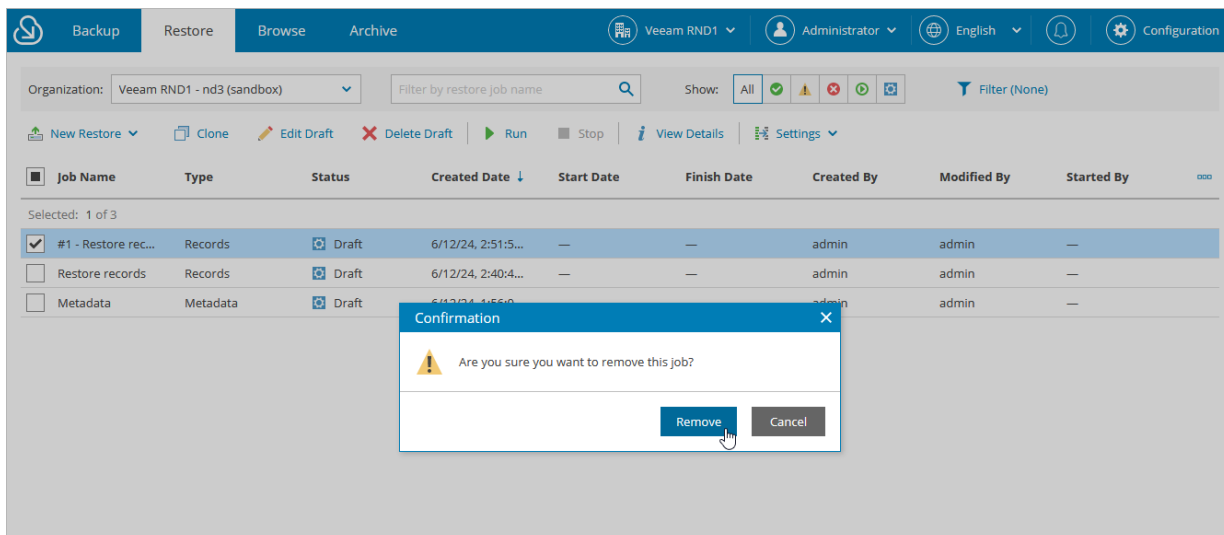
Veeam Backup for Salesforce allows you to permanently remove a draft of a restore job from the configuration database if you no longer need it. However, you cannot remove restore jobs that have already been launched.

To remove a restore job draft:

1. Navigate to the **Restore** tab.
2. From the **Organization** drop-down list, select a Salesforce organization for which the restore job has been created.
3. Select the necessary restore job with the *Draft* status.

You can filter restore jobs displayed on the **Restore** tab by using the icons in the **Show** field at the top of the list. If you select a filter, the settings will apply to all companies and will not change during the current user session. That is why if you do not see the necessary job in the list, make sure that the **All** filter is selected.

4. Click **Delete Draft**.
5. In the **Confirmation** window, click **Remove** to acknowledge the operation.



# Configuring Restore Mapping Settings

You can add alternate keys to configure mapping for a specific organization protected by a backup policy and delete object mapping rules automatically created by the product. These settings will be applied to all restore jobs launched for this organization.

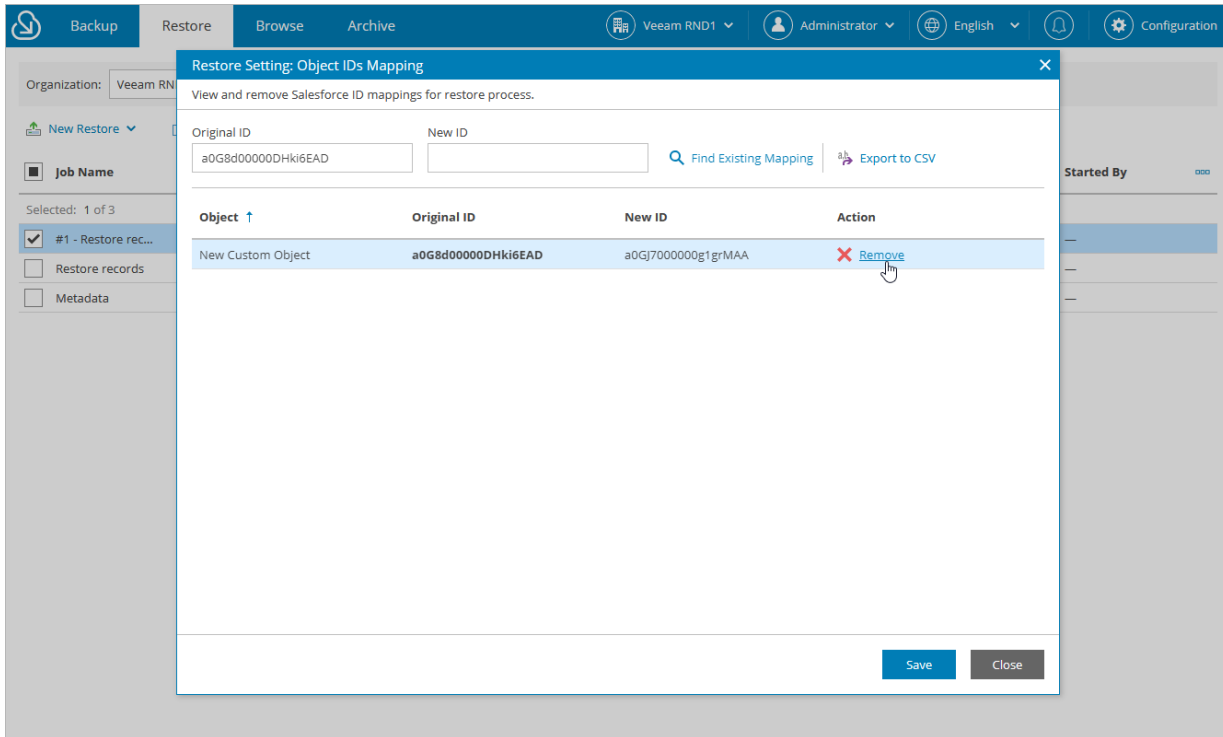
## Object Mapping by Record IDs

When restoring a record that was deleted from the Salesforce database, Veeam Backup for Salesforce creates a new record in Salesforce, assigns a new ID to this record and populates its fields with the values of the record from the backup. To associate the newly created record with the backed-up record, the product creates a default rule that maps the ID of the backed-up record with the ID of the record created in Salesforce. You can delete a mapping rule if you no longer need it. To do that:

1. Navigate to the **Restore** tab.
2. From the **Organization** drop-down list, select a Salesforce organization for which you want to delete a rule.
3. Click **Settings > Object IDs Mapping**.
4. In the **Restore Setting: Object IDs Mapping** window, do the following:
  - a. Specify the ID of the record saved in the backup file, the ID of the existing Salesforce record or both, and click **Find Existing Mapping**.
  - b. Click **Remove**.
  - c. To save the configured mapping settings, click **Save**.

## TIP

To export the list that contains all mapping rules created for the restored records, click **Export to CSV**. Veeam Backup for Salesforce will export all the mapping rules to a CSV file and download it to your local machine.



## Mapping by Alternate Keys

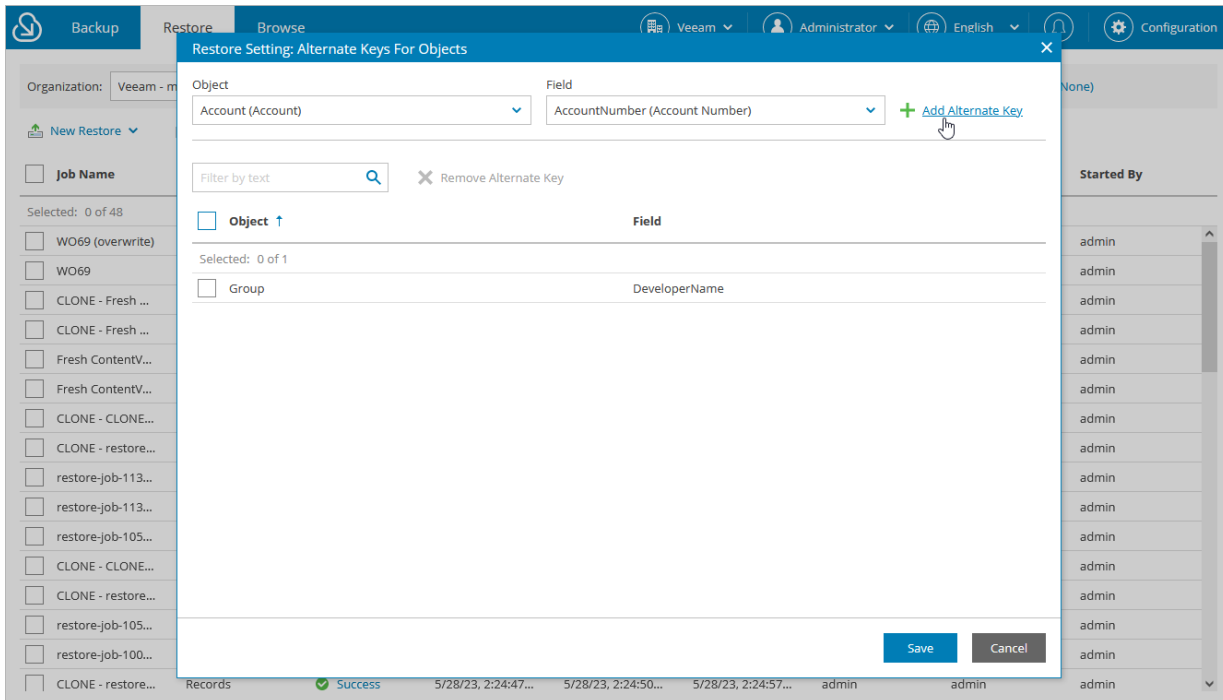
When restoring a Salesforce record, Veeam Backup for Salesforce checks whether the record already exists in the target Salesforce database. By default, the product uses the ID of the record saved in the backup file to search for the record. However, you can add an alternate key and instruct Veeam Backup for Salesforce to use this key instead of the record ID, that is, define a record field with a unique value that will be used to identify the restored record in case the product fails to find it by the record ID. For example, you can create a mapping rule and instruct the product to use the phone number or email field instead of the default record ID.

To add an alternate key, do the following:

1. Navigate to the **Restore** tab.
2. From the **Organization** drop-down list, select a Salesforce organization for which you want to add the alternate key.
3. Click **Settings > Alternate Keys**.
4. In the **Restore Setting: Alternate Keys for Objects** window, do the following:
  - a. Choose an object for which you want to configure mapping.
  - b. Choose a field that will be used for mapping instead of the default record ID. The field must be unique for the selected object.
  - c. Click **Add Alternate Key**.
  - d. To save the configured settings, click **Save**.

## NOTES

- If you want to [override values of specific fields](#) or [configure mapping by field](#) when restoring a record, keep in mind that these settings will be applied first.
- When a record is restored using an alternate key, a new [object mapping rule](#) is created. The object mapping rule will further be used to restore this record since object mapping by ID always prevails over alternate key mapping.



# Viewing Restore Job Details

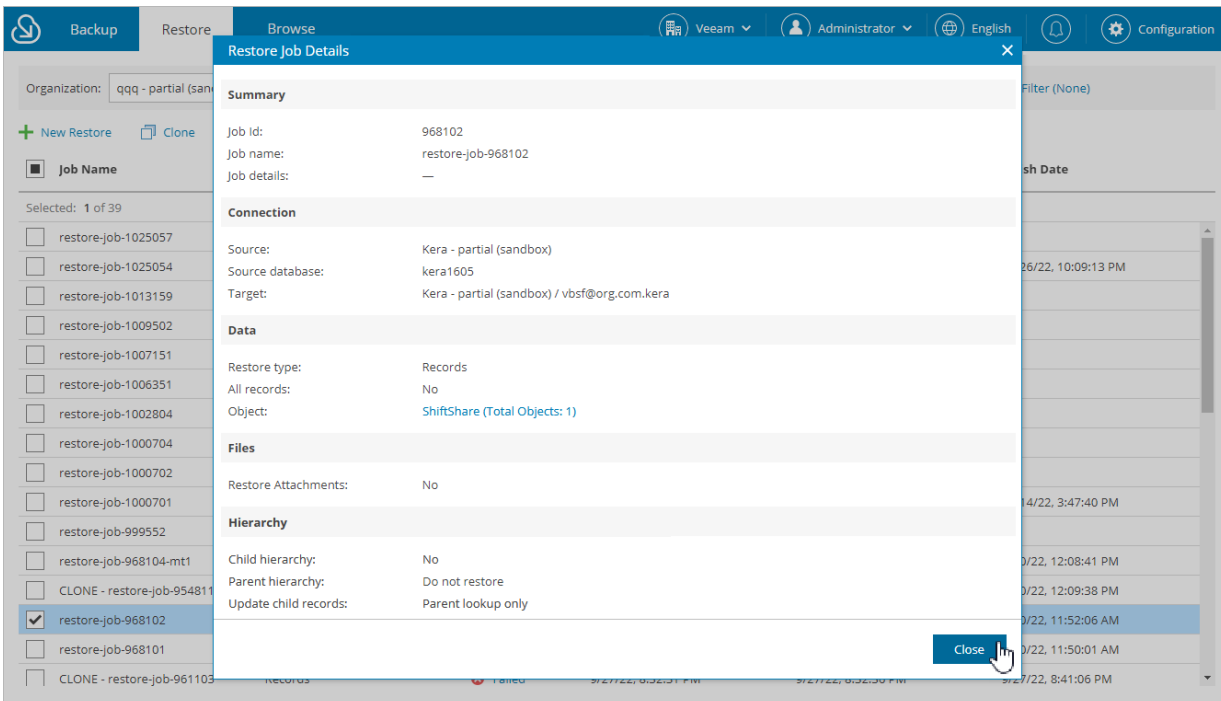
Veeam Backup for Salesforce displays all restore jobs and restore job drafts on the **Restore** tab. After you run a restore job, it cannot be edited or removed anymore. Users can only view the job details and [restore session statistics](#). Users assigned any role can see information on restore jobs created for Salesforce organizations to which data they have access.

You can filter restore jobs displayed on the **Restore** tab by using the icons in the **Show** field at the top of the list. If you select a filter, the settings will apply to all companies and will not change during the current user session. That is why if you do not see the necessary job in the list, make sure that the **All** filter is selected.

To view settings configured for a specific restore job:

1. Select the necessary restore job policy.
2. Click **View Details**.

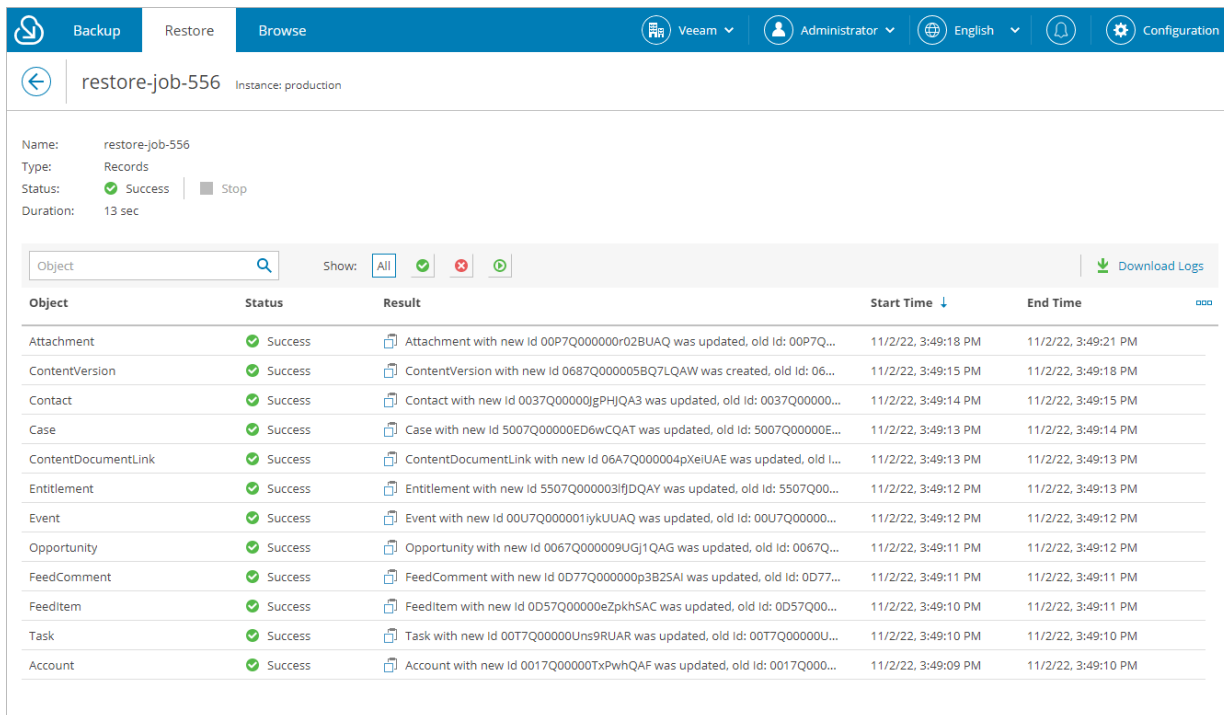
The **Restore Job Details** window will open.



# Viewing Restore Sessions

For each performed restore job, Veeam Backup for Salesforce starts a new session and stores its records in the configuration database. You can track real-time statistics of all running and completed operations on the **Restore** tab. To view the full list of tasks executed during an operation, click the link in the **Status** column. The restore session page will open.

On the restore session page, Veeam Backup for Salesforce displays only Salesforce records that have been processed during the restore session. The records are grouped by every Salesforce batch, that is why one object may appear on the page multiple times. Consider that the results shown in the **Result** column are limited due to performance reasons. To see the full results, download the restore session logs – the logs will be collected and saved to the default download folder on the local machine in a single `log.zip` archive.



The screenshot shows the Veeam Backup for Salesforce interface. The top navigation bar includes 'Backup', 'Restore', and 'Browse' tabs. The current session is 'restore-job-556' for the 'production' instance. The session details show it is a 'Records' type, 'Success' status, and lasted '13 sec'. Below this is a table of restored objects.

Object	Status	Result	Start Time ↓	End Time
Attachment	Success	Attachment with new Id 00P7Q00000r02BUAQ was updated, old Id: 00P7Q...	11/2/22, 3:49:18 PM	11/2/22, 3:49:21 PM
ContentVersion	Success	ContentVersion with new Id 0687Q000005BQ7LQAW was created, old Id: 06...	11/2/22, 3:49:15 PM	11/2/22, 3:49:18 PM
Contact	Success	Contact with new Id 0037Q000000jPHJQA3 was updated, old Id: 0037Q00000...	11/2/22, 3:49:14 PM	11/2/22, 3:49:15 PM
Case	Success	Case with new Id 5007Q00000ED6wCQAT was updated, old Id: 5007Q00000E...	11/2/22, 3:49:13 PM	11/2/22, 3:49:14 PM
ContentDocumentLink	Success	ContentDocumentLink with new Id 06A7Q000004pXeiUAE was updated, old I...	11/2/22, 3:49:13 PM	11/2/22, 3:49:13 PM
Entitlement	Success	Entitlement with new Id 5507Q000003ifjDQAY was updated, old Id: 5507Q00...	11/2/22, 3:49:12 PM	11/2/22, 3:49:13 PM
Event	Success	Event with new Id 00U7Q000001iykUUAQ was updated, old Id: 00U7Q00000...	11/2/22, 3:49:12 PM	11/2/22, 3:49:12 PM
Opportunity	Success	Opportunity with new Id 0067Q000000UGj1QAG was updated, old Id: 0067Q...	11/2/22, 3:49:11 PM	11/2/22, 3:49:12 PM
FeedComment	Success	FeedComment with new Id 0D77Q000000p3B25AI was updated, old Id: 0D77...	11/2/22, 3:49:11 PM	11/2/22, 3:49:11 PM
FeedItem	Success	FeedItem with new Id 0D57Q00000eZpkhSAC was updated, old Id: 0D57Q00...	11/2/22, 3:49:10 PM	11/2/22, 3:49:11 PM
Task	Success	Task with new Id 00T7Q000000Uns9RUAR was updated, old Id: 00T7Q00000U...	11/2/22, 3:49:10 PM	11/2/22, 3:49:10 PM
Account	Success	Account with new Id 0017Q00000TxPwhQAF was updated, old Id: 0017Q000...	11/2/22, 3:49:09 PM	11/2/22, 3:49:10 PM

# Performing Salesforce Archiving

In the Veeam Backup for Salesforce *Advanced* license package, you can configure archival policies and instruct the product to delete unwanted data from Salesforce to consume less storage space in Salesforce. You can archive only records and files that have been backed up by the product; for the list of objects that cannot be archived, see [Appendix A. Unsupported Objects](#).

## NOTE

Only users assigned the *Administrator* or *Backup Operator* role can perform archival operations in Veeam Backup for Salesforce. However, these users can create and run archival policies within their permission scope only – that is, for companies and organizations whose data they can access.

## In This Section

- [Creating Archival Policies](#)
- [Starting and Stopping Archival Policies](#)
- [Disabling and Enabling Archival Policies](#)
- [Editing Archival Policies](#)
- [Removing Archival Policy](#)
- [Viewing Archival Policy Details](#)

# Creating Archival Policies

To create an archival policy, complete the following steps:

1. [Launch the Add Archival Policy wizard.](#)
2. [Specify a name and description for the archival policy.](#)
3. [Configure connection to a Salesforce organization.](#)
4. [Choose data that will be archived.](#)
5. [Configure general archive settings.](#)
6. [Configure hierarchy settings.](#)
7. [Finish working with the wizard.](#)

## IMPORTANT

Before you create an archival policy, it is strongly recommended that you deactivate [Flows](#), [Validation Rules](#) and [Apex Triggers](#) in Salesforce since business logic and automated rules configured in Salesforce can block Veeam Backup for Salesforce archival operations and trigger undesirable side processes.



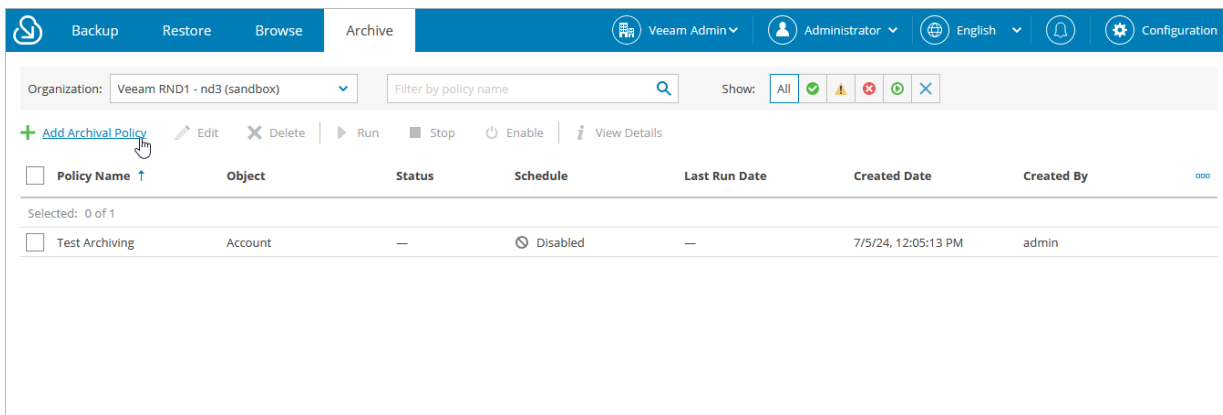
# Step 1. Launch Add Archival Policy Wizard

To launch the **Add Archival Policy** wizard, do the following:

1. Navigate to the **Archive** tab.
2. If you have added multiple companies to Veeam Backup for Salesforce, select a company to which the Salesforce organization whose data you want to be archived belongs. To do that, select the company from the drop-down list at the top of the page.

For a company to be displayed in the list of available companies, it must be added to Veeam Backup for Salesforce as described in section [Adding Companies](#). Also, the user launching the **Add Archival Policy** wizard must be granted permissions to access the company as described in section [User Roles and Permissions](#).

3. Click **Create Archival Policy**.



## Step 2. Specify Archival Policy Info

At the **Name** step of the wizard, use the **Policy name** and **Description** fields to specify a name for the new archival policy and to provide a description for future reference. The maximum length of the policy name is 100 characters.

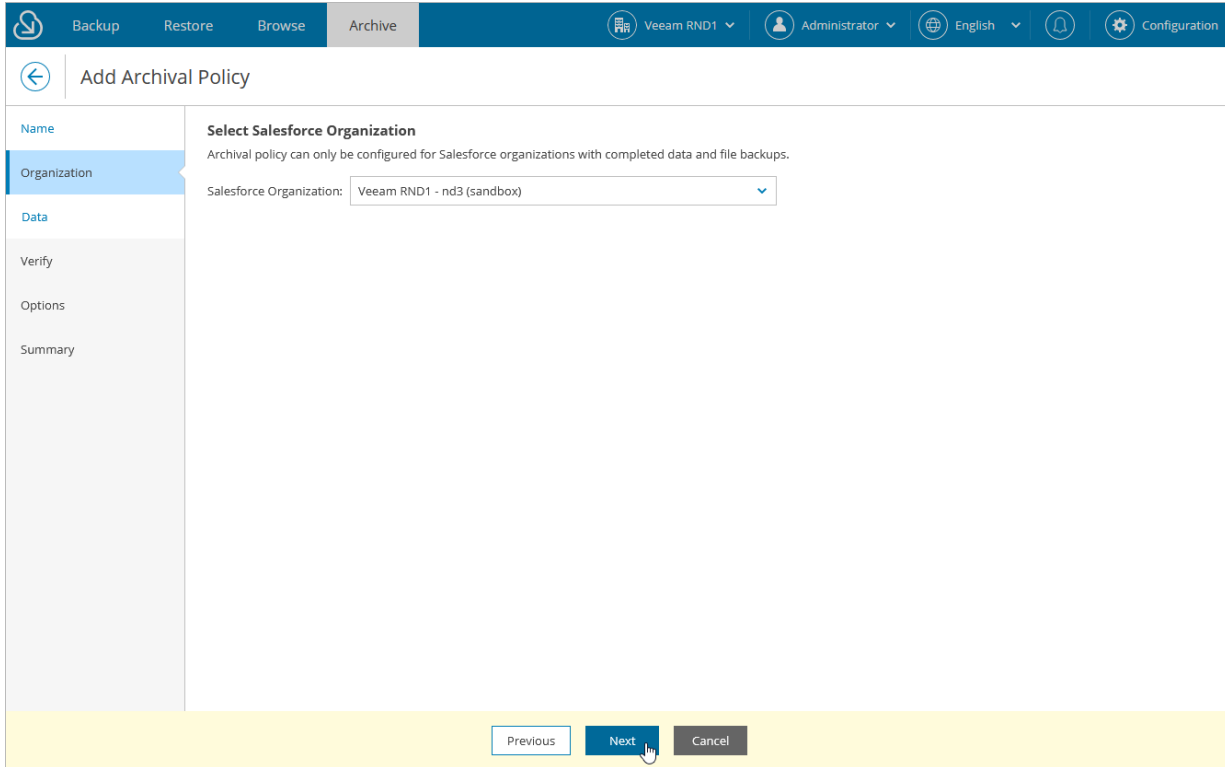
The screenshot shows the 'Add Archival Policy' wizard in Veeam Backup for Salesforce. The interface is in the 'Archive' tab. The 'Name' step is selected in the left-hand navigation pane. The main area is titled 'Archival Policy Name' and contains the following fields:

- Policy name:** Account archive
- Description:** Archive unnecessary account records

At the bottom of the wizard, there are two buttons: 'Next' (highlighted) and 'Cancel'.

# Step 3. Select Organization

At the **Organization** step of the wizard, select a Salesforce organization whose records you want to archive. For a Salesforce organization to be displayed in the list of available organizations, it must belong to the company specified at [step 1](#) of the wizard and have been backed up.



# Step 4. Choose Data to Archive

At the **Data** step of the wizard, do the following:

1. Select a Salesforce object whose records you want to archive. Note that one archival policy can archive records of one root object only. If you want to archive records of multiple root objects, create an archival policy for each object.

For a Salesforce object to be displayed in the list of available root objects, it must have a backup. If the list does not contain the necessary object, the object either does not have a backup or cannot be archived. The object may not have a backup for the following reasons:

- The object was excluded from the backup policy that protects the Salesforce organization to which this object belongs.
- The Salesforce user whose permissions are used for backup operations does not have access to the object.
- Backup of the object is not supported in the current product version. For more information, see [Appendix A. Unsupported Objects](#).

2. Select records that you want to archive. To do that, use filters in the **Records filter** section to apply specific search conditions.

Veeam Backup for Salesforce provides a number of built-in conditional operators (such as *contains*, *equals*, *starts with*, *is null* and so on) that can be used to send requests to databases. Note that the time required to process a request depends on the operator you use – for example, processing a request with the *equals* operator will take less time than processing a request with the *contains* operator.

## TIP

When adding conditions, consider the following:

- If you want to search for records with null field values, use the *is null* operator. Using the *equals* operator in this case is not supported.
- If you want to search for a list of records, you can use the *in* operator and specify the IDs of the necessary records using a comma-separated list.
- If you want to search for a record but you do not have any information on this record except for the fact that it is linked to a specific object, you can use the lookup relationship field to filter all records linked to this object. To do that, specify the ID of the necessary object in the **Value** field.

Note that the **Value** field is case sensitive for the following operators: *starts with*, *ends with*, *equals*, *in*.

By default, filters are combined by the AND logical operator. That is, a record is displayed in the search results only if all the specified conditions are met. You can change this behavior by combining filters using different operators. To do that, set the **Use filter logic** toggle to *On*, and specify the filter logic expression using condition ordinal numbers, brackets and logical operators – for example, *1 AND (2 OR 3) AND NOT 4*.

After you specify the filtering conditions, you can estimate the exact number of records that will be archived. To do that, click **Count** in the **Count sample size** section.

## IMPORTANT

If an object record that you want to archive contains encrypted fields, you will not be able to specify filters for these fields.

Backup Restore Browse Archive Veeam RND1 Administrator English Configuration

### Add Archival Policy

**Name**

**Organization**

**Data**

**Verify**

**Options**

**Summary**

**Data**

Select an object for the policy and specify filtering criteria for archived records. Archived records must be present in the backup.

Select object: Contact (Contact)

**Records Filter**

Specify conditions to find records that should be archived. For example, "LastModifiedDate" less than period "3 Years".

Field:	Operator:	Value:
IsDeleted (Deleted)	equals	false
Accountid (Account ID)	contains	00

+ Add Condition

Use filter logic:  Off

**Count Sample Size**

Count records in the backup that match specified filters. This calculation does not count related records and files that might be archived as well.

Stop

4 records found in Contact

Previous Next Cancel

# Step 5. Configure General Settings

At the **Options** step of the wizard, you can select an archival schedule, specify API request and safety control limits and run the policy in the test mode.

## Schedule Settings and API Request Limits

In the **Schedule** section, choose whether you want to launch the policy every day, every week, every month or according to a custom schedule. For a custom schedule to be displayed in the list of available schedules, it must be created for the company selected at [step 1](#) of the wizard as described in section [Creating Backup Policies](#).

## Test Mode Settings

In the **Test mode** section, you can choose whether you want to run the archival policy in the test mode without actually deleting any data. To do that, select the **Run in test mode** check box – and then, either wait for the policy to run according to the selected schedule or run it manually after you finish working with the **Add Archival Policy** wizard. When the policy completes, follow the instructions provided in section [Viewing Archival Policy Sessions](#) to view the number of records that will be archived for both the selected object and all its child objects.

## Safety Settings and API Request Limits

In the **Safety controls** section, you can specify the maximum number of root records that can be archived in one archival policy and the minimum level of the child objects hierarchy that must be archived for all the selected records.

You can also specify thresholds for REST API and BULK API requests that must not be breached during archival operations since the total number of API requests that can be sent to Salesforce within 24 hours is [limited for each Salesforce organization](#) – this will help you ensure that Veeam Backup for Salesforce does not conflict with other applications that use API requests for integration with Salesforce. To do that, click **Set API limits** and enter the necessary threshold values (in percentage) in the **Set API limits** window.

## NOTES

By design, Veeam Backup for Salesforce checks the number of remaining API requests every time it starts a new policy session:

- If any of the specified thresholds is breached, the session fails with an error indicating that the API request limit has been exceeded.
- If none of the specified thresholds is breached, Veeam Backup for Salesforce starts processing child objects added to the policy one by one.

Every time it processes a new child object, it checks the number of remaining API requests – if any of the specified thresholds is breached, the session fails with an error indicating that the API request limit has been exceeded, and all child objects that have not been processed yet remain undeleted. However, Veeam Backup for Salesforce continues sending requests to Salesforce to archive child objects whose processing started before the session failed. The latter may cause Veeam Backup for Salesforce to accidentally exceed the maximum limit of API requests that you specified.

The screenshot shows the 'Add Archival Policy' configuration page in Veeam Backup for Salesforce. The page is divided into a left sidebar with navigation tabs (Name, Organization, Data, Verify, Options, Summary) and a main content area. The 'Options' tab is selected, showing the following configuration options:

- Options**: Select policy schedule and run options.
- Schedule**: Policy Schedule: Daily (dropdown menu).
- Test mode**:  Run in test mode. Description: Running an archival policy in test mode allows to query Salesforce data without deleting it. This mode helps to verify which objects and how many records will actually be affected by the policy.
- Safety controls**: Define how many records can be archived per policy run. Archive records limit: 100000 (spinner control). Bypass restricted relationships and archive related child records down to the specified hierarchy depth. Hierarchy depth: 5 (spinner control).
- Set API limits

At the bottom of the page, there are three buttons: 'Previous', 'Next' (highlighted with a mouse cursor), and 'Cancel'.

# Step 6. Configure Hierarchy Settings

At the **Verify** step of the wizard, Veeam Backup for Salesforce will check whether all child objects related to the root object selected at [step 4](#) have backups. You must thoroughly review the list of these child objects and confirm whether they can be safely deleted from Salesforce. To do that, select the **Confirm permanent deletion** check box.

Even if a child object is not displayed in the list (which means it has a backup), Veeam Backup for Salesforce will not be able to archive this object if it is linked to the root object using any relationship other than master-detail relationship, required lookup field relationship, or optional lookup field relationship with the **Delete this record also** option enabled. For more information on object relationships, see [Salesforce documentation](#).

## TIP

If you want to keep any of the child objects, [edit the data protection settings](#) of the backup policy that protects the Salesforce organization to which the parent object belongs, [run the policy](#) to create an incremental backup – and then, modify the archival policy settings to check whether the necessary child objects now have backups.

You must also verify whether the user that is used to perform the archival operation is assigned the permissions required to archive the selected Salesforce object. To do that, click the **Not verified yet** link and wait for the check to complete. If any of the permissions are missing, you must grant them in the Salesforce console manually as described in [Salesforce documentation](#).

The screenshot shows the 'Add Archival Policy' wizard in the 'Verify' step. The interface includes a top navigation bar with 'Backup', 'Restore', 'Browse', and 'Archive' tabs. The 'Verify' step is active, showing a table of child objects and their relationships. A 'Verify permissions' section indicates that verification is completed with no issues found. At the bottom, there are 'Previous', 'Next', and 'Cancel' buttons.

Child Object	Relationship Field	Confirmation
EmailCapture	—	⚠ Delete without possibility to restore
ServiceReport	—	⚠ Delete without possibility to restore
MobileApplicationDetail	—	⚠ Delete without possibility to restore
FeedAttachment	FeedEntityId	⚠ Delete without possibility to restore
Attachment	ParentId	⚠ Delete without possibility to restore
Document	—	⚠ Delete without possibility to restore

Confirm permanent deletion

Verify permissions  
Verify permissions before running the archive policy. Learn more about [verified permissions](#).  
✔ Verification completed. No issues found.



# Step 7. Finish Working with Wizard

At the **Summary** step of the wizard, review configured settings and click **Finish**.

The screenshot shows the 'Add Archival Policy' wizard in the 'Summary' step. The interface includes a top navigation bar with tabs for Backup, Restore, Browse, and Archive. The 'Archive' tab is active. The main content area is divided into a left sidebar with navigation links (Name, Organization, Data, Verify, Options, Summary) and a main panel displaying the policy configuration summary. The summary includes sections for Summary, Organization, Data, Child Objects, and Options, each with specific configuration details. At the bottom, there are three buttons: 'Previous', 'Finish', and 'Cancel'. A mouse cursor is hovering over the 'Finish' button.

Summary	
Archival policy configuration is complete. You can browse back to adjust the scope and parameters of the policy.	
<b>Summary</b>	
Archival policy name:	Account archive
Description:	Archive unnecessary account records
<b>Organization</b>	
Salesforce Organization:	Veeam RND1 - nd3 (sandbox)
<b>Data</b>	
Object:	Contact
<b>Child Objects</b>	
Approved for permanent deletion:	42
<b>Options</b>	
Schedule:	At 12:00 AM (UTC+0:00) UTC
REST API usage limit:	80 %
BULK API usage limit:	80 %
Test mode:	No

# Starting and Stopping Archival Policies

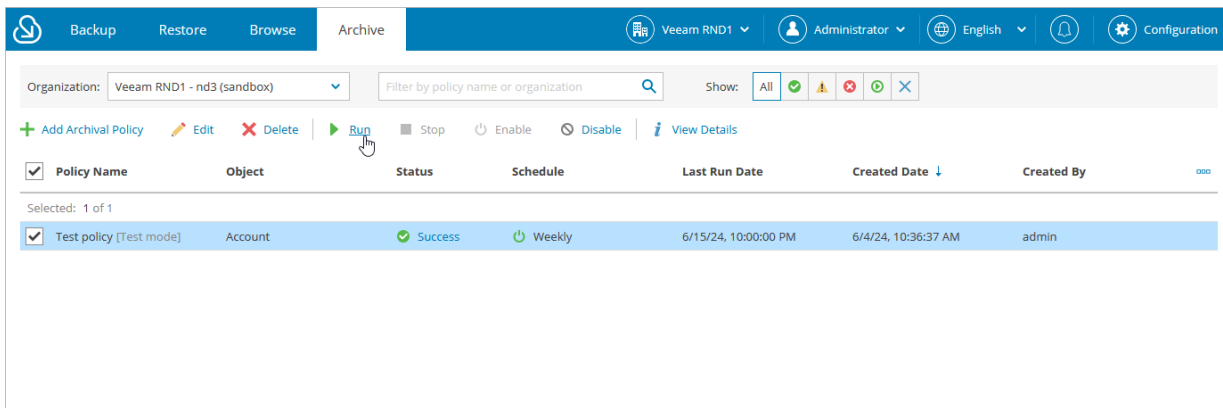
You can start an archival policy manually, for example, if you want to archive more records and do not want to modify the configured policy schedule. You can also stop a policy manually if processing is about to take too long, and you do not want the policy to have an impact on the production environment during business hours.

To start or stop an archival policy:

1. Navigate to the **Archive** tab.
2. From the **Organization** drop-down list, select a Salesforce organization for which the archival policy has been created.
3. Select the necessary archival policy.

You can filter archival policies displayed on the **Archive** tab by using the icons in the **Show** field at the top of the list. If you select a filter, the settings will apply to all companies and will not change during the current user session. That is why if you do not see the necessary policy in the list, make sure that the **All** filter is selected.

4. Click **Run** or **Stop**.



# Disabling and Enabling Archival Policies

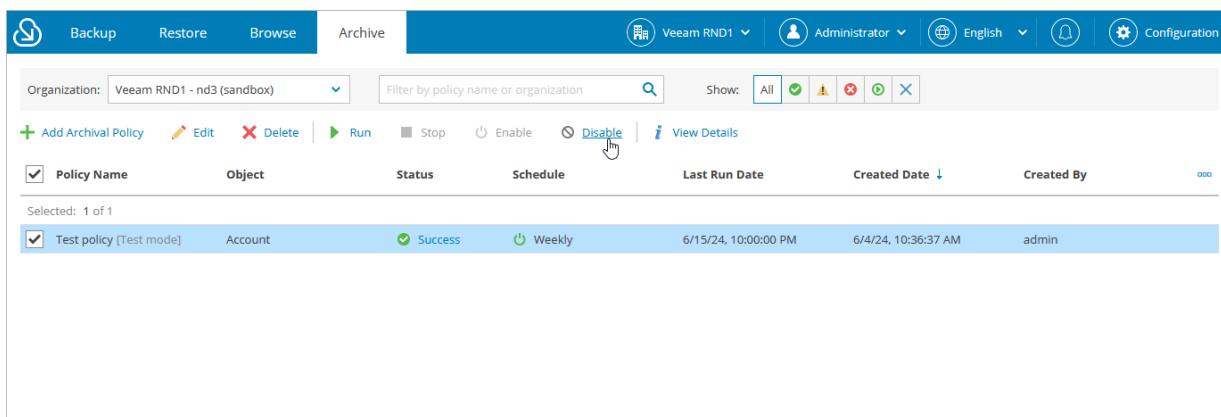
By default, Veeam Backup for Salesforce runs all created archival policies according to the specified schedules. However, you can temporarily disable an archival policy so that Veeam Backup for Salesforce does not run the policy automatically. You will still be able to manually start or enable the disabled archival policy at any time you need.

To disable or enable an archival policy, do the following:

1. Navigate to the **Archive** tab.
2. From the **Organization** drop-down list, select a Salesforce organization for which the archival policy has been created.
3. Select the necessary archival policy.

You can filter archival policies displayed on the **Archive** tab by using the icons in the **Show** field at the top of the list. If you select a filter, the settings will apply to all companies and will not change during the current user session. That is why if you do not see the necessary job in the list, make sure that the **All** filter is selected.

4. Click **Disable** or **Enable**.



The screenshot shows the Veeam Backup for Salesforce interface. The top navigation bar includes 'Backup', 'Restore', 'Browse', and 'Archive'. The 'Archive' tab is active. The organization is set to 'Veeam RND1 - nd3 (sandbox)'. The 'Show' field is set to 'All'. The table below shows the following data:

<input checked="" type="checkbox"/>	Policy Name	Object	Status	Schedule	Last Run Date	Created Date ↓	Created By
<input checked="" type="checkbox"/>	Test policy [Test mode]	Account	Success	Weekly	6/15/24, 10:00:00 PM	6/4/24, 10:36:37 AM	admin

# Editing Archival Policies

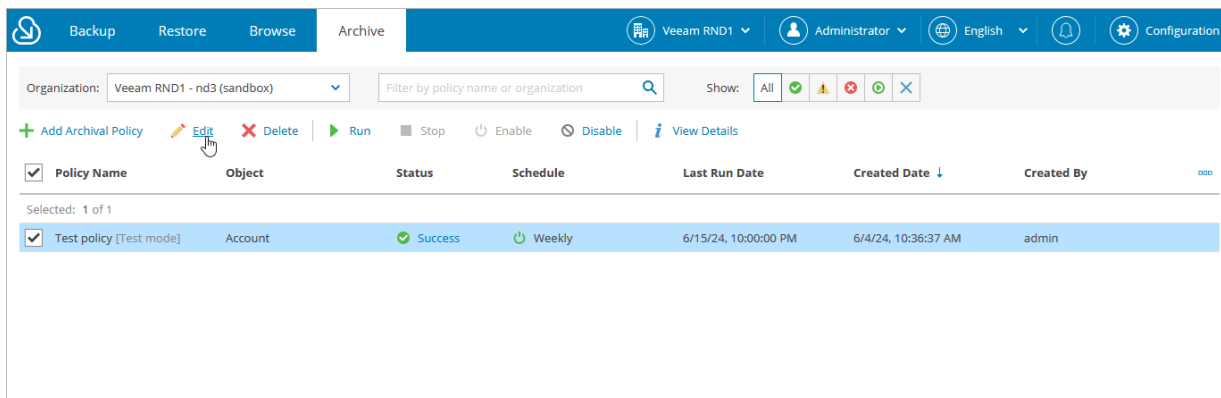
You can edit archival policies created in Veeam Backup for Salesforce. For example, you may want to modify some settings for an archival policy, change the policy schedule and so on.

To edit archival policy settings, do the following:

1. Navigate to the **Archive** tab.
2. From the **Organization** drop-down list, select a Salesforce organization for which the archival policy has been created.
3. Select the necessary archival policy.

You can filter archival policies jobs displayed on the **Archive** tab by using the icons in the **Show** field at the top of the list. If you select a filter, the settings will apply to all companies and will not change during the current user session. That is why if you do not see the necessary job in the list, make sure that the **All** filter is selected.

4. Click **Edit**.
5. Complete the **Edit Archival Policy** wizard:
  - a. To change the name and description of the policy, follow the instructions provided in section [Creating Archival Policies](#) (step 2).
  - b. To modify the list of records that you want to archive, follow the instructions provided in section [Creating Archival Policies](#) (step 4).
  - c. To change the schedule configured for the policy, follow the instructions provided in section [Creating Archival Policies](#) (step 5).
  - d. To verify permissions and confirm permanent deletion of associated child objects, follow the instructions provided in section [Creating Archival Policies](#) (step 6).
  - e. At the **Summary** step of the wizard, review configuration information and click **Finish** to confirm the changes.



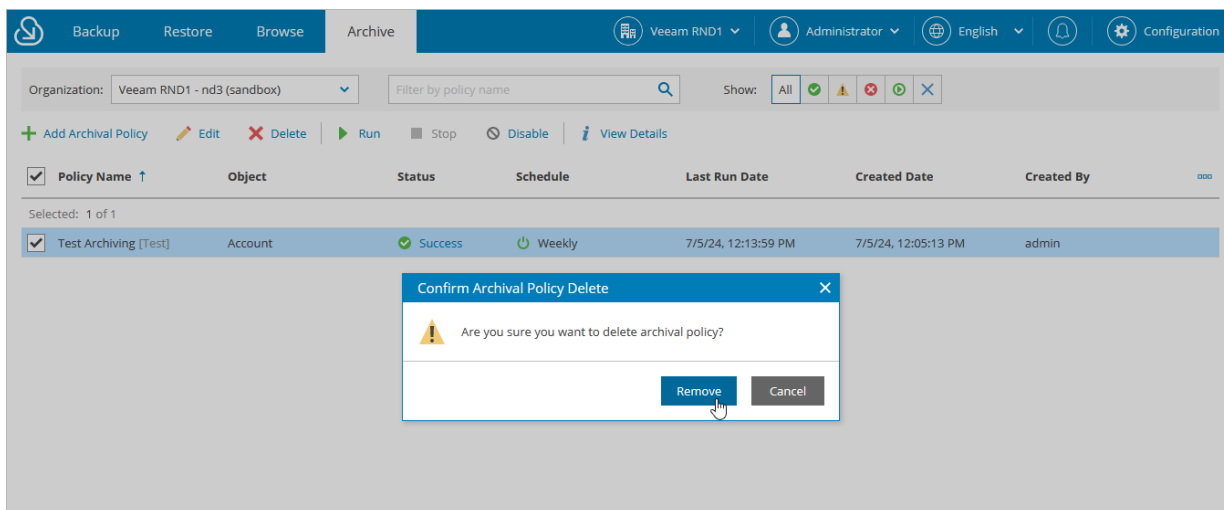
# Removing Archival Policy

Veeam Backup for Salesforce allows you to permanently remove an archival policy from the configuration database if you no longer need it:

1. Navigate to the **Archive** tab.
2. From the **Organization** drop-down list, select a Salesforce organization for which the archival policy has been created.
3. Select the necessary archival policy.

You can filter archival policies displayed on the **Archive** tab by using the icons in the **Show** field at the top of the list. If you select a filter, the settings will apply to all companies and will not change during the current user session. That is why if you do not see the necessary policy in the list, make sure that the **All** filter is selected.

4. In the **Confirm Archival Policy Delete** window, click **Remove** to acknowledge the operation. The archived data and files will not be affected.



# Viewing Archival Policy Details

After you create archival policies, Veeam Backup for Salesforce displays the policies on the **Archive** tab. Users assigned any role can see information on archival policies created for Salesforce organizations to which data they have access.

You can filter archival policies displayed on the **Archive** tab by using the icons in the **Show** field at the top of the list. If you select a filter, the settings will apply to all companies and will not change during the current user session. That is why if you do not see the necessary policy in the list, make sure that the **All** filter is selected.

Each policy in the list is described with the following set of properties:

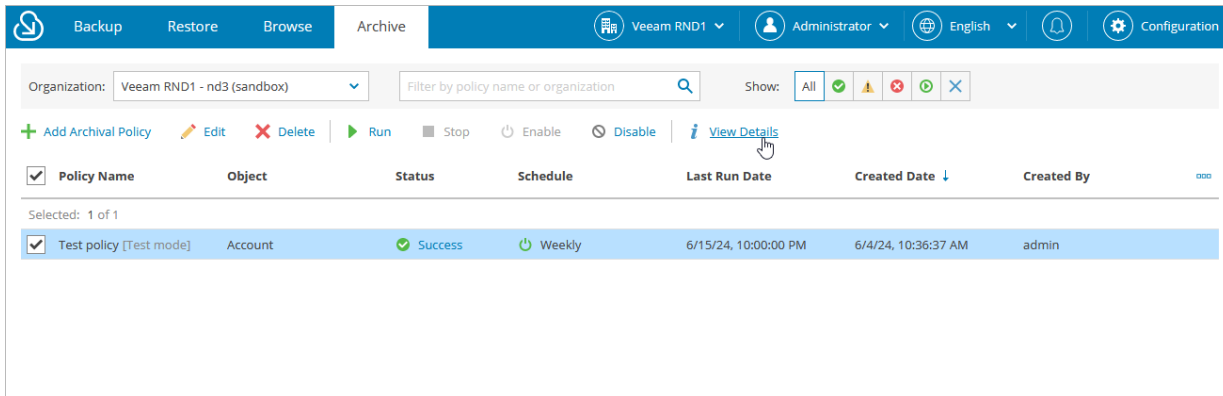
- **Policy Name** – the name of the archival policy.
- **Object** – the object that will be archived by this policy.
- **Status** – the status of the latest archival policy session.

To see all policy sessions, click the link in the **Status** column. For more information, see [Viewing Archival Policy Sessions](#).

- **Schedule** – the name or status of the schedule configured for the archival policy.
- **Last Run Date** – the date and time when the latest archival policy session started.
- **Created by** – the name of a user that created the archival policy.
- **Created Date** – the date and time when the archival policy was created.

## TIP

You can view settings configured for a specific archival policy. To do that, select the necessary archival policy and click **View Details**.



The screenshot shows the Veeam Backup for Salesforce interface. At the top, there are navigation tabs: Backup, Restore, Browse, and Archive. The Archive tab is active. Below the tabs, there is a header bar with the organization name 'Veeam RND1 - nd3 (sandbox)', a search filter, and a 'Show:' dropdown menu with icons for All, Success, Warning, Error, and Refresh. Below the header, there is a toolbar with buttons for Add Archival Policy, Edit, Delete, Run, Stop, Enable, Disable, and View Details. The main area contains a table with the following columns: Policy Name, Object, Status, Schedule, Last Run Date, Created Date, and Created By. The table shows one policy: 'Test policy [Test mode]' with Object 'Account', Status 'Success', Schedule 'Weekly', Last Run Date '6/15/24, 10:00:00 PM', Created Date '6/4/24, 10:36:37 AM', and Created By 'admin'.

Policy Name	Object	Status	Schedule	Last Run Date	Created Date	Created By
Test policy [Test mode]	Account	Success	Weekly	6/15/24, 10:00:00 PM	6/4/24, 10:36:37 AM	admin

# Viewing Archival Policy Sessions

For each performed archival operation, Veeam Backup for Salesforce starts a new session according to the created archival policies, and stores the session details in the product database. You can track real-time statistics of all running and completed operations on the **Archive** tab. To view the full list of tasks executed during an operation, click the link in the **Status** column.

The **Archival Sessions** section of the **Archive** tab displays information on all sessions of the archival policy. Each session is described with the following set of properties:

- **Session ID** – the ID assigned to the session.
- **Test Run** – the indication whether the policy was launched in the [test mode](#).
- **Start Date** – the date and time when the session started.
- **Finish Date** – the date and time when the session ended.
- **Status** – the current status of the session.
- **Processed Objects** – the total number of objects processed during the session.
- **API Usage** – the total number of API calls sent during the session.
- **Archived Records** – the total number of Salesforce records archived during the session.
- **Failed** – the total number of Salesforce records that Veeam Backup for Salesforce failed to process.
- **Result** – the explanation why Veeam Backup for Salesforce failed to process the records (applies only to sessions with the *Warning* and *Error* statuses).

The **Session Details** section of the **Archive** tab displays information on all objects included in a specific policy session. Each object is described with the following set of properties:

- **Object / Event** – the name of the archived object.
- **Parent Object** – the name of a parent object to which the archived object is linked (if any).
- **Start Time** – the date and time when Veeam Backup for Salesforce started a new task to process the object.
- **Status** – the current status of the task.
- **API Usage** – the total number of API calls sent during the task.
- **Archived Records** – the total number of Salesforce records archived during the task.
- **Failed** – the total number of Salesforce records that Veeam Backup for Salesforce failed to process.

- **Result** – the explanation why Veeam Backup for Salesforce failed to process the records (applies only to tasks with the *Warning* and *Error* statuses).

## TIP

If you want to view logs of a specific archival session, select the session and click **Download Logs**. Veeam Backup for Salesforce will collect the session logs and save them as a single .ZIP archive to the default download folder on the local machine.

The screenshot displays the Veeam Backup for Salesforce interface. At the top, there is a navigation bar with tabs for Backup, Restore, Browse, and Archive. The current view is 'Test Archiving' for an 'Account'. Below the navigation bar, there is a section for 'Archival Session' with a 'Show:' filter set to 'All' and buttons for 'Stop', 'View Details', and 'Start Restore'. There are also links for 'Export to CSV' and 'Download Logs'. A table lists the archival sessions:

Session ID ↓	Test Run	Start Date	Finish Date	Status	Result	Processed...	API Usage	Archived ...	Failed
1	Yes	7/5/24, 12:...	7/5/24, 12:...	Success	—	0	0	4	0

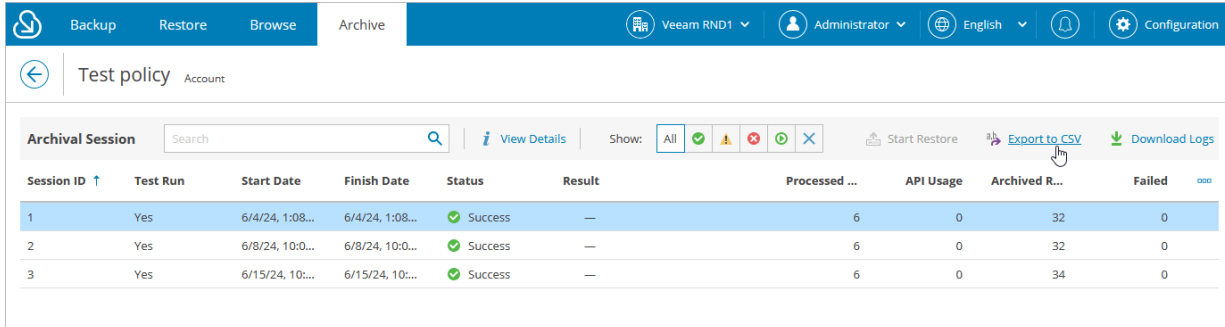
Below the archival session table is a section for 'Session Details' with a search box for 'Object / Event' and a 'Show:' filter set to 'All'. A table lists the session details:

Object / Event	Parent Object	Start Time ↓	Status	Result	API Usage	Archived Reco...	Failed
Opportunity	—	7/5/24, 12:14:2...	Success	—	0	2	0
Account	—	7/5/24, 12:14:1...	Success	—	0	2	0



# Collecting Archived Data

You can export the list that contains all fields of the archived records as a single .CSV file. To do that, navigate to the **Archive** tab and click **Export to CSV**. Veeam Backup for Salesforce will save the file with the exported data to the default download folder on the local machine.



The screenshot shows the Veeam Backup for Salesforce interface. The top navigation bar includes 'Backup', 'Restore', 'Browse', and 'Archive' (which is selected). The user is logged in as 'Administrator' and the language is set to 'English'. The main content area is titled 'Test policy Account'. Below the title, there is a search bar and a 'View Details' link. A 'Show:' dropdown is set to 'All'. Action buttons include 'Start Restore', 'Export to CSV' (highlighted with a mouse cursor), and 'Download Logs'. Below this is a table of archival sessions.

Session ID ↑	Test Run	Start Date	Finish Date	Status	Result	Processed ...	API Usage	Archived R...	Failed
1	Yes	6/4/24, 1:08...	6/4/24, 1:08...	Success	—	6	0	32	0
2	Yes	6/8/24, 10:0...	6/8/24, 10:0...	Success	—	6	0	32	0
3	Yes	6/15/24, 10:...	6/15/24, 10:...	Success	—	6	0	34	0

# Updating Veeam Backup for Salesforce

Veeam Backup for Salesforce allows you to check for new product versions and available package updates, download and install them right from the Web UI.

To view the product details:

1. Switch to the **Configuration** page.
2. Navigate to **About**.

The **About** section displays the currently installed version of Veeam Backup for Salesforce.

It is recommended that you timely install available updates to avoid performance issues while working with the product. For example, timely installed security updates may help you prevent potential security issues and reduce the risk of compromising sensitive data.

## In This Section

- [Upgrading Veeam Backup for Salesforce](#)
- [Checking for Updates](#)
- [Installing Updates](#)
- [Viewing Updates History](#)

# Upgrading Veeam Backup for Salesforce

You can upgrade from Veeam Backup for Salesforce 1.0 and 2.0 to Veeam Backup for Salesforce 3.0 using the Veeam updater service as described in section [Installing Updates](#). Veeam Backup for Salesforce will automatically notify you about the newly released product version.

After you upgrade to Veeam Backup for Salesforce 3.0, consider the following:

- The domain name or IP address of the management server displayed on the **About > Advanced Settings** tab of the **Configuration** page must match the Callback URL specified in the [Connected App settings](#). To change the domain name or IP address, modify the `backend.domain` parameter value. For more information on the advanced settings, see [Configuring Advanced Settings](#).
- Veeam Backup for Salesforce 3.0 supports API version 60.0, while Veeam Backup for Salesforce 2.0 supported API version 57.0. The API version is automatically updated upon the product upgrade. To see the supported API version, check the `sf.api.version` parameter value as described in section [Configuring Advanced Settings](#).
- If you have previously added a Salesforce Sandbox organization to Veeam Backup for Salesforce 1.0 but no backups have been created for this organization yet, you must delete this organization from Veeam Backup for Salesforce 3.0 and add it again. Otherwise, the product will fail to reauthorize the connection to the organization.
- If you previously did not have the product installed, Veeam Backup for Salesforce 3.0 will store backed-up data in the `/opt/vbsf/data` folder. However, if you upgrade from version 1.0 to 3.0, Veeam Backup for Salesforce will store the data in the folder that has already been used in version 1.0 – that is, the `/opt/vbsf/vbsf-backup/data` folder. If you want to change the folder after upgrading the product, modify the `data.storage.location` parameter value as described in section [Configuring Advanced Settings](#).

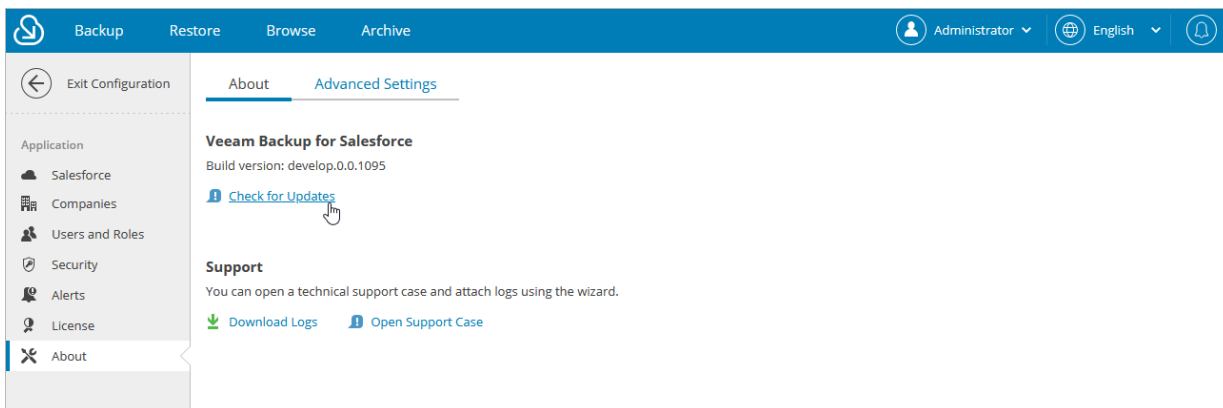
For more information on the issues that you may encounter while upgrading the product, see the [Veeam Backup for Salesforce Release Notes](#).

# Checking for Updates

Veeam Backup for Salesforce automatically notifies you about newly released product versions and package updates available for the operating system running on the Veeam Backup for Salesforce server. However, you can check for available updates manually if required:

1. Switch to the **Configuration** page.
2. Navigate to **About**.
3. In the **Veeam Backup for Salesforce** section, click **Check for Updates**.

If new updates are available, they will be displayed on the **Updates** tab of the **Veeam Updater** page. To view detailed information on an update, select the check box next to the update and click **What's new?**.



# Installing Updates

Use the Veeam updater service to download and install new product versions and available package updates . You can also [set a reminder to send update notifications](#)

## IMPORTANT

Veeam Backup for Salesforce does not allow you to schedule the update installation as it may cause interrupting of running activities, which may result in unpredictable data loss. It is recommended that you make sure that all backup policies are disabled and restore jobs are finished before you install a product update.

## Installing Updates

To download and install available product and package updates:

1. Open the **Veeam Updater** page. To do that:
  - a. Switch to the **Configuration** page.
  - b. Navigate to **About**.
  - c. In the **Veeam Backup for Salesforce** section, click **Check for Updates**.
2. On the **Veeam Updater** page, do the following:
  - a. In the **Updates are available for this system** section, select check boxes next to the necessary updates.
  - b. In the **Choose action** section, select the **Install updates now** option, select the **Reboot automatically after install if required** check box to allow Veeam Backup for Salesforce to reboot the server if needed, and then click **Install Updates Now**.

Veeam Backup for Salesforce will download and install the updates; the results of the installation process will be displayed on the **History** tab. Keep in mind that it may take several minutes for the installation process to complete.

## NOTE

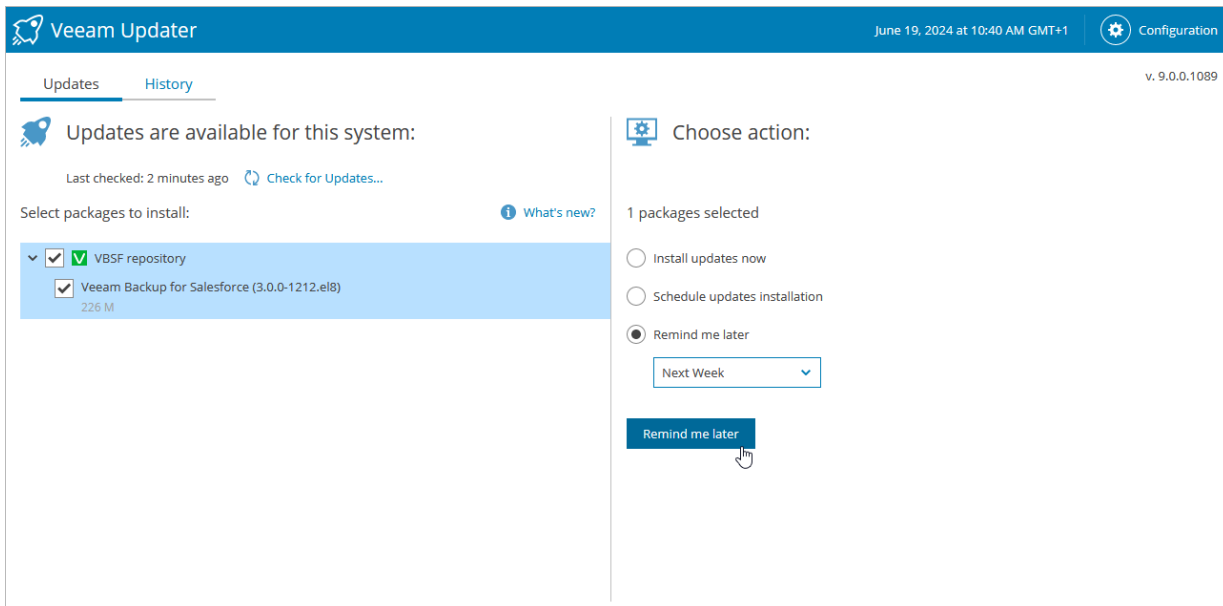
When installing product updates, Veeam Backup for Salesforce restarts all services running on the management server, including the Web UI service. That is why Veeam Backup for Salesforce will log you out when the update process completes.

# Setting Update Reminder

If you have not decided when to install updates, you can set an update reminder – instruct Veeam Backup for Salesforce to send an update notification later.

To do that, on the **Veeam Updater** page, in the **Choose action** section, do the following:

1. Select the **Remind me later** option and choose when you want to receive the reminder.  
If you select the **Next Week** option, Veeam Backup for Salesforce will send the reminder in 7 days.
2. Click **Remind me later**.



# Viewing Updates History

To see the results of the update installation performed on the management server, do the following:

1. Switch to the **Configuration** page.
2. Navigate to **About**.
3. In the **Product updates** section, click **Check for Updates**.
4. On the **Veeam Updater** page, switch to the **History** tab.

For each date when an update was installed, **Veeam Updater** will display the name of the update and its status (whether the installation process completed successfully, completed with warnings or failed to complete).

To download logs for the installed updates, select the necessary date in the **Date** section, and click **View Full Log**. Veeam Backup for Salesforce will save the logs as a single file to the default download directory on the local machine.

The screenshot shows the Veeam Updater interface. At the top, there is a blue header with the Veeam logo and the text 'Veeam Updater' on the left, and the date and time 'September 19, 2024 at 03:56 PM GMT+4' on the right. Below the header, there are two tabs: 'Updates' and 'History', with 'History' being the active tab. The main content area is divided into two sections. On the left, there is a section titled 'Update sessions history' with a clock icon. Below this title, there is a table with a 'Date' column and an upward arrow. A single row is highlighted in light blue, showing the date 'September 19, 2024 at 12:41 PM'. On the right, there is a section titled 'View Full Log' with a document icon. Below this title, there is a table with two columns: 'Package' and 'Status'. The table contains three rows of log entries, each with a green checkmark in the status column.

Date ↑	Package	Status
September 19, 2024 at 12:41 PM	Preparing for the update operation	Success
	Veeam Backup for Salesforce (3.0.0-3955.el7)	Success
	Update operation has been completed	Success

# Getting Technical Support

If you have any questions or issues with Veeam Backup for Salesforce, you can search for a resolution on [Veeam R&D Forums](#) or submit a support case in the [Veeam Customer Support Portal](#).

When you submit a support case, it is recommended that you provide the Veeam Customer Support Team with the following information:

- [Version information for the product and its infrastructure components](#)
- The error message or an accurate description of the problem you are facing
- [Log files](#)

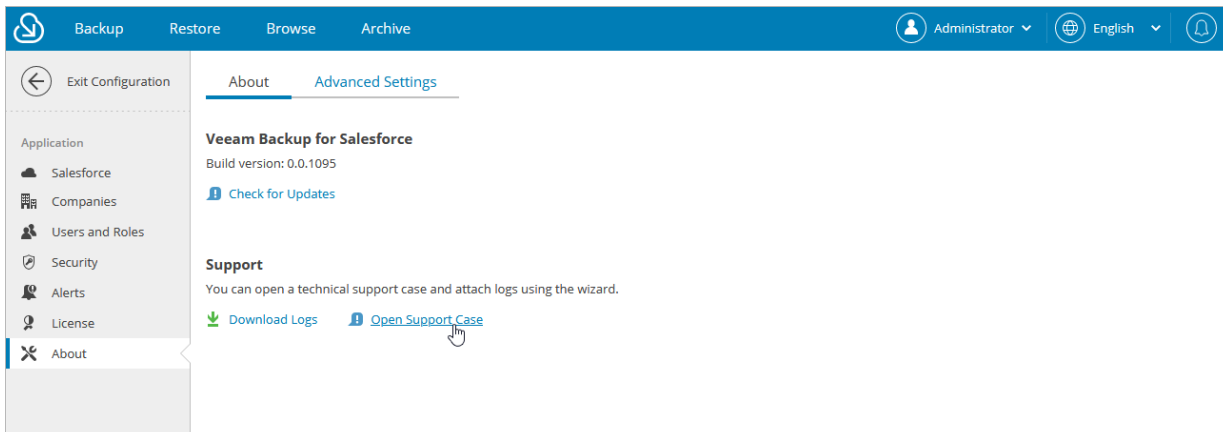
## Opening Support Case

To open a support case:

1. Switch to the **Configuration** page.
2. Navigate to **About**.
3. In the **Support** section, click **Open Support Case**.

### NOTE

It is recommended that you open only support cases related to the Veeam Backup for Salesforce specific issues from the Web UI. For general and license issues, use the [Veeam Customer Support Portal](#).





# Downloading Product Logs

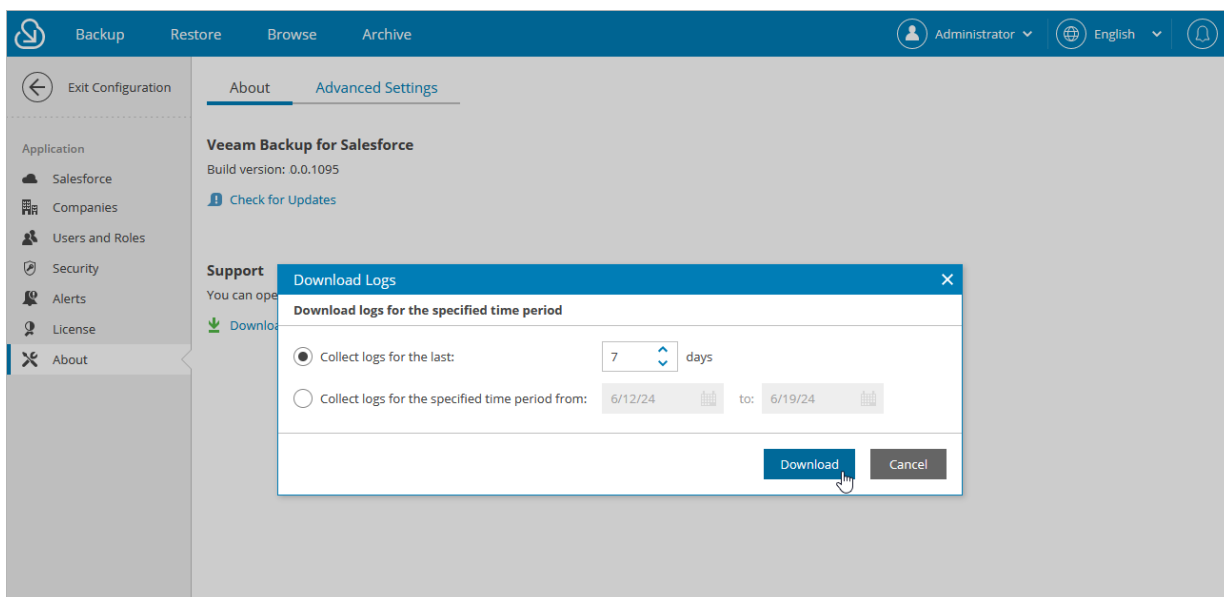
To download the product logs, do the following:

1. Switch to the **Configuration** page.
2. Navigate to **About**.
3. In the **Support** section, click **Download Logs**.
4. In the **Download Logs** window, specify a time interval for which logs must be collected:
  - Select the **Collect logs for the last** option if you want to collect data for a specific number of days in the past.
  - Select the **Collect logs for the specified time period** option if you want to collect data for a specific period of time in the past.
4. Click **Download**.

Veeam Backup for Salesforce will collect logs for the specified time interval and save them to the default download folder on the local machine in a single `log.zip` archive.

## NOTE

Product logs are available only to users with the *Administrator* role assigned. However, all users can download backup or restore session logs. To learn how to download these logs, see sections [Viewing Policy Sessions](#) and [Viewing Restore Sessions](#).



# Appendices

See in this section:

- [Appendix A. Unsupported Objects](#)
- [Appendix B. Replacing Security Certificate](#)

# Appendix A. Unsupported Objects

Veeam Backup for Salesforce supports backup of objects available in API version 60 and earlier. However, most of the objects that cannot be restored are not collected. You can tell these objects in Salesforce by the following flags assigned: *creatable = false, updatable = false*. The only exception is that backup of the **\*History** objects is supported. For more information on backup and restore limitations, see [Considerations and Limitations](#).

Operation	Unsupported Objects
Backup	*_b, *_ViewStat, *_VoteStat, *_x, *_hd, *_ChangeEvent, *_VersionHistory, *Event, *EventStream, *Feed, AccountUserTerritory2View, ActivityMetric, ActivityMetricRollup, AggregateResult, AnalyticsBotSession, AnlytDataAssetEventStore, ApexEmailNotification, ApexPageInfo, ApexTestQueueItem, ApexTestResult, ApexTestResultLimits, ApexTestRunResult, ApexTestSuite, AppTabMember, AuraDefinitionInfo, BackgroundOperationResult, BotAnalytics, BotEventLog, BulkApiResultEventStore, CleanDataService, CollaborationGroupRecord, ColorDefinition, ContentFolderItem, ContentFolderMember, ContentHubItem, DatacloudAddress, DatacloudCompany, DatacloudContact, DatacloudDandBCompany, DatacloudSocialHandle, DataStatistics, DataType, DcSocialProfile, DcSocialProfileHandle, EmbeddedServiceLabel, EngagementHistory, EntityDefinition, EntityParticle, FieldDefinition, FieldHistoryArchive, FlexQueueItem, FlowDefinitionView, FlowVariableView, FlowVersionView, IconDefinition, Idea, IdeaComment, IdeaReputation, IdeaReputationLevel, IdeaTheme, InstalledPackage, InterfaceFieldMapping, ListViewChartInstance, ManagedCintentType, NetworkUserHistoryRecent, OAuthToken, OmniRoutingEventStore, OutgoingEmail, OutgoingEmailRelation, OwnerChangeOptionInfo, PermissionSetEventS, PicklistValueInfo, PlatformAction, RecentlyViewed, RecordActionHistory, RecordRecommendation, RecordVisibility, Regular_articles_kav, RelationshipDomain, RelationshipInfo, SalesStore, SearchLayout, SiteDetail, SubscriberPackage, TenantUsageEntitlement, UserAppMenuItem, userEmailCalendarSync, UserEntityAccess, UserFieldAccess, UserProfileFeed, UserRecordAccess, Vote
Archive	*History, *Share, *Tag, AccountPartner, ContentNote, ContentFolder, MailmergeTemplate, MobileApplicationDetail, OpportunityPartner, Organization, Profile, RecordType, SelfServiceUser, User, standard Salesforce objects that cannot be deleted through API.

# Appendix B. Replacing Security Certificate

When you install Veeam Backup for Salesforce, it automatically generates a default self-signed certificate. You can replace this default certificate with your own self-signed certificate or with a certificate obtained from a Certificate Authority (CA).

The `/etc/nginx/certs` default SSL configuration file contains paths to the following certificate files:

- `ssl_certificate "/opt/vbsf/nginx/certificate/vbsf.crt"` – a file that contains the self-signed certificate.
- `ssl_certificate_key "/opt/vbsf/nginx/certificate/vbsf.key"` – a file that contains a private key used to generate the certificate.
- `ssl_password_file "/opt/vbsf/nginx/certificate/passout"` – a file that contains a password to decrypt the private key. This file is not required if the private key is not encrypted.

## Installing SSL Certificate on Nginx Server

To replace the default certificate, do the following:

1. Log in to the machine where Veeam Backup for Salesforce is installed.
2. Upload new SSL certificate files to the `/opt/vbsf/nginx/certificate/` folder.
3. Set the `vbsf` user as the owner of the new files and add these files to the `vbsf` group. To do that, run the command:

```
sudo chown vbsf:vbsf /opt/vbsf/nginx/certificate/*
```

4. Update the configuration parameters in the `/etc/nginx/certs` configuration file specifying the paths to the new certificate files:

```
ssl_certificate "<path_to_the_new_file>";  
ssl_certificate_key "<path_to_the_new_file>";  
ssl_password_file "<path_to_the_new_file>";
```

If the private key is not encrypted, remove the password line from the `/opt/vbsf/nginx/certificate/passout` file.

5. Restart the `nginx` service. To do that, run the command:

```
sudo systemctl restart nginx
```

To learn how to create and configure your own certificate, see documentation of the relevant SSL providers (for example, [Digicert documentation](#)).