Veeam Backup for Salesforce

Version 2.0

User Guide

January, 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

CONTACTING VEEAM SOFTWARE 6
OVERVIEW 7
SOLUTION ARCHITECTURE 8
PLANNING AND PREPARATION 10
System Requirements 11
Ports 14
Permissions 15
Considerations and Limitations 17
Sizing and Scalability Guidelines 18
PostgreSQL 19
Log Storage 21
File Storage 21
LICENSING 22
Installing and Removing License 24
Viewing License Information 26
DEPLOYMENT 27
Installing Veeam Backup for Salesforce on RedHat, Oracle and CentOS Machines 28
Installing Veeam Backup for Salesforce on Ubuntu Machines 32
Performing Initial Configuration 36
Step 1. Accept License Agreement 37
Step 2. Create Local Administrator 38
Step 3. Connect to Database 39
Step 4. Provide License File 41
Step 5. Create Connected App 42
Step 6. Connect to Salesforce 44
Step 7. Set Backup Policy Schedule 46
Step 8. Finish Working with Wizard 47
ACCESSING VEEAM BACKUP FOR SALESFORCE 48
CONFIGURING VEEAM BACKUP FOR SALESFORCE 49
Managing Salesforce Organizations 50
Adding Organizations 51
Editing Organizations 52
Removing Organizations 57
Managing Companies 58
Adding Companies 58
Editing Companies 59
Removing Companies 60

Managing Databases....62
Adding Databases....62
Editing Database Connections....64
Removing Databases....65
Managing Users....66
User Roles and Permissions....67
Adding Users....69
Editing Users....71
Removing Users....73
Configuring Security Settings....74
Changing Connected App Tokens....75
Configuring IdP and SSO Settings....77
Viewing Audit Trail....81
Managing Alerts....82
Configuring Notification Settings....83
Creating Alerts....86
Editing Alerts....88
Configuring Advanced Settings....89
PERFORMING SALESFORCE BACKUP....92
Creating Backup Policies....93
Step 1. Launch Add Backup Policy Wizard....94
Step 2. Configure Connection to Salesforce Organization....95
Step 3. Configure Backup Settings....97
Step 4. Enable Backup of Files and Attachments....103
Step 5. Configure Retention Settings....104
Step 6. Finish Working with Wizard....106
Starting and Stopping Backup Policies....107
Disabling and Enabling Backup Policies....108
Editing Backup Policies....109
Removing Backup Policies....110
Viewing Backup Policy Details....111
Viewing Policy Sessions....112
VIEWING BACKED-UP DATA....115
PERFORMING SALESFORCE RESTORE....117
Creating Restore Jobs....118
Restoring Records....119
Restoring Field Values....133
Restoring Files....144
Restoring Metadata....151
Starting and Stopping Restore Jobs....159

Cloning and Editing Restore Jobs....160
Removing Restore Job Drafts....162
Configuring Restore Mapping Settings....163
Viewing Restore Job Details....165
Viewing Restore Sessions....166
UPDATING VEEAM BACKUP FOR SALESFORCE....167
Upgrading Veeam Backup for Salesforce....168
Checking for Updates....169
Installing Updates....170
Viewing Updates History....172
GETTING TECHNICAL SUPPORT....173
APPENDICES....175
Appendix A. Unsupported Objects....175
Appendix B. Replacing Security Certificate....179

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
- Veeam R&D Forums: forums.veeam.com

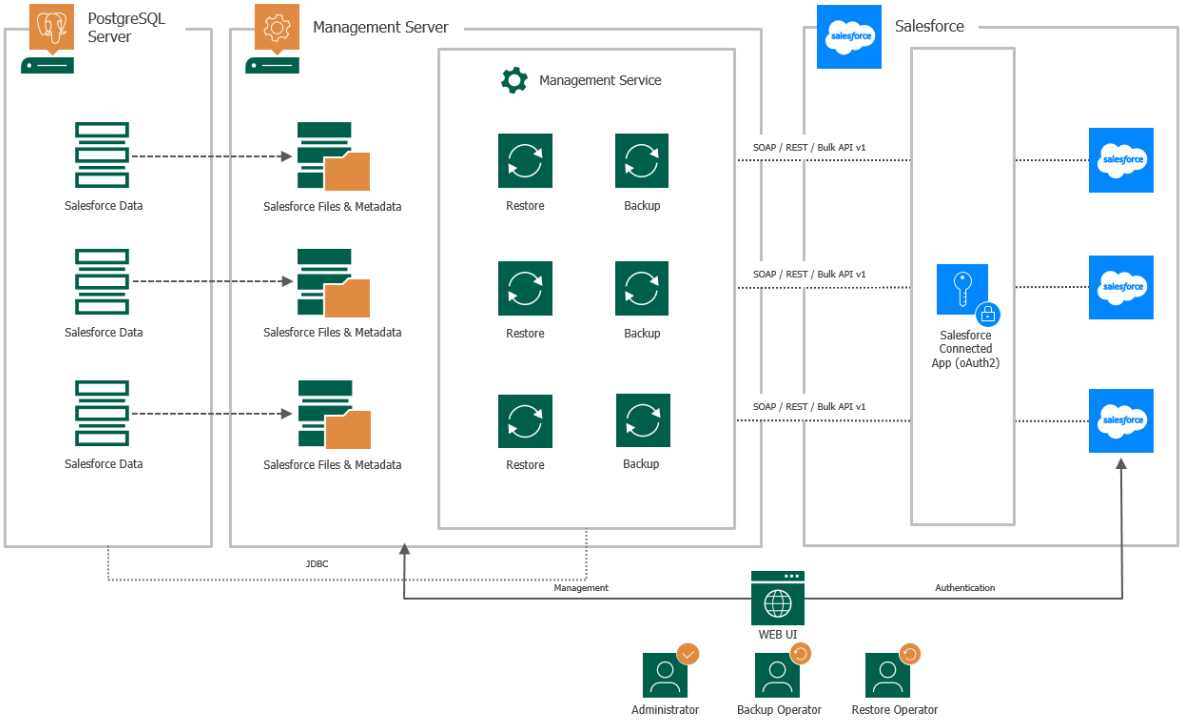
Overview

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

- Run your backup environment anywhere: on-premises, in AWS, Microsoft Azure and so on.
- Manage backup and restore operations for multiple Salesforce organizations.
- Back up Salesforce files, data and metadata.
- Back up Salesforce files as often as every 5 minutes.
- Restore files, data and metadata including object hierarchies and custom fields.
- Configure granular backup schedules and retention settings at the object level.
- Compare different versions of Salesforce records and metadata.
- Create real-time alerts for backup, recovery, licensing and connection issues.
- Control access to the product functionality with the help of user roles and scopes.
- Use Azure Active Directory (AD) or Salesforce as a single sign-on (SSO) provider to log in the product Web UI.

Solution Architecture

This section provides information on the Veeam Backup for Salesforce architecture and its components.



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/logs/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.

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	**CPU**: 4 cores (minimum) **Memory**: 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. **Free space**: 100 GB (minimum), excluding file and log storage space. For file storage space requirements, see File Storage. For log storage space requirements, see Log Storage. **Network bandwidth**: 10 Mbps (minimum) **Note**: To improve performance of the management server, it is recommended that you use SSDs for databases and file storage.
OS	• CentOS 7 (centos-release-7-9.2009.1.el7.centos.x86_64 and later) • RedHat Linux 7, 8 • Oracle Linux 7, 8 • AlmaLinux 8.8 • Rocky Linux 8.8 • Ubuntu 20.04 LTS, 22.04 LTS **Note**: Starting from version 2.1, Veeam Backup for Salesforce can be installed on a machine running the AlmaLinux 8.8 or Rocky Linux 8.8 operating system. However, this support is experimental. For more information, see this Veeam KB article.

PostgreSQL Servers

Specification	Requirement
Hardware	**CPU**: 4 cores (minimum) **Memory**: 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. **Free space**: 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 Sizing and Scalability Guidelines. To learn how to monitor your data storage and used file space in the Salesforce database, see Salesforce Documentation. **Note**: To improve performance of PostgreSQL servers, it is recommended that you use SSDs on the machines running the servers.
Software	PostgreSQL 12, 13, 14 (recommended), 15 **Note**: PostgreSQL 15 is experimentally supported in Veeam Backup for Salesforce version 2.1 and later. For more information on experimental support, see this Veeam KB article.

File Storage

Specification	Requirement
Hardware	Veeam Backup for Salesforce stores file data and metadata in the `/opt/vbsf/data` 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. Make sure that you provide your file storage with enough space taking into account the total size of the files used in the Salesforce database and your daily change rate. To view the amount of space used by your files, open the Salesforce UI, navigate to **Setup** > **Company Information** and check the **Used File Space** field. **Note**: To improve performance of the management server, it is recommended that you use SSDs for the file storage.

Log Storage

Specification	Requirement
Hardware	Veeam Backup for Salesforce stores its logs in the `/var/logs/vbsf/` 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 Sizing and Scalability Guidelines.

Salesforce

Specification	Requirement
Salesforce API	By default, Veeam Backup for Salesforce 2.0 uses Salesforce API version 57.0. Any objects available in later API versions will not be discovered and protected by the product. **Note**: You can change the API version used by the product as described in section Configuring Advanced Settings.

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

Salesforce User	Veeam Backup for Salesforce requires a Standard User with the *Salesforce* 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.
	
	The user whose credentials are used to authorize the connection must be assigned full permissions required to read and modify data:
	• System Administrator profile (grants broad permissions immediately, but not all the required ones).
	• Permission set that has the following permissions enabled:
	  ○ Query All Files permission to back up all files.
	  ○ View and Edit Converted Leads permission to restore converted leads.
	  ○ Permissions for all custom record types of objects to restore records of custom types.
	  ○ Set Audit Fields upon Record Creation permission to restore original values in audit fields when restoring deleted records.
	  ○ Update Records with Inactive Owners permission to restore deleted records owned by inactive users.
	  ○ Update Email Messages permission to restore attachments of email messages.
	• Permission set licenses for any managed application license that is required for accessing the data (for example, HVS, CPQ).
	• Feature-based user permissions: Marketing User, Service Cloud User, Knowledge User, Salesforce CRM Content User.
	
	For sandboxes, any managed application needs to be enabled and license provided to the user. For example, **High Velocity Sales** requires application activation.

Account	Required Permissions
Salesforce Connected App	Secure and encrypted connection to Salesforce is established using the Connected App tokens. The Connected App must be assigned the following OAuth scopes: • **Full access** (full) • **Perform requests at any time** (refresh_token, offline_access) • **Access unique user identifiers** (openid) The latter option applies only if you use Salesforce as an identity provider. For more information on OAuth scopes in Salesforce, see Salesforce Documentation. To learn how to create the app, see this Veeam KB article.

Veeam Backup for Salesforce Components

Account	Required Permissions
PostgreSQL Database User	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. **Note**: 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 Adding Databases, before you create any backup policies.

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 2.0 supports backup of all data and objects available on the Salesforce Platform if these resources can be retrieved using the Salesforce API version 57 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 personal reports and dashboards is not supported since Salesforce does not provide API to export and restore this type of data.
- Backup of encrypted field types is not supported.
- 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.
- Restore of the *MobileApplicationDetail* and *MailmergeTemplate* types of content is not supported.
- 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.

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 Salesforce.

You can use the following formula to calculate the required disk space: (*Salesforce Used Data Space * 1.6) + (Size of Added Data * Planned Period of Data Backup) + (Size of Changed Data * 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 KB / 1024 = 0.02 GB*).
- *Planned Period of Data Backup* — data is planned to be backed up daily for a period of 5 years (that is, *5 *365 days = 1825 days*).
- *Size of Changed Data* — 10,000 records of 2 KB each are changed in the Salesforce each backup cycle (that is, *10,000 * 2 KB / 1024 = 0.02 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 GB * 1.6) + (0.02 GB * 1825) + (0.02 GB * 24 * 180) = 320 GB + 36.5 GB + 86.4 GB = 443 GB*.

PostgreSQL Configuration Settings

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

Parameter	Value
max_connections	300 or more*
superuser_reserved_connections	7
shared_buffers	20% of RAM
random_page_cost	1.1
work_mem	15% of RAM
maintenance_work_mem	128 MB
max_wal_size	3 GB
min_wal_size	2 GB
checkpoint_completion_target	0.9
effective_io_concurrency	200
effective_cache_size	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 PostgeSQL 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/logs/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.
- 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* license type reported by the Salesforce platform. Only Salesforce user licenses consumed by production organizations whose data is protected are counted.

The Veeam license is not required for:

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

If the quantity of total 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 not be able to perform backup operations, and 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.

> **NOTE**
>
> Users of Salesforce sandbox organizations do not consume license units, you can protect as many sandbox organizations as you want — the total number of user licenses of sandbox organizations does not affect license usage. However, you cannot use the *Community Edition* or other license type to protect a sandbox organization if the quantity of Salesforce users in this organization exceeds the limit of licensed Users in your Veeam license.

To learn how to obtain the license, contact a Veeam sales representative at Sales Inquiry.

Grace Period

A grace period provides a short-term buffer in cases when the license renewal was delayed, the licensed User threshold was exceeded or licensing servers cannot be reached. The grace period is usually enabled once for the next 30 days starting from the violation date and automatically reset when the violation is resolved.

Installing and Removing License

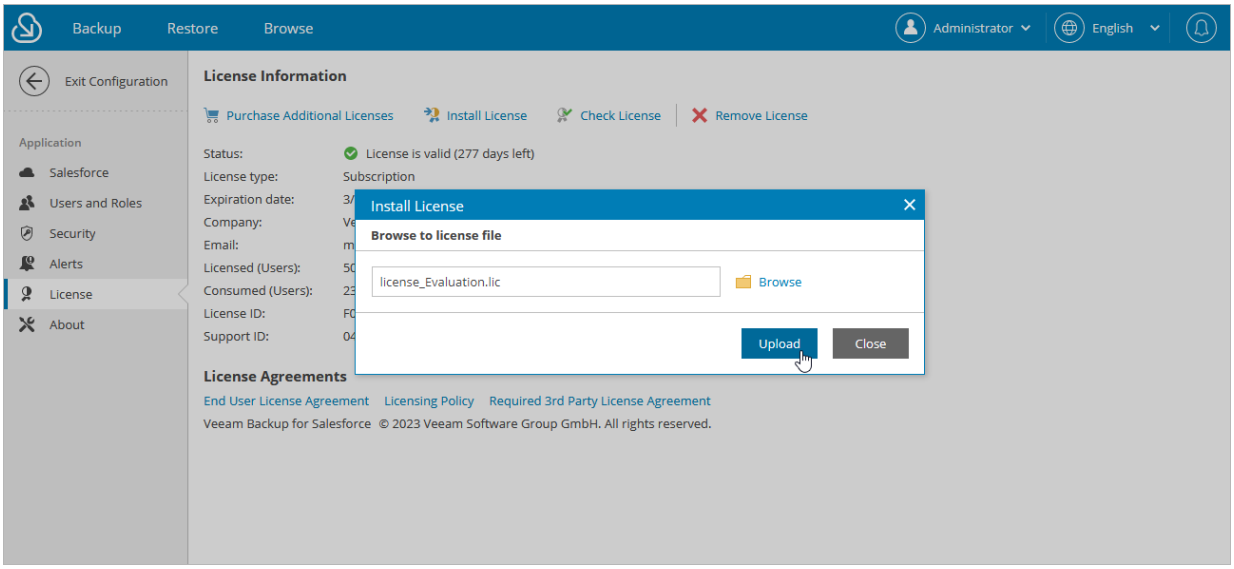
On the **License** tab, you can see the current license details, install a new license or remove the currently used license.

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:

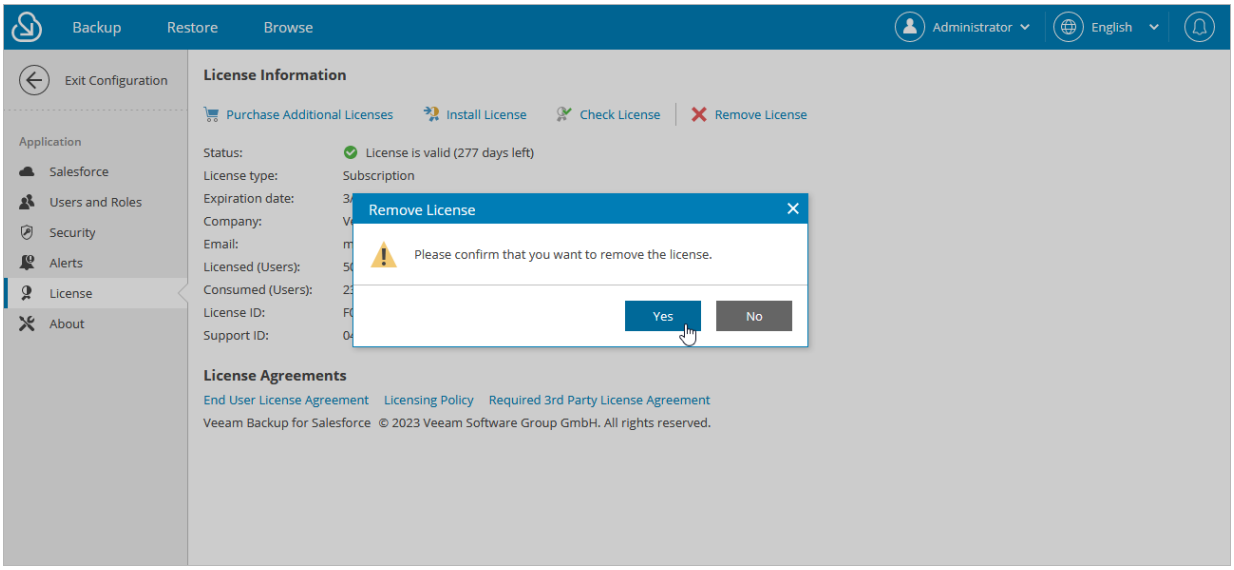
1. Switch to the **Configuration** page.
2. Navigate to **License**.
3. Click **Install License**.
4. In the **Install License** window, click **Browse** to browse to a license file, and then click **Upload**.



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

After 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.

Viewing License Information

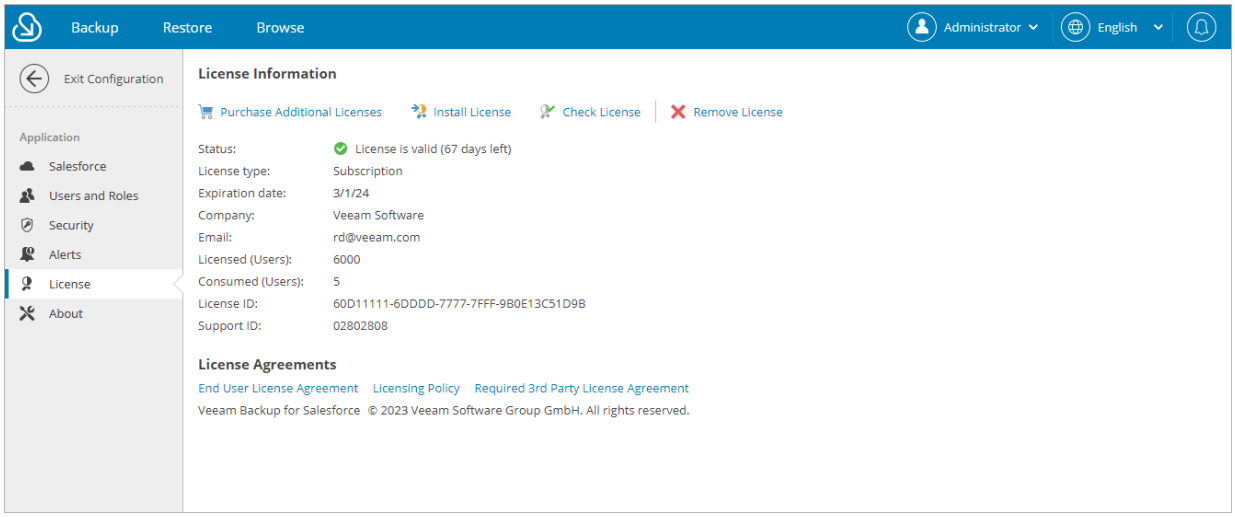
The license validity is verified by the Veeam License Server right after the installation and, then, periodically once a week. You can also verify the license manually, to do that:

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*).
- **Expiration date** – the date when the license will expire.
- **Company** – the name of a company to which the license was issued.
- **Email** – email address of the license administrator.
- **Licensed (Users)** – the total number of licensed Users.
- **Consumed (Users)** – the total number of consumed user licenses across all protected Salesforce 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
   ```

4. [Applies to CentOS 7 only] An EPEL repository must be added to allow nginx installations. To add the repository, run the following command:

   ```
   sudo yum install epel-release
   ```

   For more information on EPEL, see EPEL Documentation.

Installing Veeam Backup for Salesforce on RedHat, Oracle and CentOS Machines

You can install Veeam Backup for Salesforce on a RedHat, Oracle or CentOS 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-locale 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 --out
   put ./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-locale 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
   ```

4. Install the Veeam software repository:

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

5. 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/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, you can find the web address URL in the `/opt/vbsf/access_token.txt` file on the machine where Veeam Backup for Salesforce is installed.

7. Copy the automatically generated URL and paste it into a web browser to proceed with the initial configuration of Veeam Backup for Salesforce.

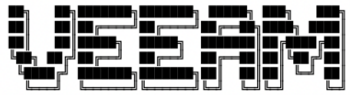
> **IMPORTANT**
>
> By default, the URL contains an IP address of the management server. If the specified IP address is not available over HTTPS, replace it with the public IP of the management server or the DNS name configured for the machine where the Veeam Backup for Salesforce is installed.

```
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-locale 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-scrip
   t.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-locale 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
   ```

4. Install the Veeam software repository:

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

5. 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/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, you can find the web address URL in the `/opt/vbsf/access_token.txt` file on the machine where Veeam Backup for Salesforce is installed.

7. Copy the automatically generated URL and paste it into a web browser to proceed with the initial configuration of Veeam Backup for Salesforce.

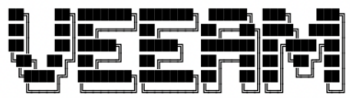
> **IMPORTANT**
>
> By default, the URL contains an IP address of the management server. If the specified IP address is not available over HTTPS, replace it with the public IP of the management server or the DNS name configured for the machine where the Veeam Backup for Salesforce is installed.

```
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.

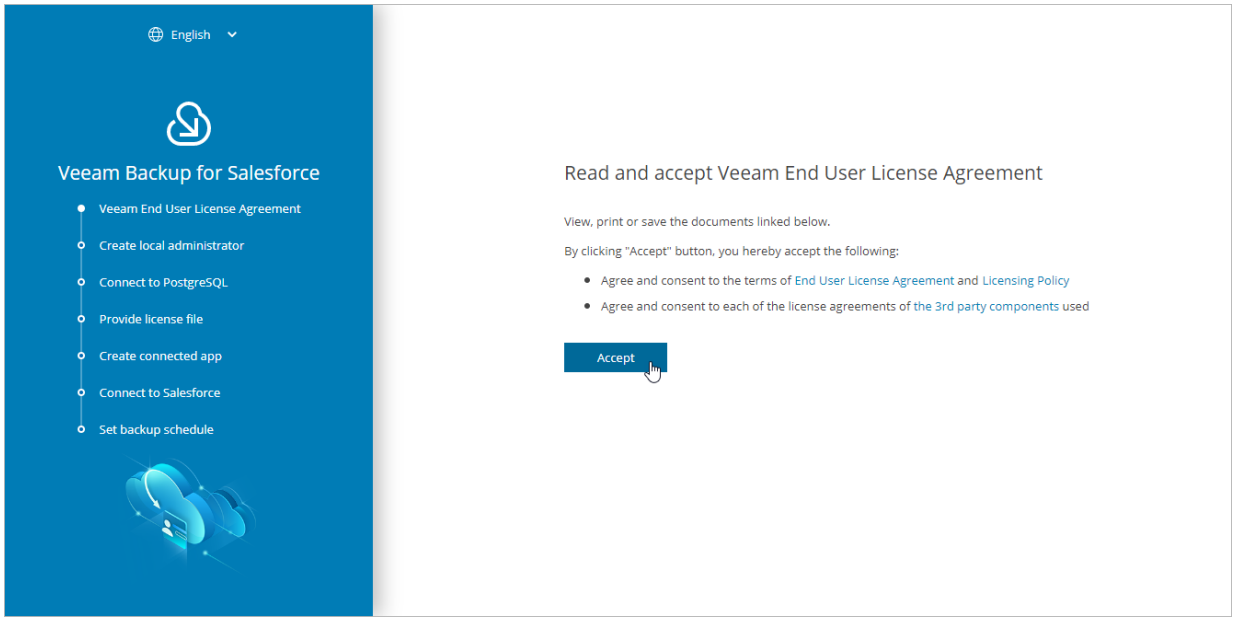
> **IMPORTANT**
>
> Consider the following:
>
> - Internet Explorer is not supported. To access Veeam Backup for Salesforce, use the latest versions of Microsoft Edge, Mozilla Firefox (except Mozilla Firefox for Linux), Safari and Google Chrome.
> - You must be able to access the Salesforce authentication 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.

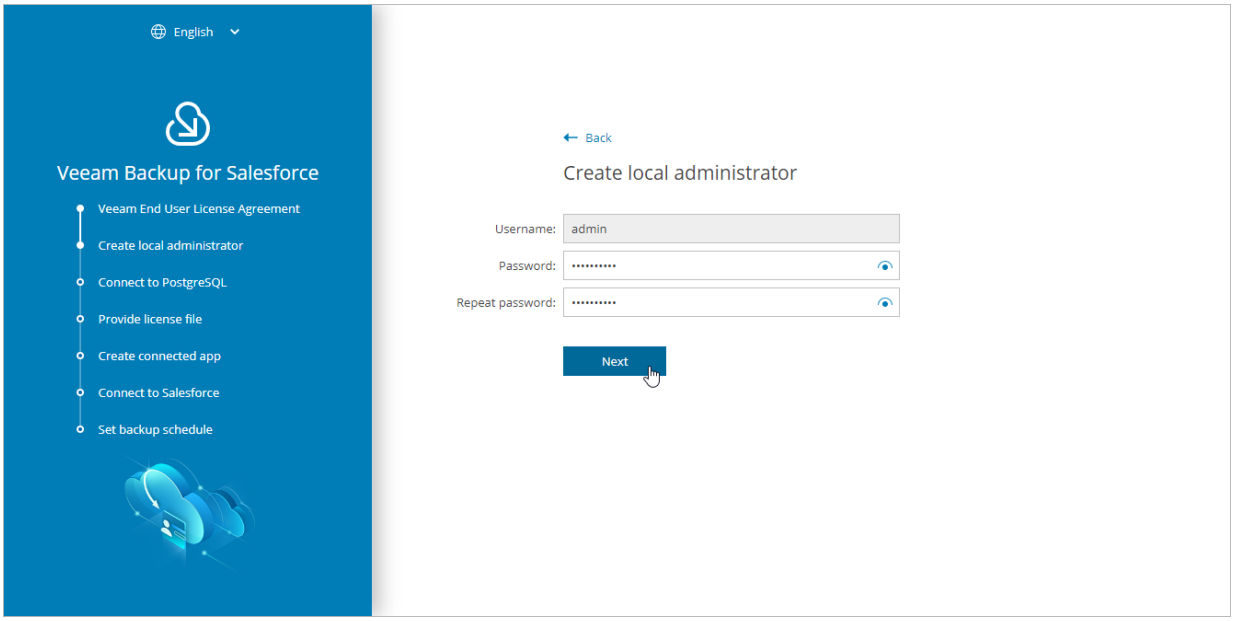


Step 2. Create Local Administrator

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.



Step 3. Connect to Database

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.

> **NOTE**
>
> If you perform configuration of the existing deployment of Veeam Backup for Salesforce, at the **Connect to PostgreSQL** step of the wizard, specify connection settings that will be used to access the existing configuration database.

To configure connection settings, do the following:

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.

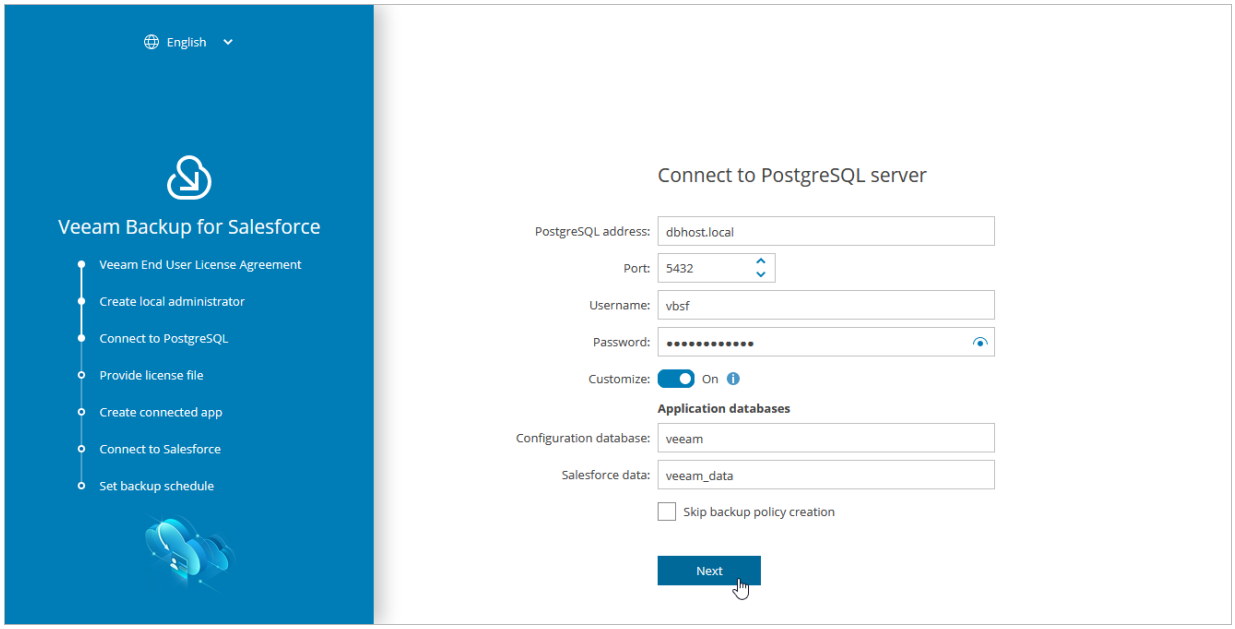
By default, Veeam Backup for Salesforce creates new databases with the following names:

- **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

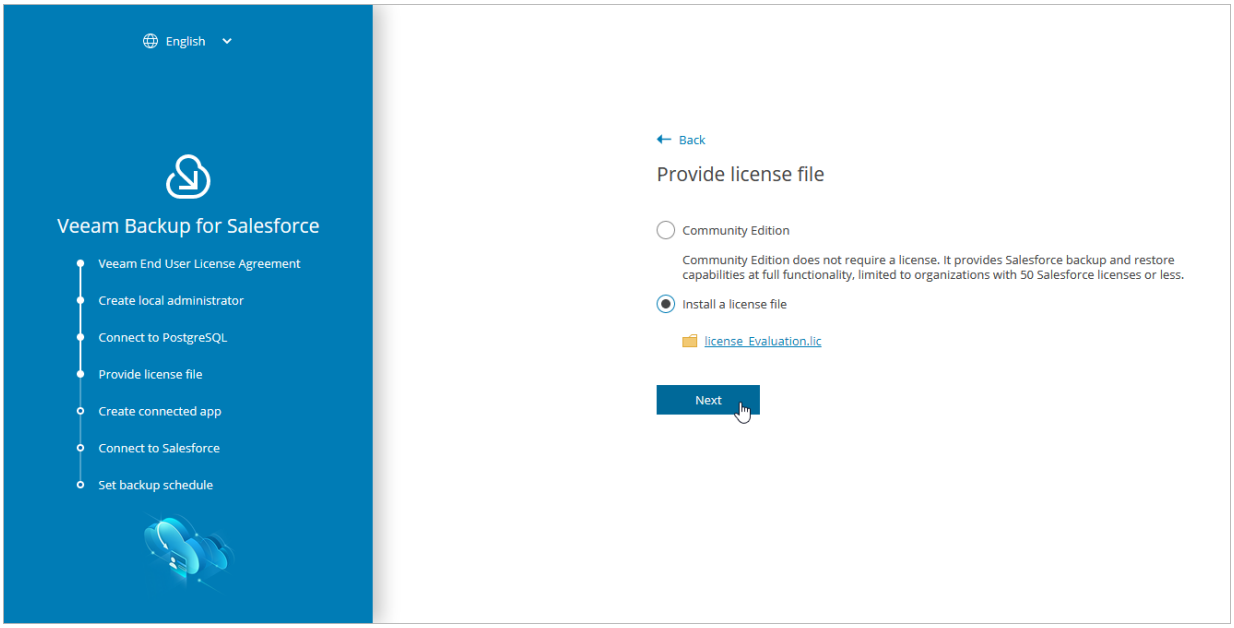
During the initial configuration, you will be prompted to connect to a Salesforce organization that will be protected by a backup policy, which is automatically created by the product. You can skip the default policy creation and connect to a database later when you create a backup policy.



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 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*.

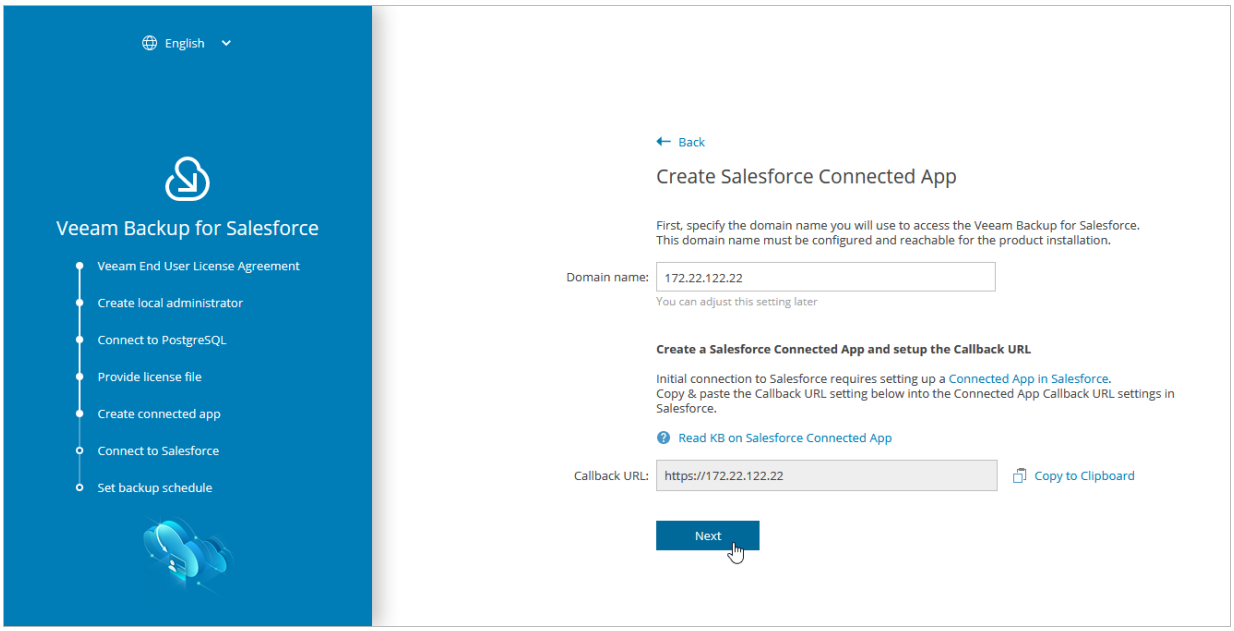
  After that, your *Callback URLs* list will contain the following URLs:

  - 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:

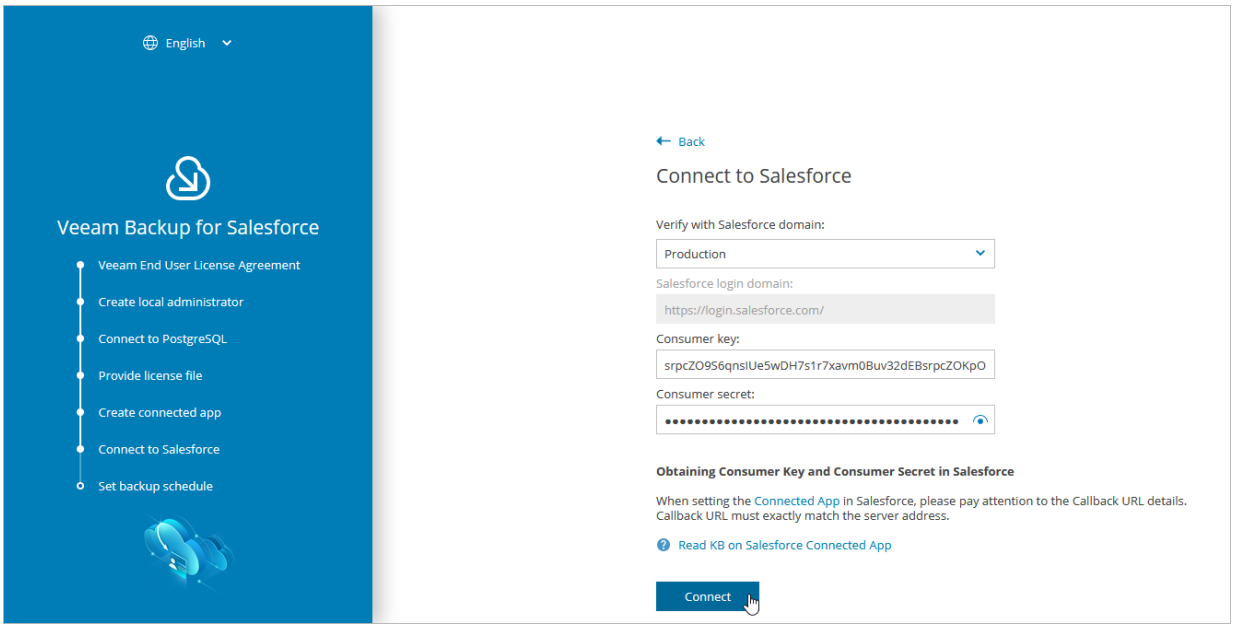
1. Choose whether you want to connect to a Salesforce organization hosted on a production instance, sandbox instance or custom domain.

   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.



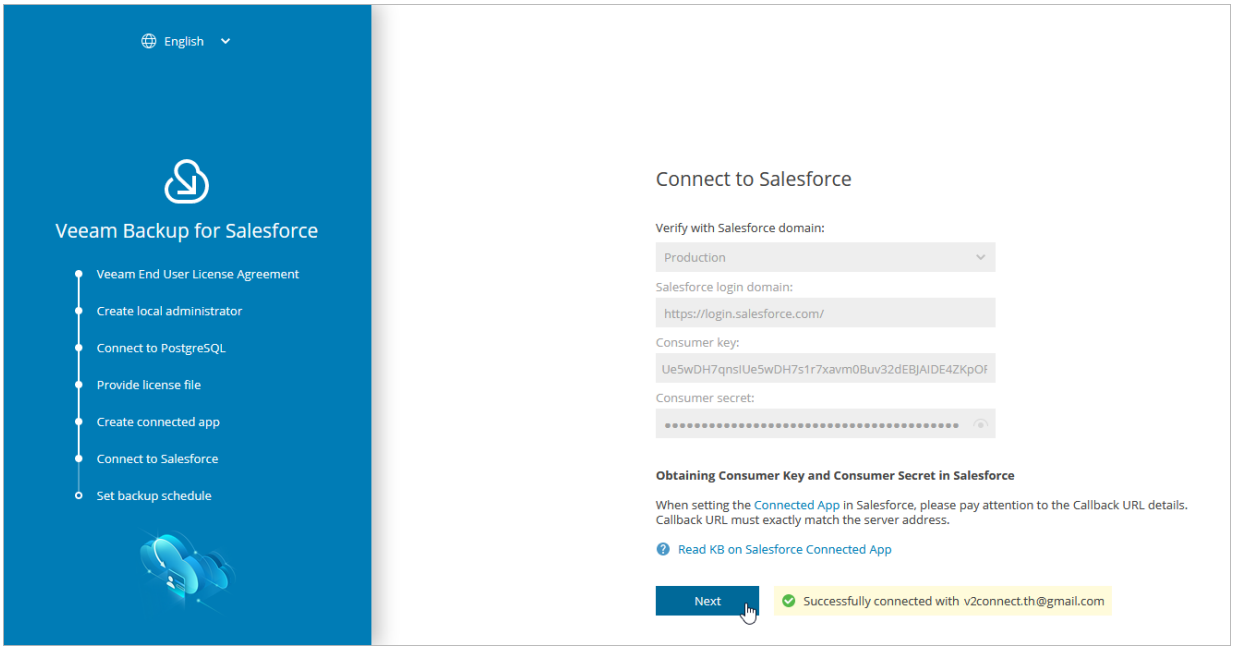
3. On the Salesforce authentication webpage, enter credentials of an account created in the Salesforce organization that you want to protect, and click **Log in**.

   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

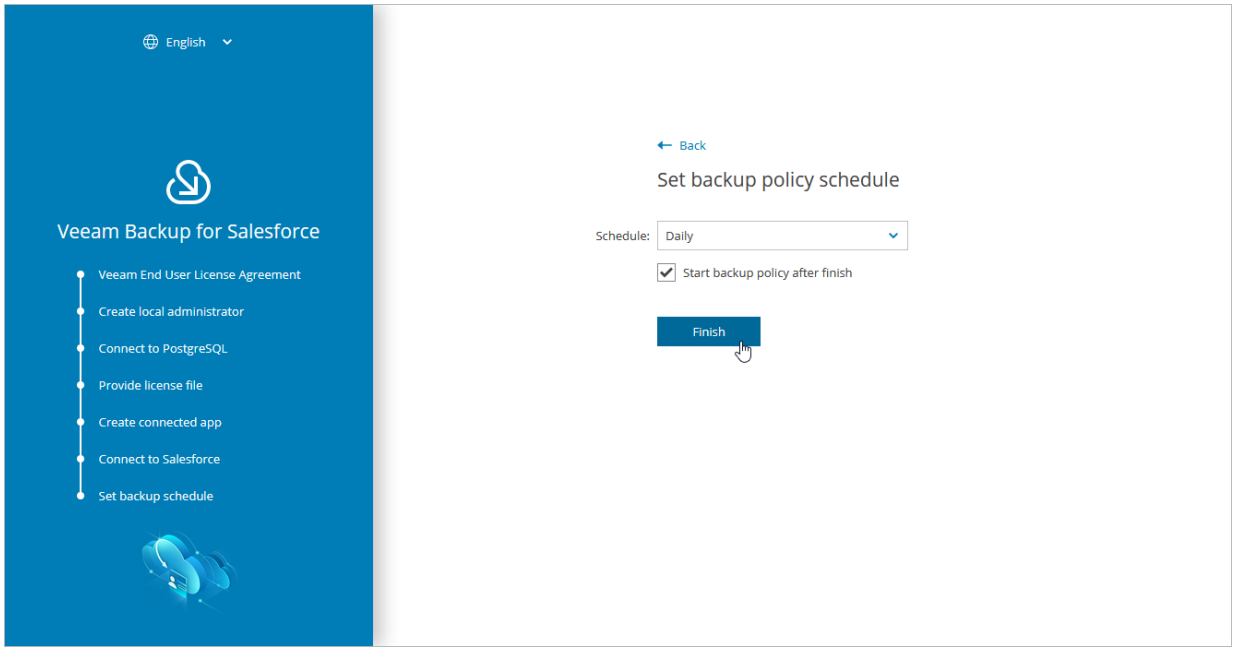
[Applies only if you have not selected the **Skip backup policy creation** check box]

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.

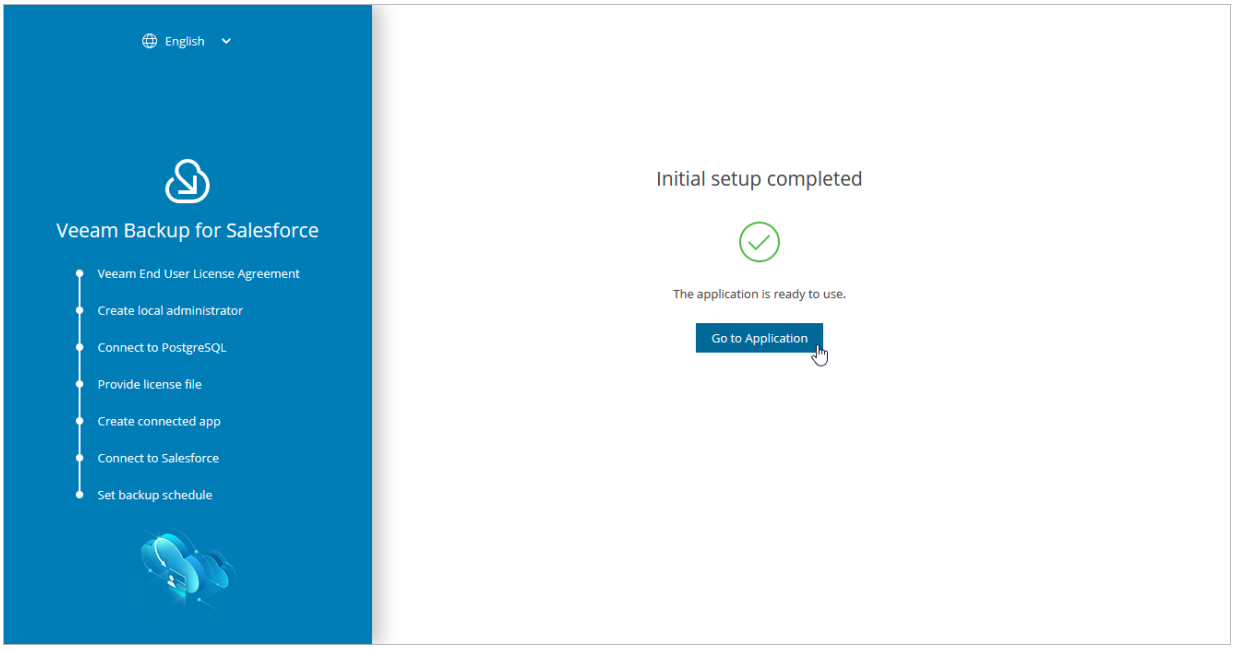
You can change these settings later as described in section Editing Backup Policies.

> **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

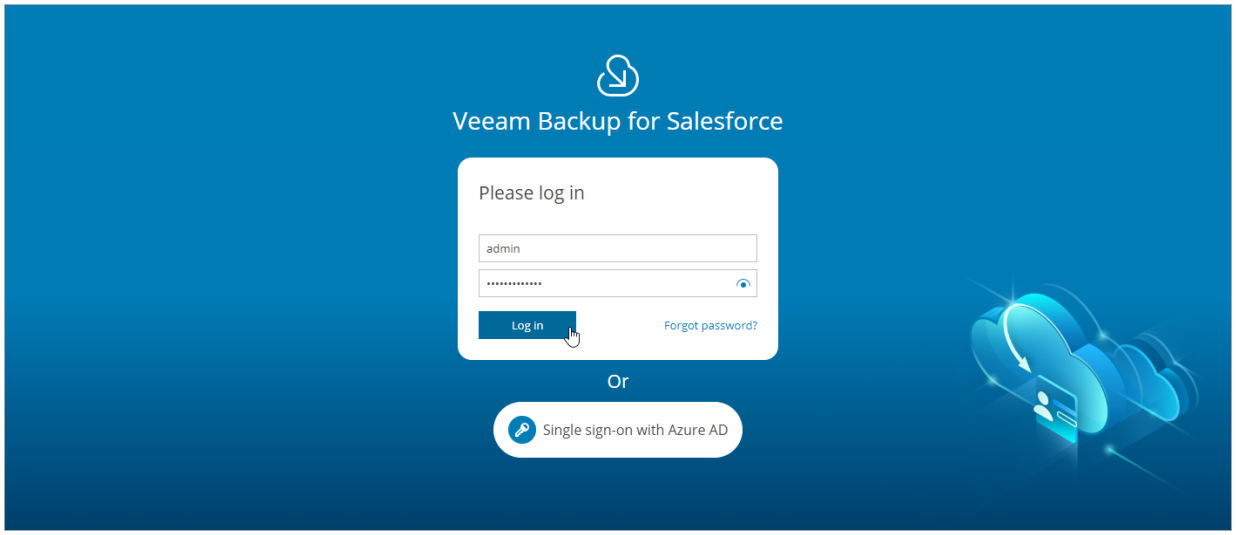
To log in to Veeam Backup for Salesforce, do the following:

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 an Azure AD or enabled a Salesforce organization as an identity provider in Veeam Backup for Salesforce, you can click **Single sign-on with Azure AD** 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
- Managing Alerts
- Changing Connected App Tokens

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

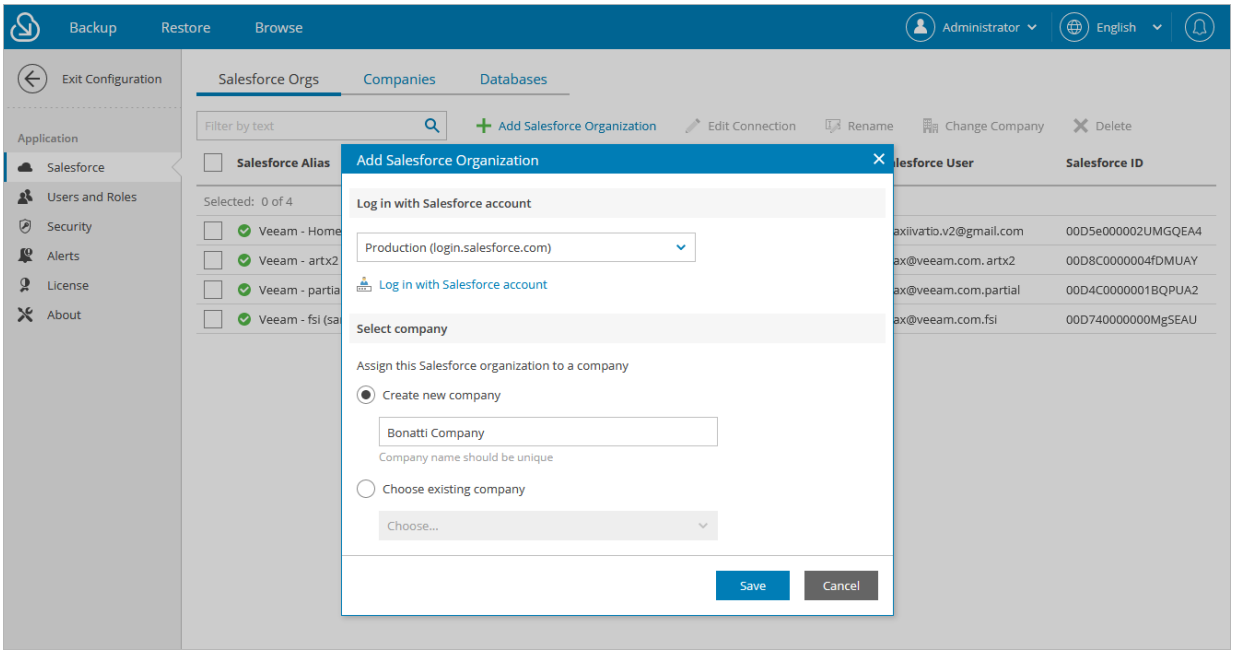
Adding Organizations

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, it must be created beforehand as described in section Adding Companies.
6. Click **Save**.



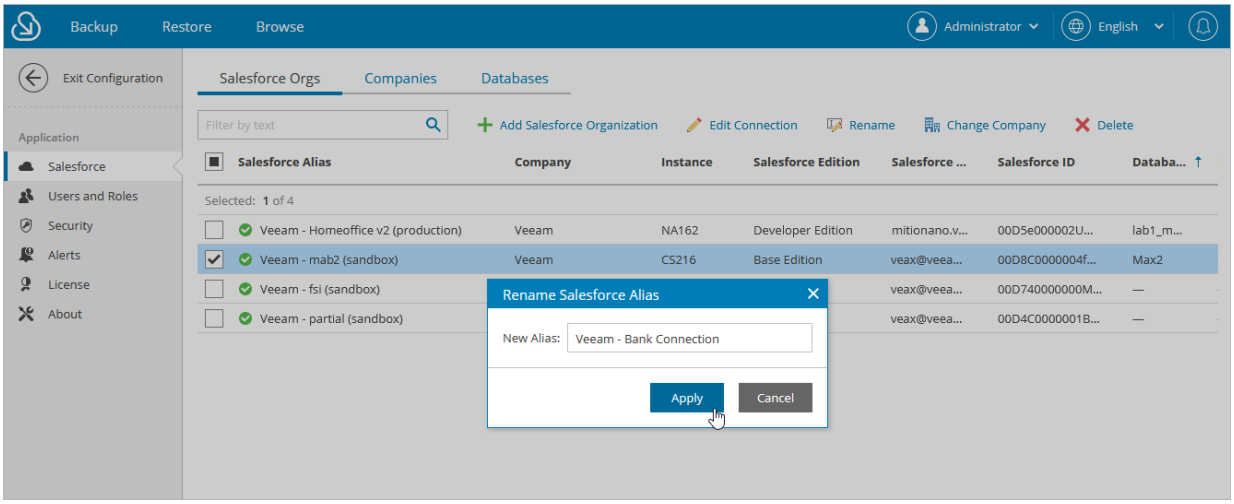
Editing Organizations

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**.



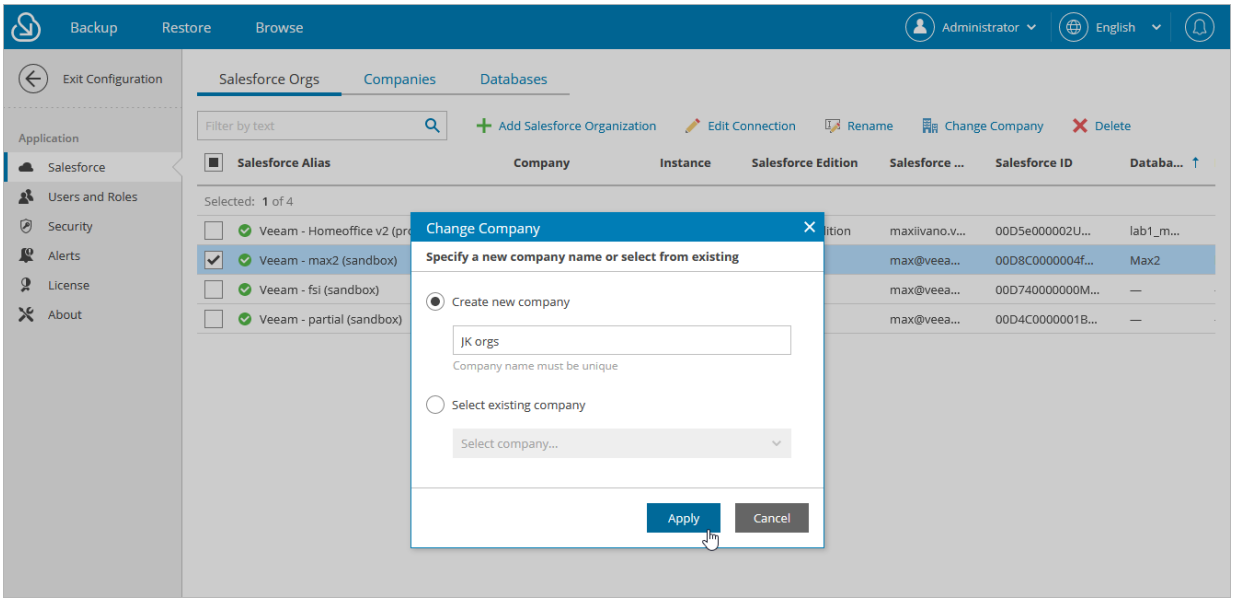
Changing Company

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, it must be created beforehand 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**.

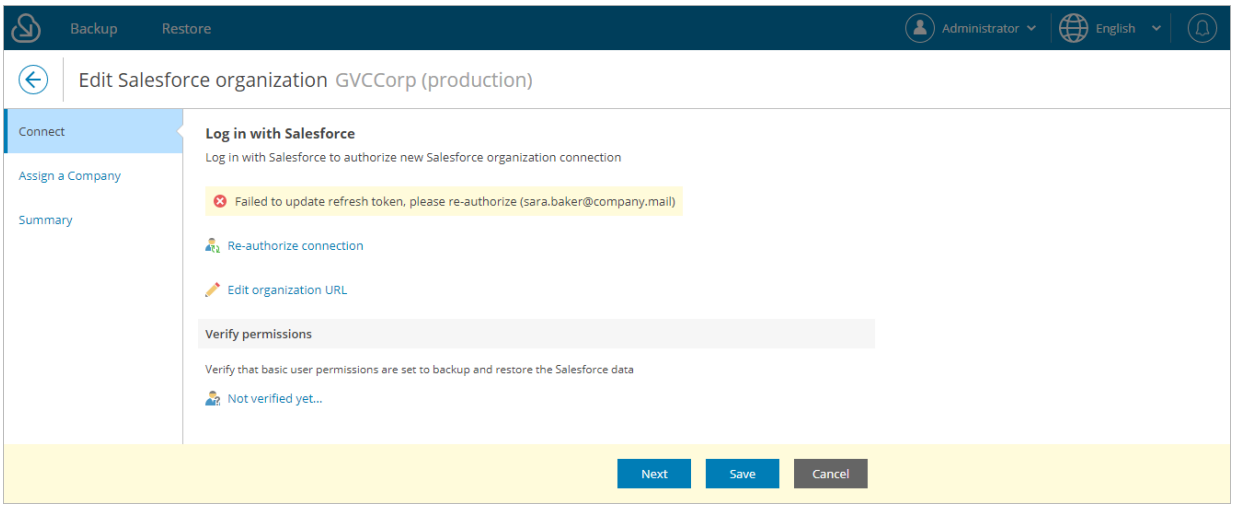
   The **Edit Salesforce organization** wizard will open.
4. At the **Connect** step of the wizard:
   a. To re-authorize connection to the organization, click **Re-authorize connection**. You will be redirected to the Salesforce authentication webpage.

      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**.

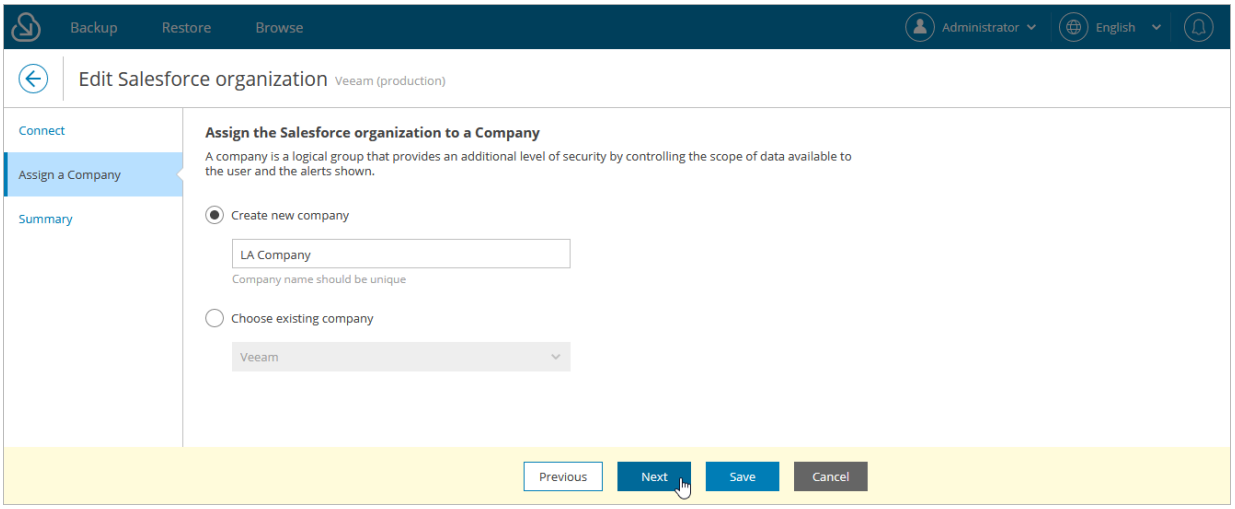
c. To verify whether permissions assigned to the specified user are enough to perform backup and restore operations, click the link in the **Verify permissions** section and wait for the check to complete.



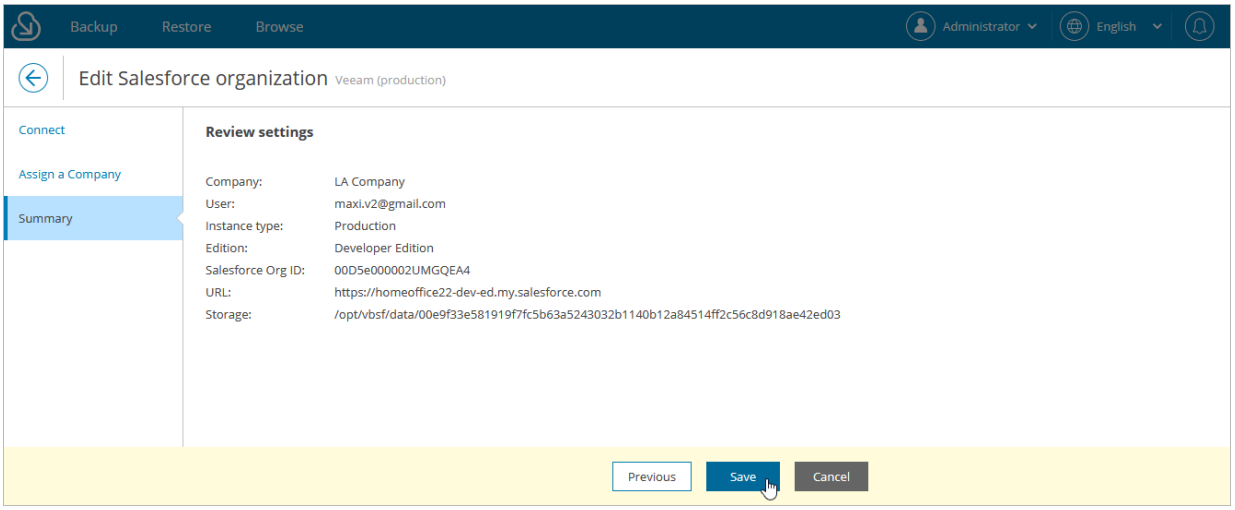
5. At the **Assign a Company** step of the wizard, choose whether you want to re-assign the organization to another company:

   - 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, it must be created beforehand as described in section Adding Companies.



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



Removing Organizations

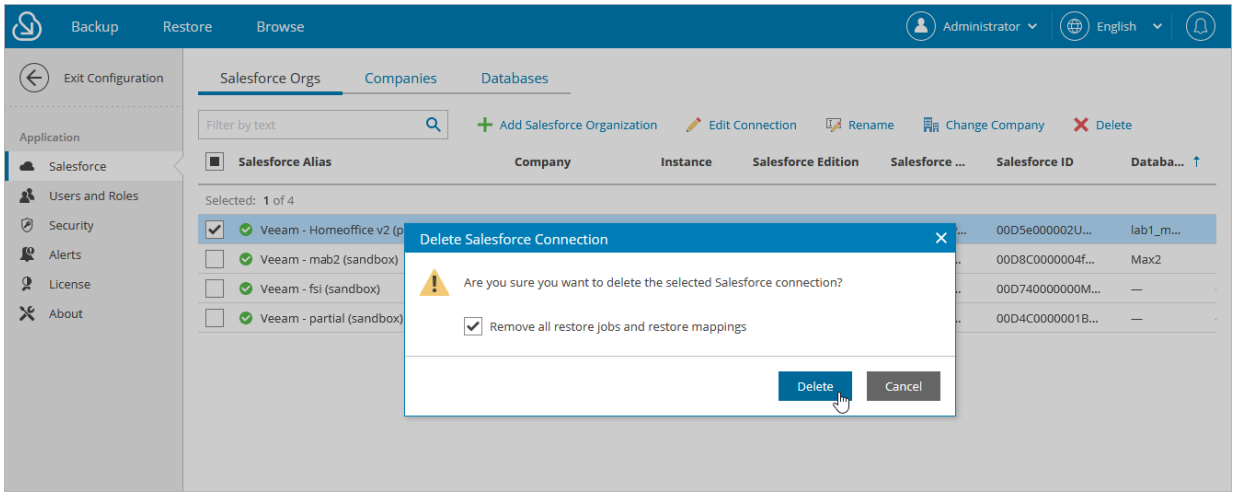
You can remove Salesforce organizations from the configuration database.

> **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, files and attachments) 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.

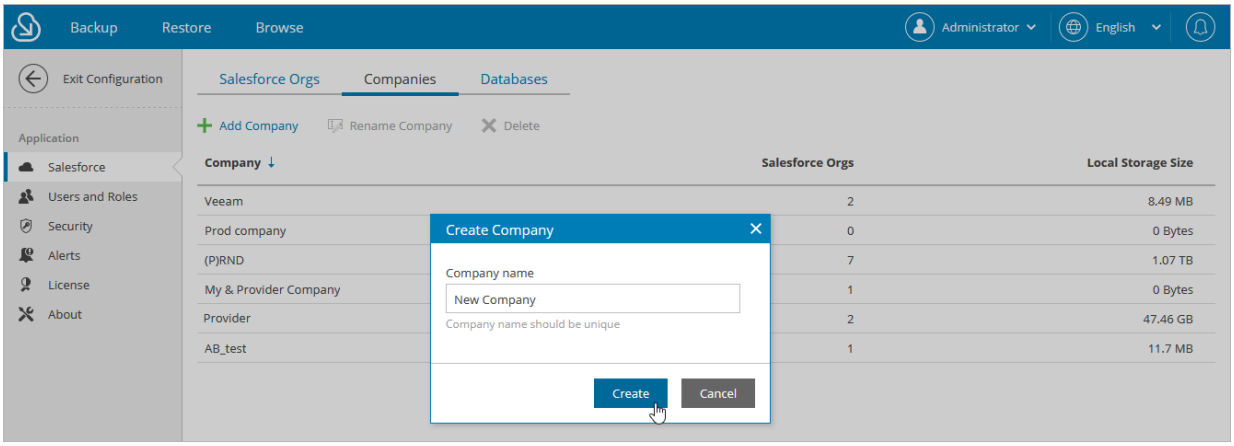
A company is created automatically when you connect to a Salesforce organization during the initial configuration of the management server. You can also add companies manually, edit created companies, re-assign company organizations and remove companies.

> **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:

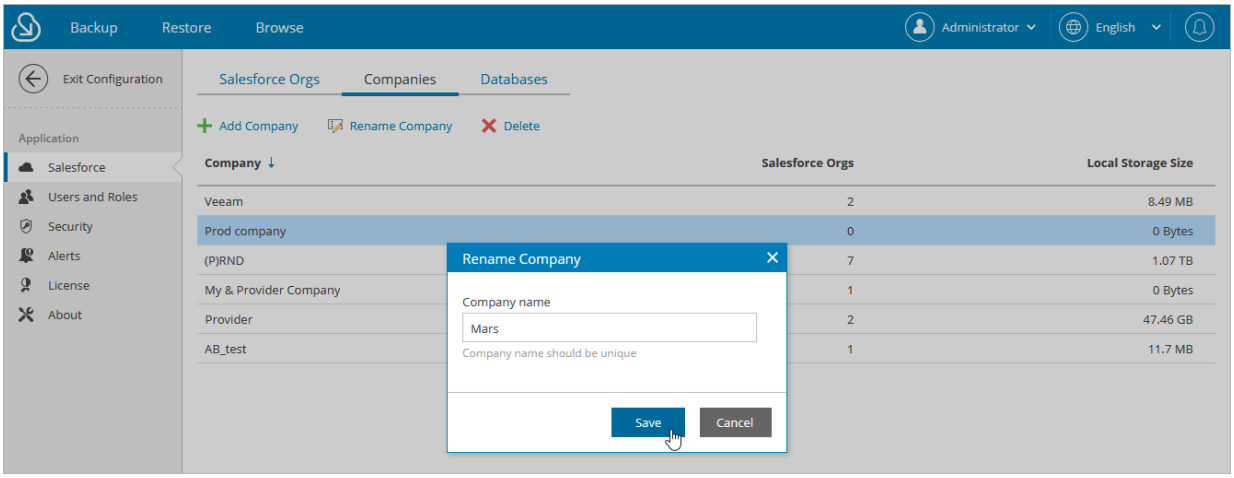
1. Switch to the **Configuration** page.
2. Navigate to **Salesforce** > **Companies**.
3. Click **Add Company**.
4. In the **Create Company** window, specify a name of a new company and click **Create**.



Editing Companies

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

1. Switch to the **Configuration** page.
2. Navigate to **Salesforce** > **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

You can remove companies from the configuration database. 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.

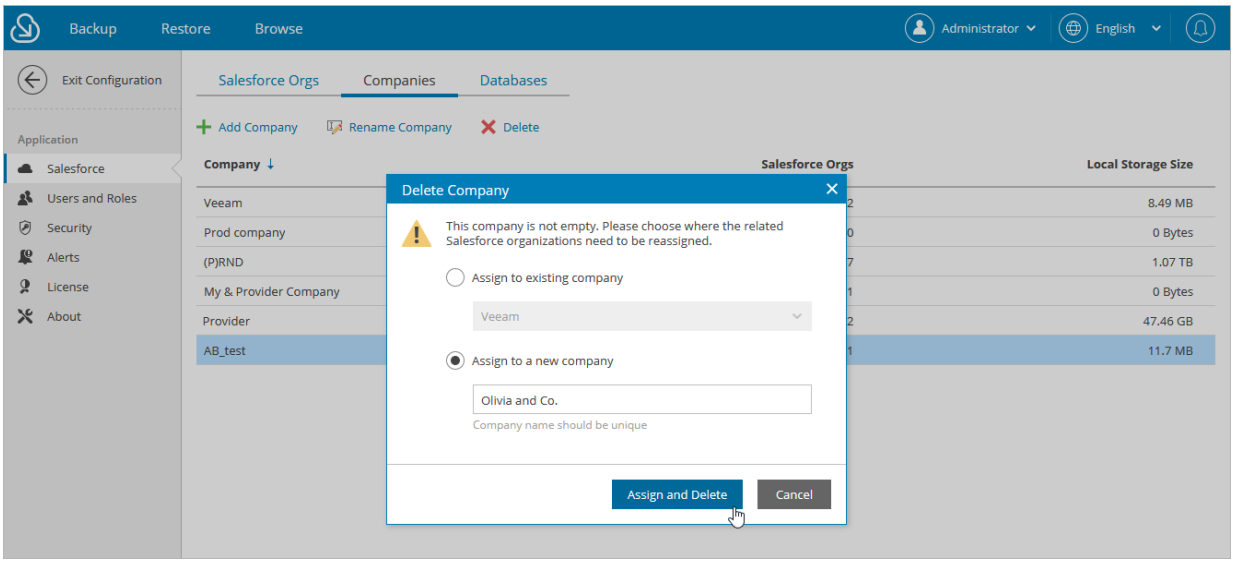
> **IMPORTANT**
>
> When you remove a company and re-assign organizations to another company:
>
> - Users that have company-wide permissions to the new company will automatically get permissions to access data of all re-assigned Salesforce organizations.
> - Users that have permissions to access the 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 **Salesforce** > **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, it must be created beforehand 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 Databases

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.

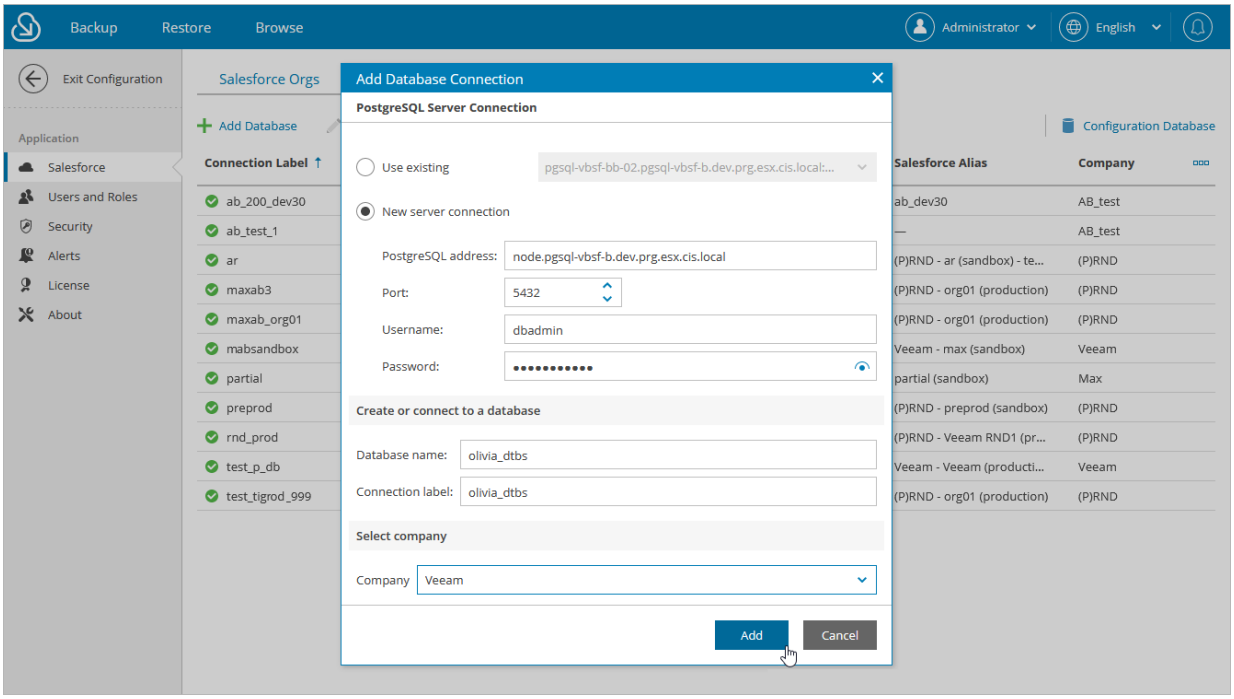
   c. Use the **Username** and **Password** fields to provide credentials of the PostgreSQL user that will be used to access the databases. The user must be assigned permissions required to create database schemas.

      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**.

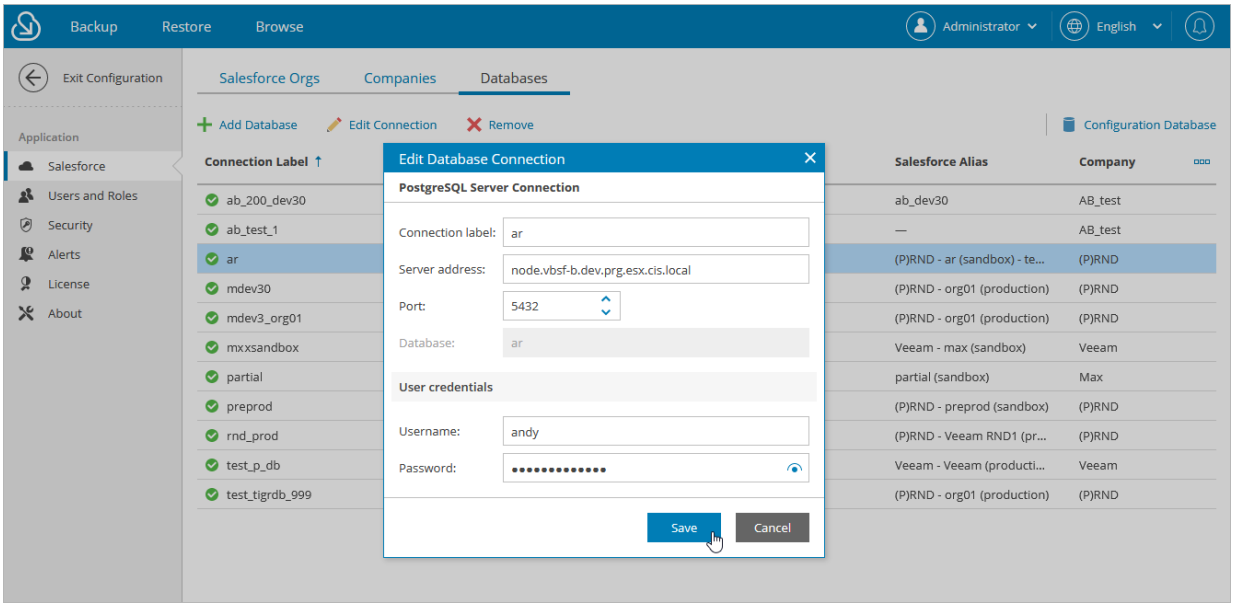


Editing Database Connections

For each PostgreSQL database added to Veeam Backup for Salesforce you can edit the connection settings:

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.



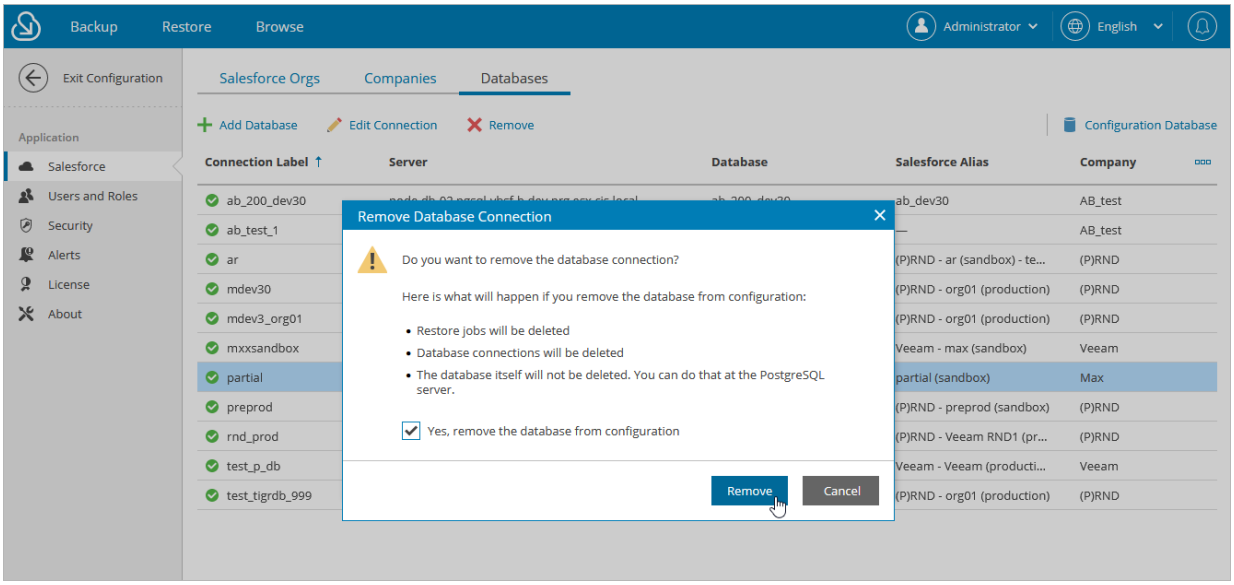
Removing Databases

You can permanently remove a database from Veeam Backup for Salesforce if you no longer need it. However, the removed 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. If you want to provision more users and leverage the role-based access, you can do that by connecting to an identity provider (IdP).

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 the protected data and perform all restore 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, backup sessions	Viewing backup policies, backup 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	-
Configuration					
Salesforce	Managing companies	Full	-	-	-

Tab	Functionality	Administrator	Backup Operator	Restore Operator	Viewer
	Managing Salesforce organizations	Full	Adding and viewing Salesforce organizations	-	-
	Managing databases	Full	Full	-	-
	Managing Connected App	Full	-	-	-
Users and Roles	Managing users	Full	-	-	-
Alerts	Managing notifications	Full	Full	-	-
License	Managing license	Full	Viewing license information	-	-
About	Downloading product logs	Full	-	-	-
	Configuring advanced settings	Full	-	-	-

Adding Users

To be able to add users and assign specific roles to them, you must first configure the IdP settings.

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

1. Switch to the **Configuration** page.
2. Navigate to **Users and Roles** > **Users**.
3. 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 an Azure AD 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 Azure AD. Otherwise, they will not be able to log in to the product.

4. In the **Assign Roles** window:
   a. In the **User or group** section, click the link and select the necessary IdP user or group of users in the **Select User or Group** window. Click **Select**.
   b. From the **Role** drop-down list, 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 different groups, the user will inherit the more privileged role from 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.

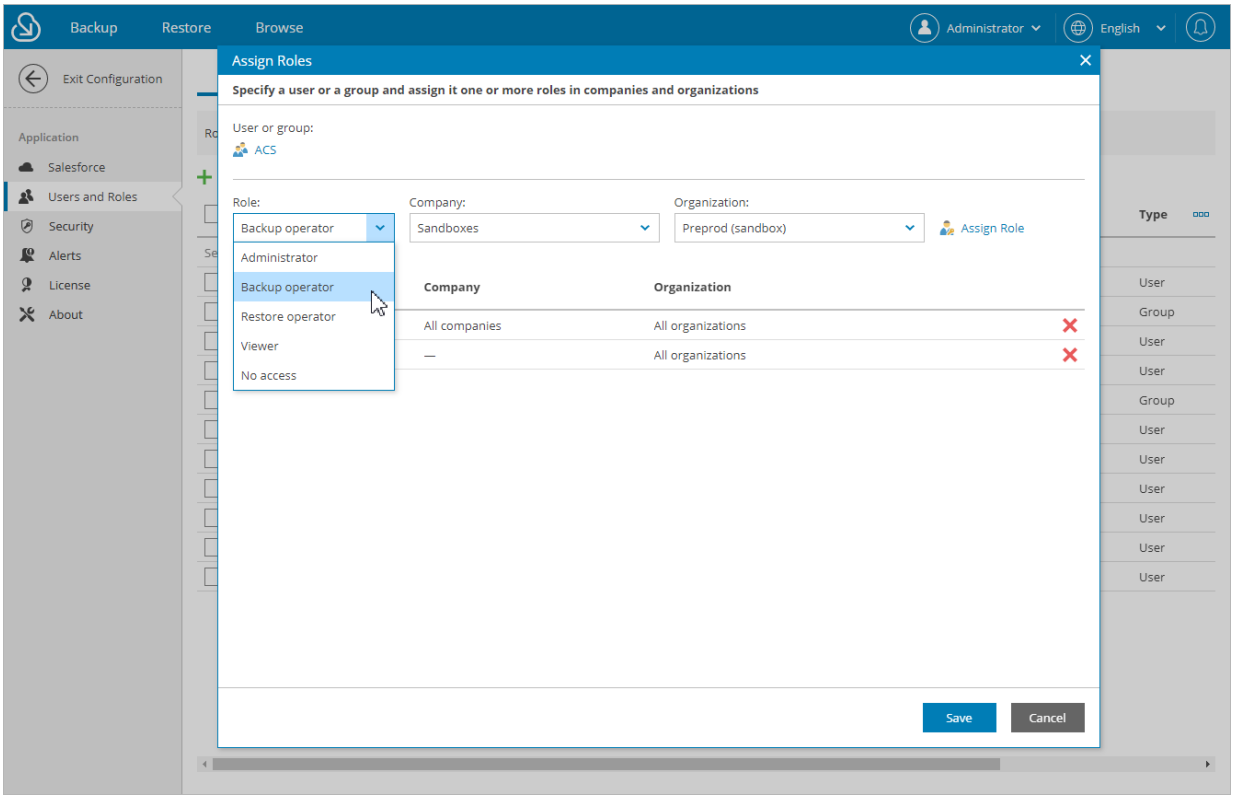
> **NOTE**
>
> You cannot limit the scope of resources for the *Administrator* role. By default, this role provides access to all companies and Salesforce organizations added to Veeam Backup for Salesforce.

   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.**


Backup
Restore
Browse
Administrator
English
Exit Configuration
Application
Salesforce
Users and Roles
Security
Alerts
License
About
Assign Roles
Specify a user or a group and assign it one or more roles in companies and organizations
User or group:
ACS
Role:
Backup operator
Company:
Sandboxes
Organization:
Preprod (sandbox)
Assign Role
Administrator
Backup operator
Restore operator
Viewer
No access
Company
Organization
All companies
All organizations
—
All organizations
Type
User
Group
User
User
Group
User
User
User
User
User
Save
Cancel

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/vbsf-backend/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

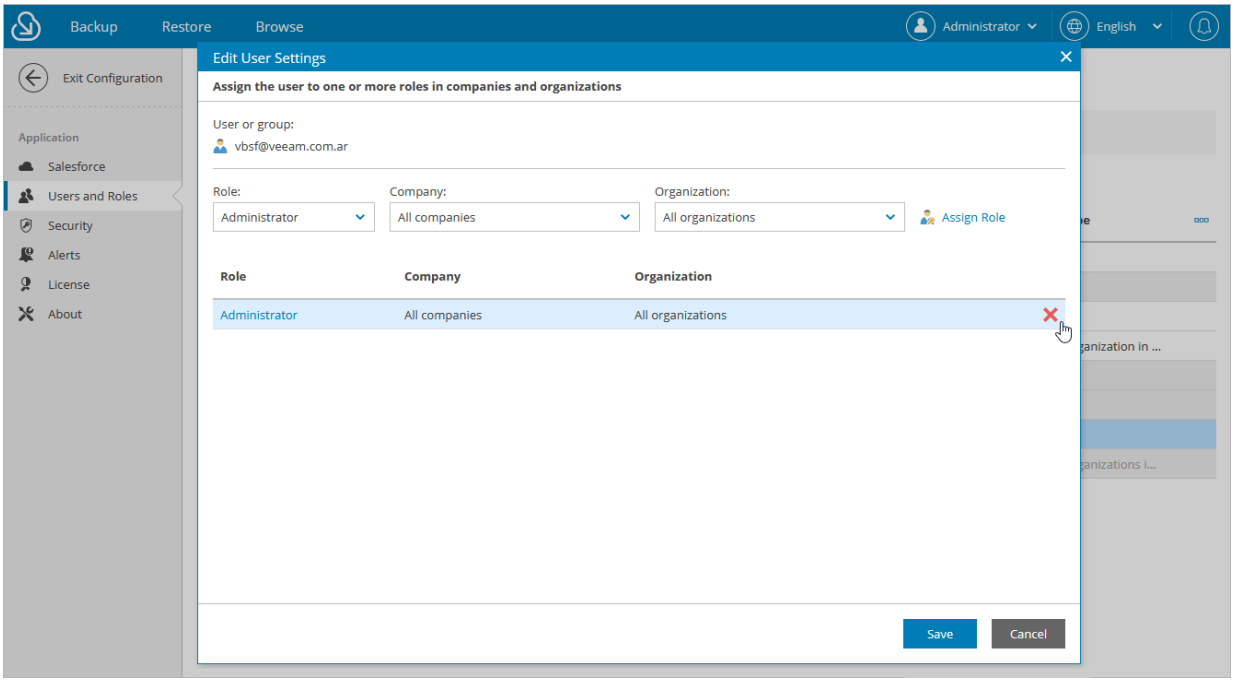
You can edit permissions assigned to users and user groups in Veeam Backup for Salesforce. To do that:

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:
    a. To unassign a role from the user or group of users, click the cross button in the necessary row of the user roles table.
    b. 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 and restore jobs started and scheduled by this user will not be affected.

NOTE

If you rename a group of users in Azure Active Directory, 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.

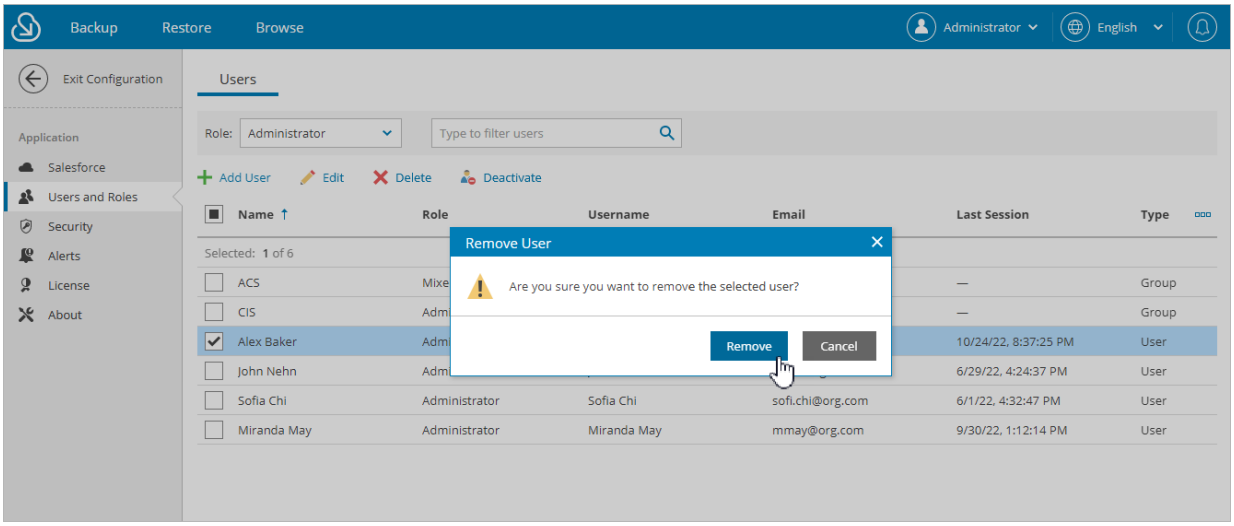


Removing Users

You can remove Veeam Backup for Salesforce 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 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
- Viewing Audit Trail

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

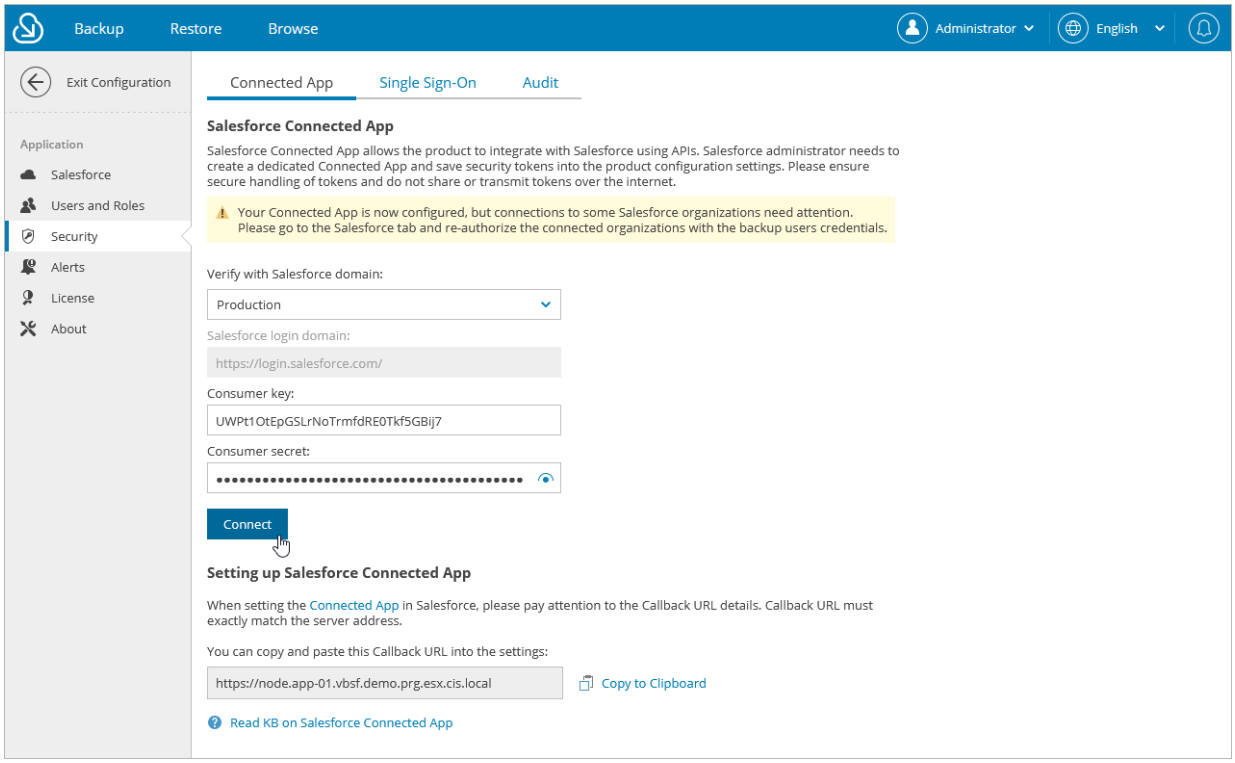
To change the OAuth tokens, do the following:

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**.

NOTE

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

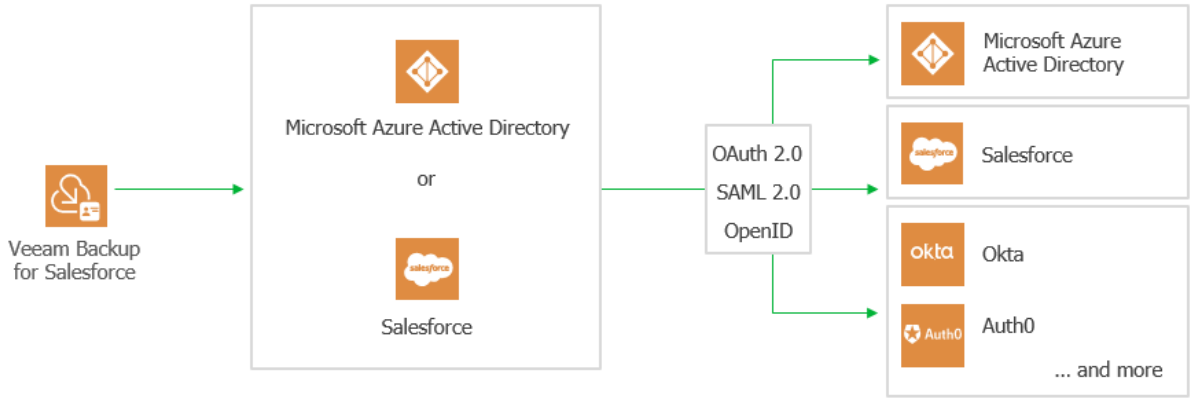
- The Connected App must be assigned the *Full access (full)* and *Perform requests at any time (refresh_token, offline_access)* OAuth scopes. For more information on OAuth scopes in Salesforce, see Salesforce Documentation.
- If you have configured Salesforce as an identity provider in Veeam Backup 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.



Configuring IdP and SSO Settings

Veeam Backup for Salesforce supports single sign-on (SSO) authentication using Azure Active Directory 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 Azure Active Directory

To configure IdP settings using Azure Active Directory, you must first create an Azure AD application for Veeam Backup for Salesforce in the Microsoft Azure portal. 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.

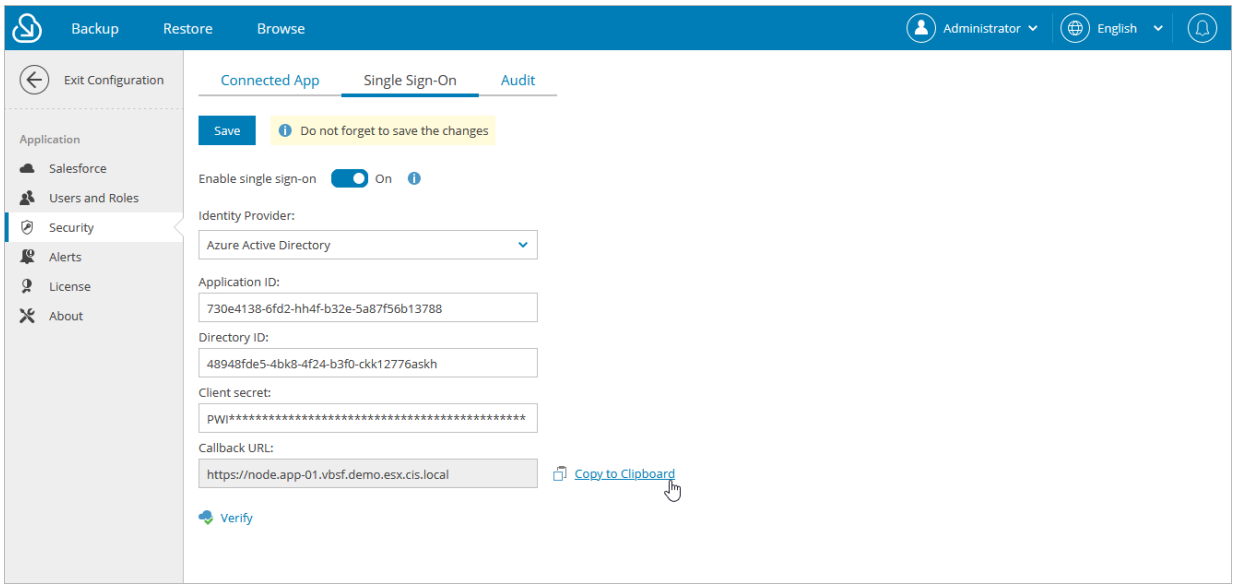
Configuring IdP Settings on Veeam Backup for Salesforce Side

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 *Azure Active Directory*.
5. In the **Application ID** field, provide the *Application (client) ID* of the registered Azure AD application. You can find the ID on the app registration **Overview** pane in the Microsoft Azure portal.
6. In the **Directory ID** field, specify the *Directory (tenant) ID* of the registered Azure AD application. You can find the ID on the app registration **Overview** pane in the Microsoft Azure portal.
7. In the **Client secret** field, enter the value of a client secret created in the specified Azure AD 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 Azure AD 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*.

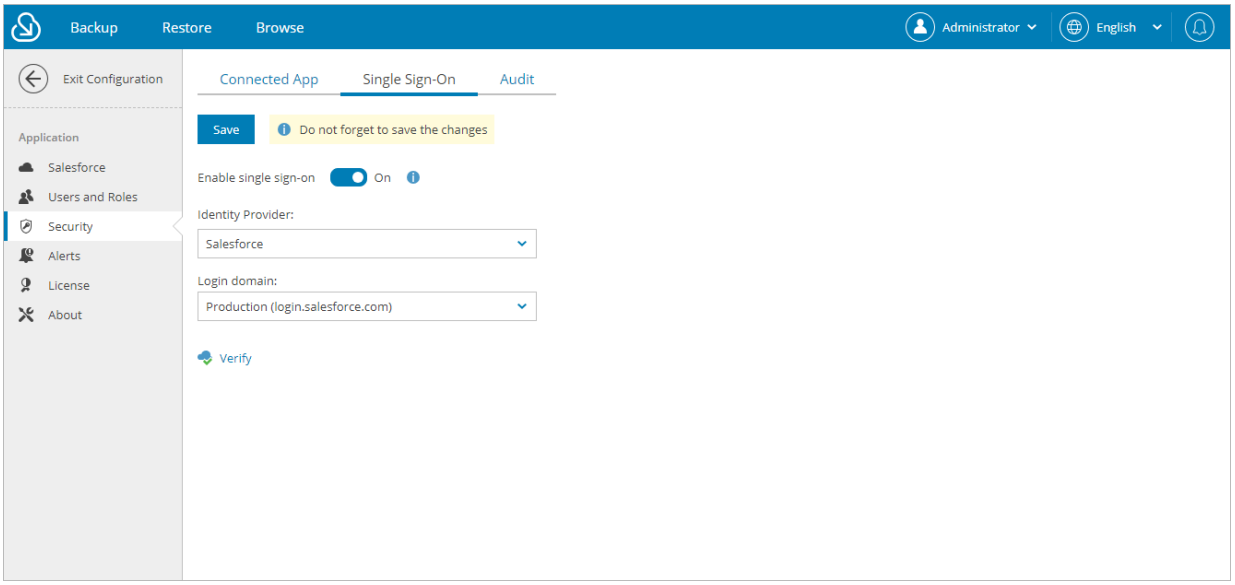
     If you select the **Custom** option, you must also specify the organization domain name.
6. Click **Save**. You will be redirected to the Salesforce authentication webpage.

   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.



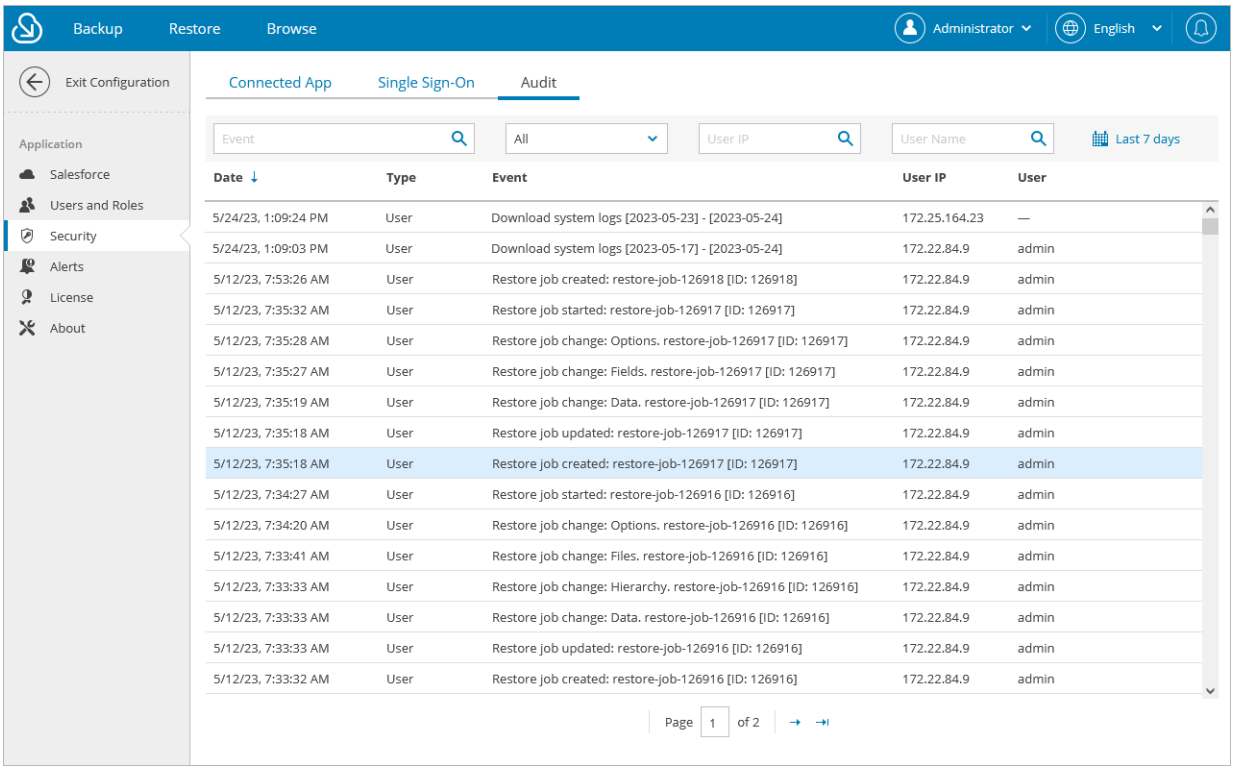
Viewing Audit Trail

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]`.



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.

> **NOTE**
>
> Users with the *Administrator* or the *Backup operator* role can assign types of alerts that users with the *Restore operator* or *Viewer* roles can view.

You can create alerts for the following type of events:

- Backup policy — an alert created for this type of event can be triggered by the specified backup session results, for example, you can choose whether you want to receive notifications in case backup policies complete successfully, complete with warnings or complete with errors.
- Restore job — an alert created for this type of event can be triggered by the specified restore session results, for example, you can choose whether you want to receive notifications in case restore jobs complete successfully, complete with warnings or complete with errors.
- Database connection — an alert created for this type of event can be triggered if the connection to PostgreSQL databases is lost.
- Salesforce connection — an alert created for this type of event can be triggered if the connection to Salesforce is lost.
- License — an alert created for this type of event can be triggered if the license acquires a specific status after a regular license check performed weekly by Veeam Backup for Salesforce or a license check performed manually by a user. To learn how to perform a license check manually, see Viewing License Information.
- File storage size — an alert created for this type of event can be triggered by the disk space usage check. The check is performed daily at 9:00 UTC, the alert will be sent if the specified threshold for the disk used space is breached.

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 an Azure AD application for Veeam Backup for Salesforce in the Microsoft Azure portal. 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 Azure AD application. You can find the ID on the app registration **Overview** pane in the Microsoft Azure portal.
3. In the **Directory ID** field, specify the Directory (tenant) ID of the registered Azure AD application. You can find the ID on the app registration **Overview** pane in the Microsoft Azure portal.
4. In the **Client secret** field, enter the value of a client secret created in the specified Azure AD 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 Azure portal. In the Microsoft Azure portal, navigate to the created Azure AD 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 Azure portal. Sign in using a Microsoft Azure 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.

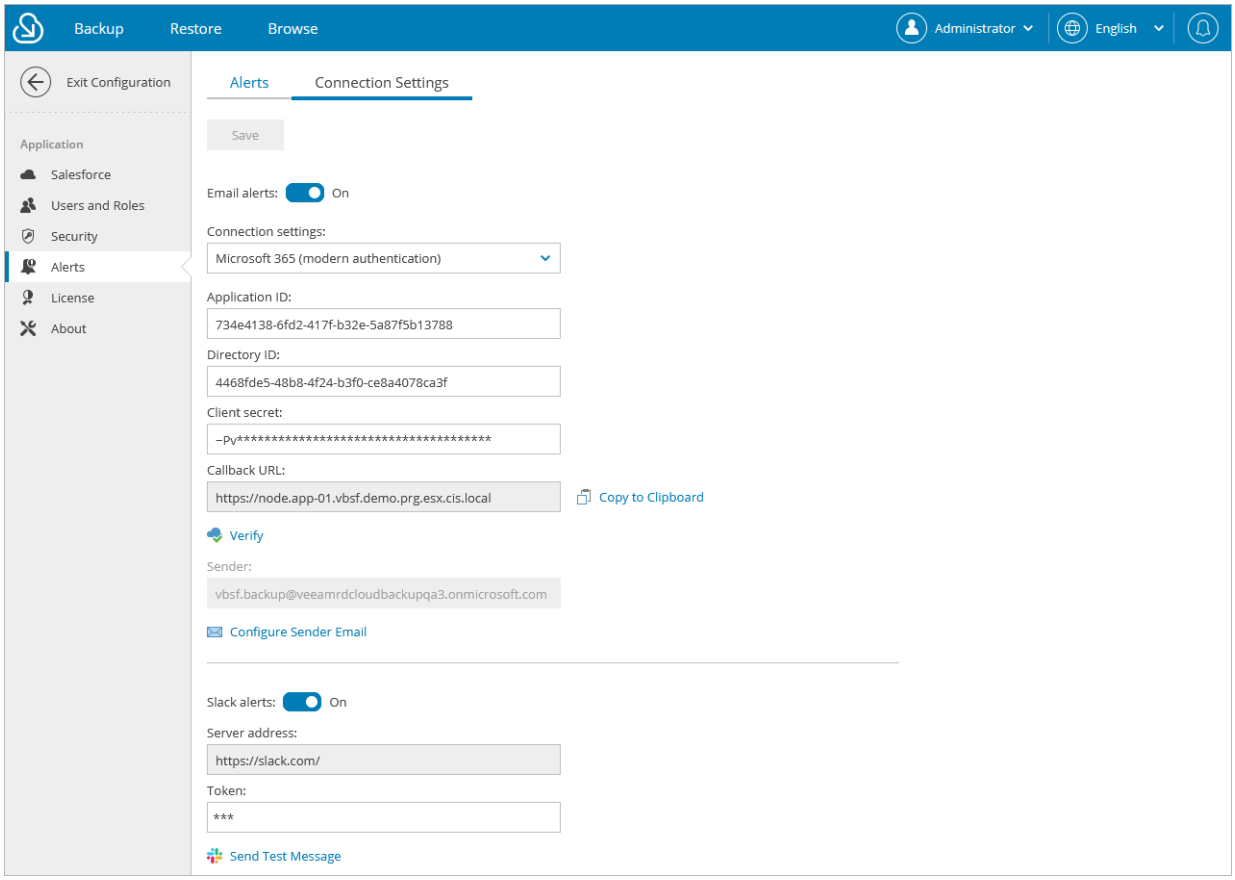
Configuring Slack Settings

To receive 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.



Creating Alerts

To create an alert:

1. Switch to the **Configuration** page.
2. Navigate to **Alerts**.
3. Click **Add**. The **Add Alert** wizard will open.
4. At the **Alert Type** step of the wizard, select the type of an event for which you want to create an alert from the **Event** drop-down list, and specify the conditions under which the alert will be sent.
5. At the **Recipients** step of the wizard, specify notification settings for the alert:
   a. Specify the recipients of the alert notifications:
      - In the **Roles** section, you can choose user roles that must be assigned to users or user groups to receive notifications. In this case, the notifications will be sent in the Veeam Backup for Salesforce Web UI and by email to all users assigned these roles within their permission scopes. To the groups of users, notifications will be sent only in the Web UI. For a user group to receive notifications by email, a group email address must be added to the user group settings in Azure Active Directory.
      - In the **Custom recipients** section, you can specify names of Slack channels, users and additional email addresses. In this case, the notifications will be sent to these recipients by email and in Slack. Use a semicolon and a space character to separate multiple recipient addresses.

        Addresses of the email recipients must be specified in the following format: *email@domain.com*; addresses of the Slack recipients can be specified in the following formats: *@username*, *#channelname*, *@userid*, *channelid*.

> **NOTE**
>
> To receive email and Slack notifications, the notifications settings must be properly configured as described in section Configuring Notification Settings.

   b. In the **Subject** field, specify a subject for notifications. You can use runtime variables listed in section Alert Variables.
   c. In the **Threshold** field, specify the number of events that must occur before the notification is sent. Consider the following example: the threshold is set to 5, the notification will be sent only when the 6 event occurs.
6. [This step applies only if you have selected the *Backup policy* or *Restore job* type of the alert] At the **Scope** step of the wizard, choose companies and Salesforce organizations to which the alert conditions will apply.
7. Click **Finish**.

Alert Variables

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

- *[%job_name%]* — the backup policy or restore job name.
- *[%job_status%]* — the backup policy or restore job status.
- *[%job_type%]* — the type of a job.
- *[%company_name%]* — the company name.
- *[%salesforce_name%]* — the name of a Salesforce organization with which the connection was lost.
- *[%api_usage%]* — number of API requests sent.
- *[%deleted%]* — number of records that were removed from Salesforce.
- *[%failed%]* — number of records that were failed to process.
- *[%changed%]* — number of records that were updated.
- *[%inserted%]* — number of records that were added to a database.

Editing Alerts

You can edit, enable, disable and remove the created alerts:

1. Switch to the **Configuration** page.
2. Navigate to **Alerts**.
3. Select the necessary alert from the list and do one of the following:
   - To edit the alert settings, click **Edit** and complete the wizard as described in section Creating Alerts.
   - To disable the enabled alert, click **Disable**.
   - To enable the disabled alert, click **Enable**.
   - To remove the alert, click **Delete**.

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** list shows general settings of the management server and key settings that Veeam Backup for Salesforce uses for backup operations:

- `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.
- `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.add.domain.filename` — defines whether the product adds the backend domain name to the name of the downloaded log archive file.
- `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.xmx` — the maximum amount of memory allocated to the Java Virtual Machine (JVM) used by the backup service to process metadata.
- `backup.metadata.xms` — the initial amount of memory allocated to the JVM used by the backup service to process metadata.
- `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.xmx` — the maximum amount of memory allocated to the JVM used by the backup service to process files and attachments.
- `backup.file.xms` — the initial amount of memory allocated to the JVM used by the backup service to process files and attachments.

- `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.data.xmx` — the maximum amount of memory allocated to the JVM used by the backup service to process Salesforce data. It is recommended that you add 256 MB of memory for each 1 TB of storage resources used by your organization.
- `backup.data.xms` — the initial amount of memory allocated to the JVM used by the backup service to process Salesforce data.
- `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 Azure.

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

- `suppress.sf.unknown.fields` — defines whether the product ignores fields that are present in backed-up databases but missing in the Salesforce database while running restore jobs. If you set this parameter value to `true`, the product will proceed with the restore process regardless of the missing fields. If you set this parameter value to `false`, the product will stop a restore job as soon as a missing field is discovered.
- `sf.composite.batch.size` — the number of records the product sends to Salesforce in one request (batch) during a restore session.
- `sf.bulk.records.threshold` — the maximum number of records before the product switches to Bulk API 2.0.
- `sf.bulk.batch.size` — the number of records the product sends to Salesforce in one request (batch) during a restore session. The product switches to this setting when the `sf.bulk.records.threshold` value is reached.
- `sf.api.version` — the Salesforce API version of the Veeam restore service.
- `min.free.memory.size.percents` — the minimum amount of free memory (in percentage) of the management server required to start a restore session.
- `log.obfuscation.level` — the level of masking sensitive data in restore logs.
- `hierarchy.restore.on.max.input.records` — the number of records that can be selected for one restore session (if hierarchy restore is enabled).
- `hierarchy.restore.off.max.input.records` — the number of records that can be selected for one restore session (if hierarchy restore is disabled).
- `hierarchy.restore.default.depth` — the maximum level to which child records are automatically restored. This setting is applied only to those records that have not been reviewed 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 the 1st level of child records.
- `hierarchy.max.parents.depth` — the default value of the **Restore parent hierarchy** parameter that is specified when configuring hierarchy advanced settings.

- `fields.restore.max.input.records` — the number of records that can be selected for one field value restore session.
- `backend.url` — the FQDN or IP address of the management server.

Performing Salesforce Backup

Only users assigned the Administrator or Backup operator roles can perform backup operations in Veeam Backup for Salesforce. Users can perform backup operations within their permission scope — only for companies and organizations to which data they have access.

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. One backup policy can be used to protect one Salesforce organization.

When performing the initial configuration, a user adds a Salesforce organization, and specifies a schedule for the backup policy that will protect this organization and a database that will be used to store backed-up data and metadata. This policy is created automatically by Veeam Backup for Salesforce and has the following preconfigured settings: backup of files and attachments is disabled, restore points created for Salesforce objects are stored for 1 year. You can edit these settings as described in section Editing Backup Policies.

If you want to back up more Salesforce organizations, you can create new backup policies. Each Salesforce organization can be protected by only one backup policy.

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

When you create a new backup policy to protect a Salesforce organization, you can instruct Veeam Backup for Salesforce:

- To back up Salesforce object data and metadata.
- To back up files and attachments associated with the Salesforce objects.
- To exclude specific objects and fields from the backup scope.
- To automatically protect new objects and fields.
- To apply different schedules used to launch backup sessions for different groups of objects.
- To remove the backed-up data according to the specified retention settings.

To create a backup policy, complete the following steps:

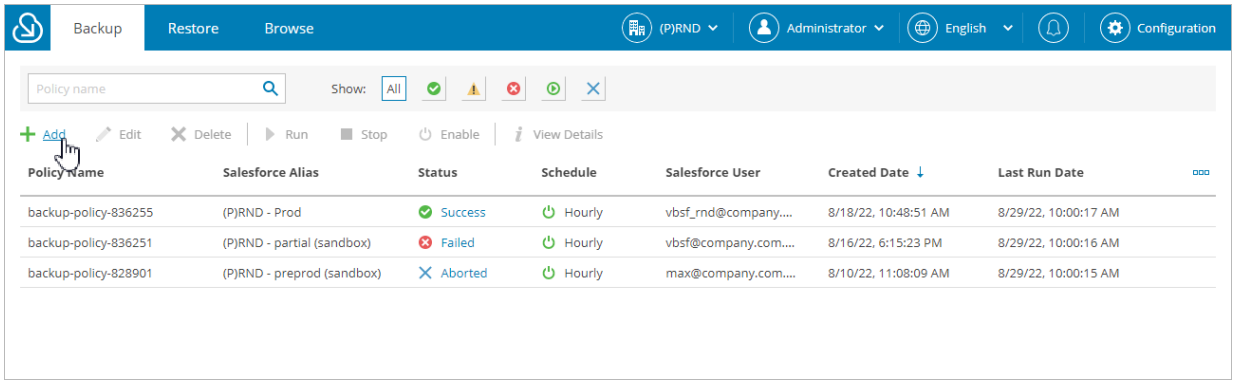
1. Launch the Add Backup Policy wizard.
2. Configure connection to a Salesforce organization.
3. Configure policy schedule and backup options.
4. Enable backup of files and attachments.
5. Configure retention settings.
6. Finish working with the wizard.

Step 1. Launch Add Backup Policy Wizard

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

1. Navigate to the **Backup** tab.
2. Click **Add**.

> **NOTE**
>
> If you have added multiple companies to Veeam Backup for Salesforce, before you launch the **Add Backup Policy** wizard, select the company to which a Salesforce organization that you want to protect belongs from the company drop-down list at the top of the page.
>
> For a company to be displayed in the list, it must be added to Veeam Backup for Salesforce beforehand as described in section Adding Companies, and the user must have permissions to access the company. For more information on user permissions, see User Roles and Permissions.



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, 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. 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, you can 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.

b. In the **Connect to a database** section, choose a database that will be used to protect the specified 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:

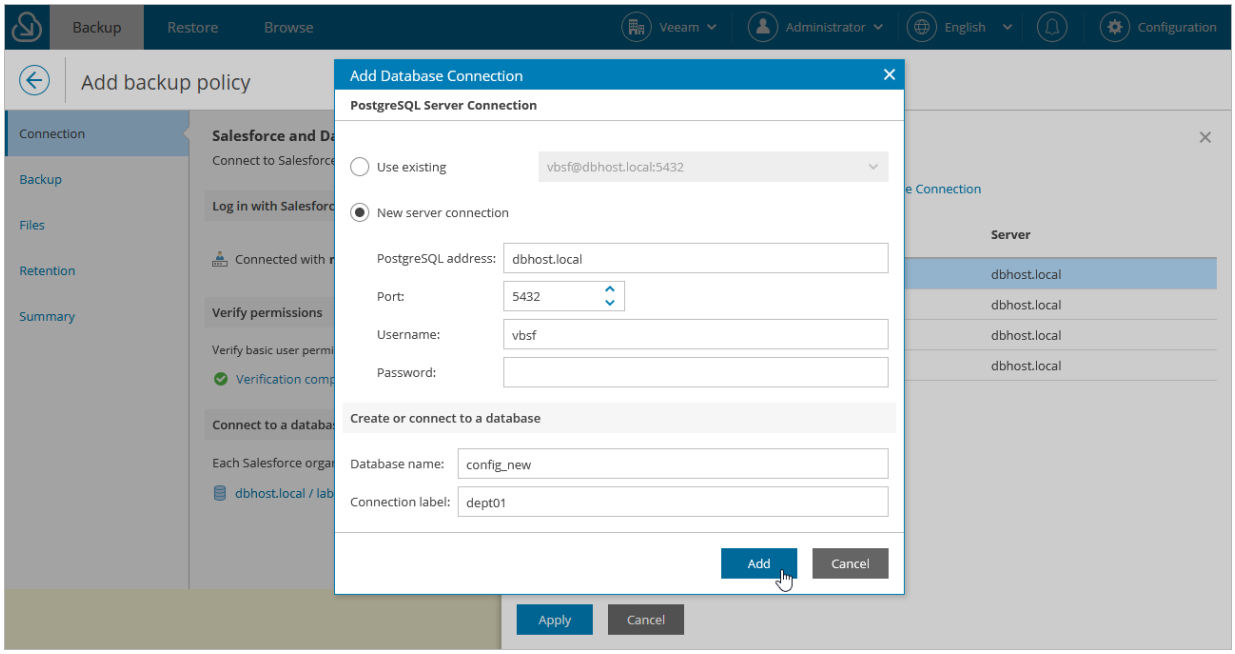
   - To add a database without closing the **Add Backup Policy** wizard, click **New Database Connection** and specify connection settings in the **Add Database Connection** window as described in section Adding Databases.
   - To specify an already added database, select the database from the list. For a database to be displayed in the list, it must be created beforehand 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.

   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.

NOTE

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.



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 3.1 Configure Backup Schedules

In the **Backup schedule** section of the **Backup** step of the wizard, configure the 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 the default policy schedule that will be used to back up all 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, 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 distinct backup session to protect each group of objects according to the assigned schedules. It is recommended that you assign the same schedule to the related Salesforce objects to ensure that these objects can be restored properly.

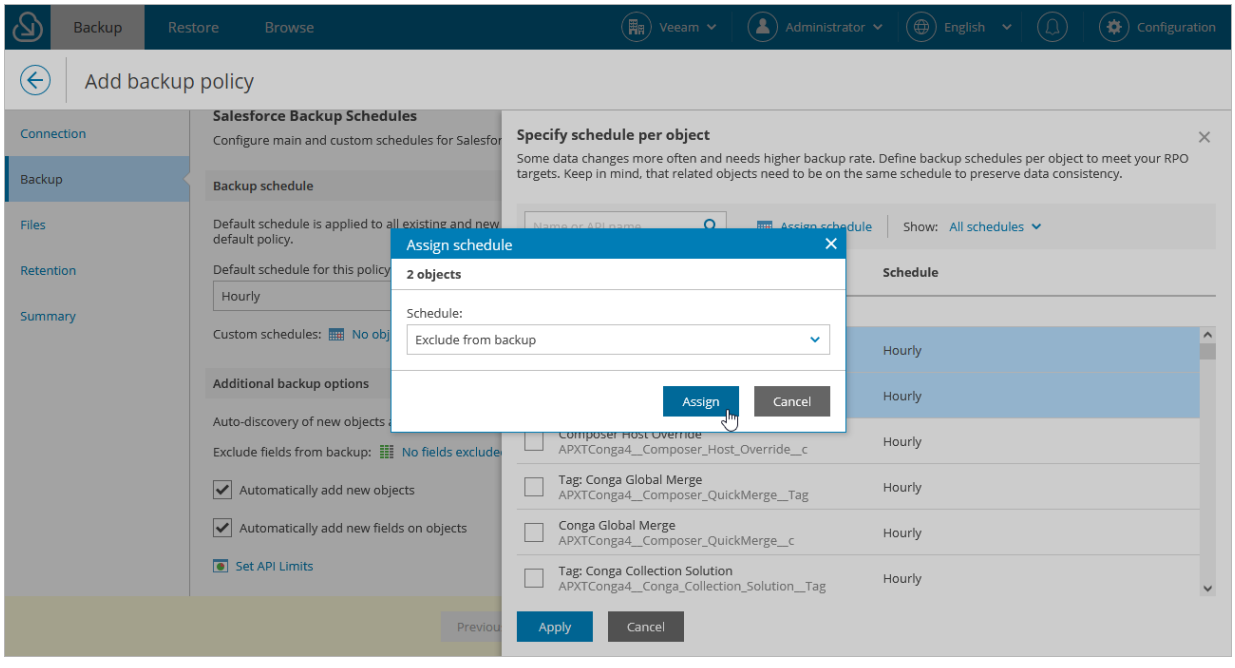
To assign a schedule to an object, do the following:

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 can not 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 in Veeam Backup for Salesforce.
   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.

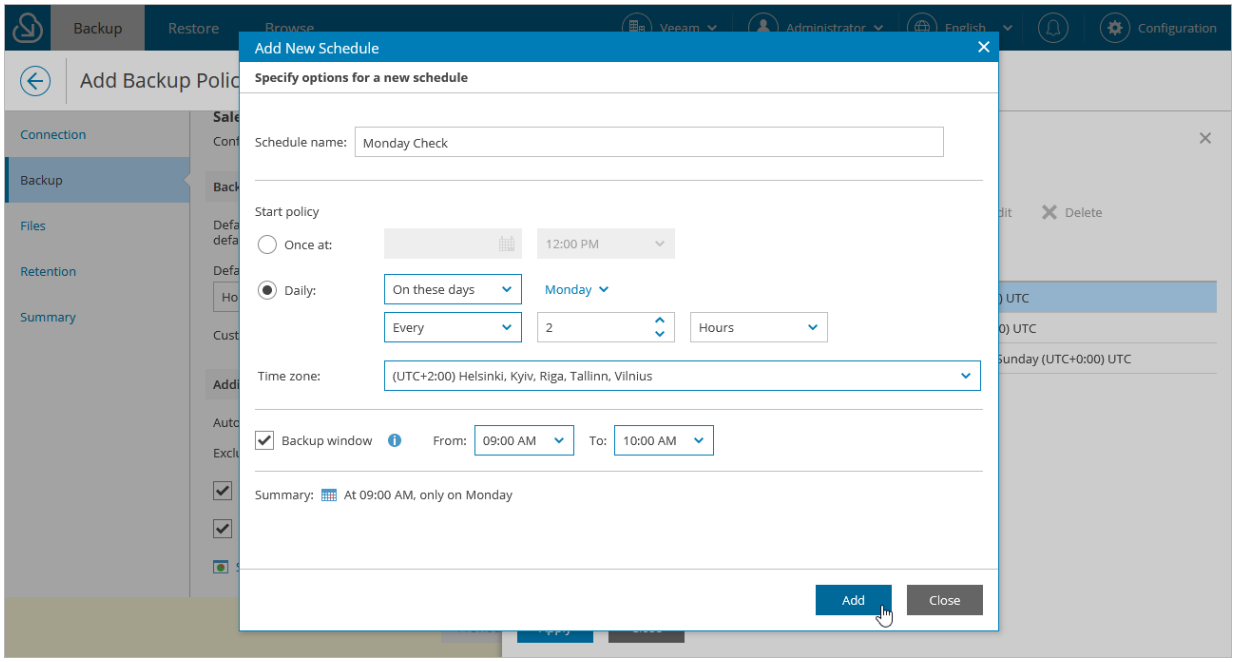
> **NOTE**
>
> The configured schedules are stored in the CRON format and used to run policy sessions. If you specify to run a session every 9 hours, Veeam Backup for Salesforce will follow the following schedule (UTC): Mon 00:00, Mon 09:00, Mon 18:00, Tue 00:00 and so on.

   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 3.2 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

Salesforce limits the total API requests per 24-hour period 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 the limits of REST API and BULK API requests that must not be exceeded by Veeam Backup for Salesforce when performing backup and restore operations. For more information on API request limits, see Salesforce Documentation.

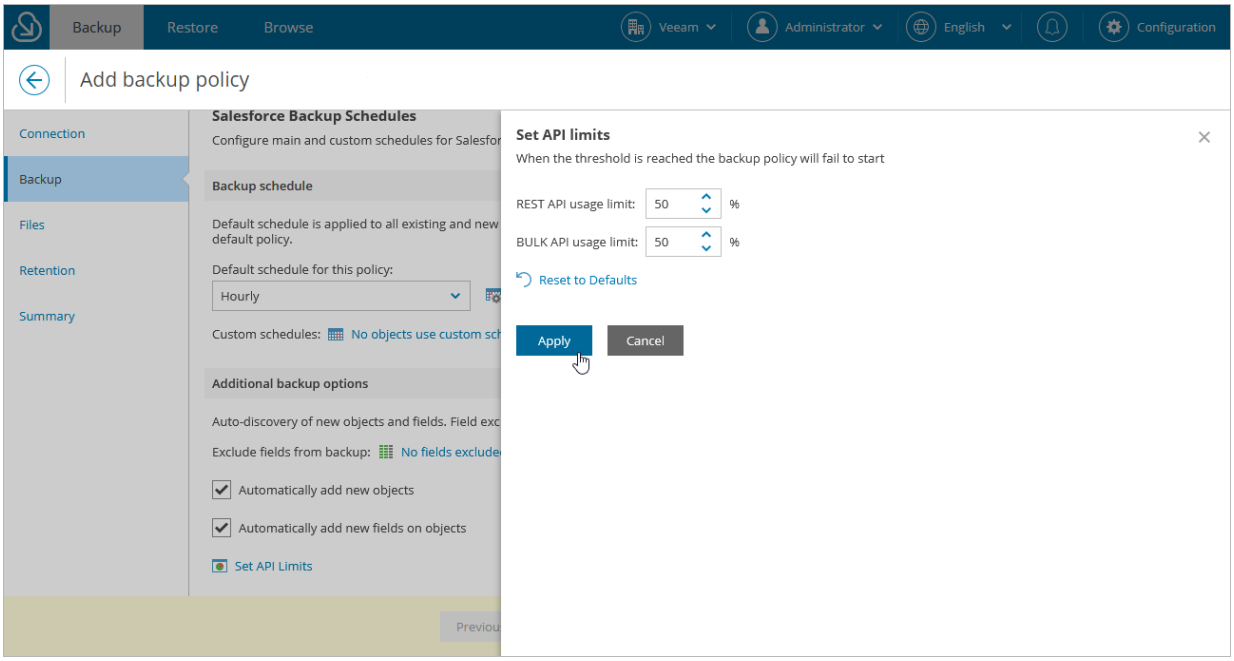
To limit API requests sent by Veeam Backup for Salesforce to Salesforce, do the following:

1. Click **Set API Limits**.
2. In the **Set API limits** window, specify the maximum limits for the REST API and BULK API requests, and click **Apply**.

How API Request Limits Work

After you set the maximum limit of API requests that can be used, Veeam Backup for Salesforce checks the quantity of remaining API requests each time before starting a new policy session. If the specified threshold is breached, the session fails with an error indicating that the API request limit has been exceeded.

If the specified threshold is not reached, then the policy session is started and Veeam Backup for Salesforce checks the quantity of API requests left before starting every new cycle of objects selection. Once the specified threshold is breached, backup of objects remaining in the queue fails with an error indicating that the API request limit has been exceeded. However, backup of objects that are already being processed continues until Salesforce accepts API requests. This may cause Veeam Backup for Salesforce to accidentally exceed the maximum limit of API requests that you specified.



Step 4. Enable Backup of Files and Attachments

> **IMPORTANT**
>
> This option is available only if you have assigned the *Query All Files* permission to your Salesforce user. For more information, see Permissions.

At the **Files** step of the wizard, to back up Files, Content, Documents and Attachments, do the following:

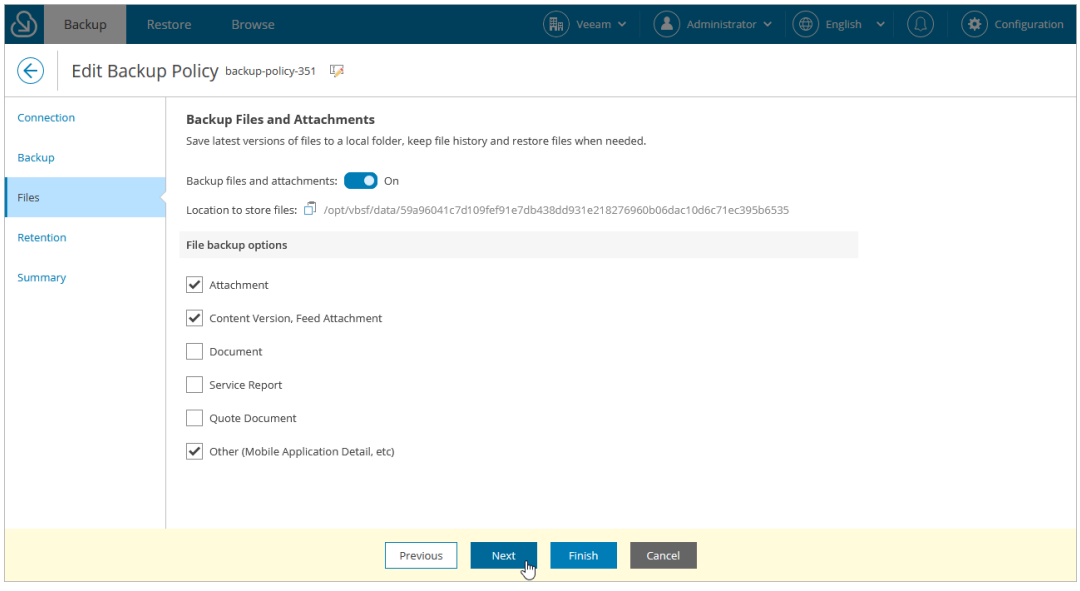
1. Set the **Backup files and attachments** toggle to *On*.

   Veeam Backup for Salesforce will display the local directory on the management server that will be used to store the backed-up files in the **Location to store files** field.

> **NOTE**
>
> Consider the following:
>
> - Note that 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.
> - It is recommended that you mount additional storage to the specified location to prevent the shortage of storage capacity. 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.
> - If you remove the 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.

2. In the **File backup options** section, select the type of data that you want to back up.

> **IMPORTANT**
>
> In Veeam Backup for Salesforce 2.0, you can back up but cannot restore using in-built product functionality the *MobileApplicationDetail* and *MailmergeTemplate* type of content. The restore functionality for these content types will be added in forthcoming versions.



Step 5. 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 the restore points will be kept. It allows you to consume less storage space by deleting the restore points that are older than the specified time period. Consider that the time period is calculated since creation of a backup of a Salesforce record, not since creation of the record itself.

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 backups of Salesforce objects and attachments.

      Note that Veeam Backup for Salesforce will always keep the latest restore point in the backup chain even if the specified retention limit is reached.

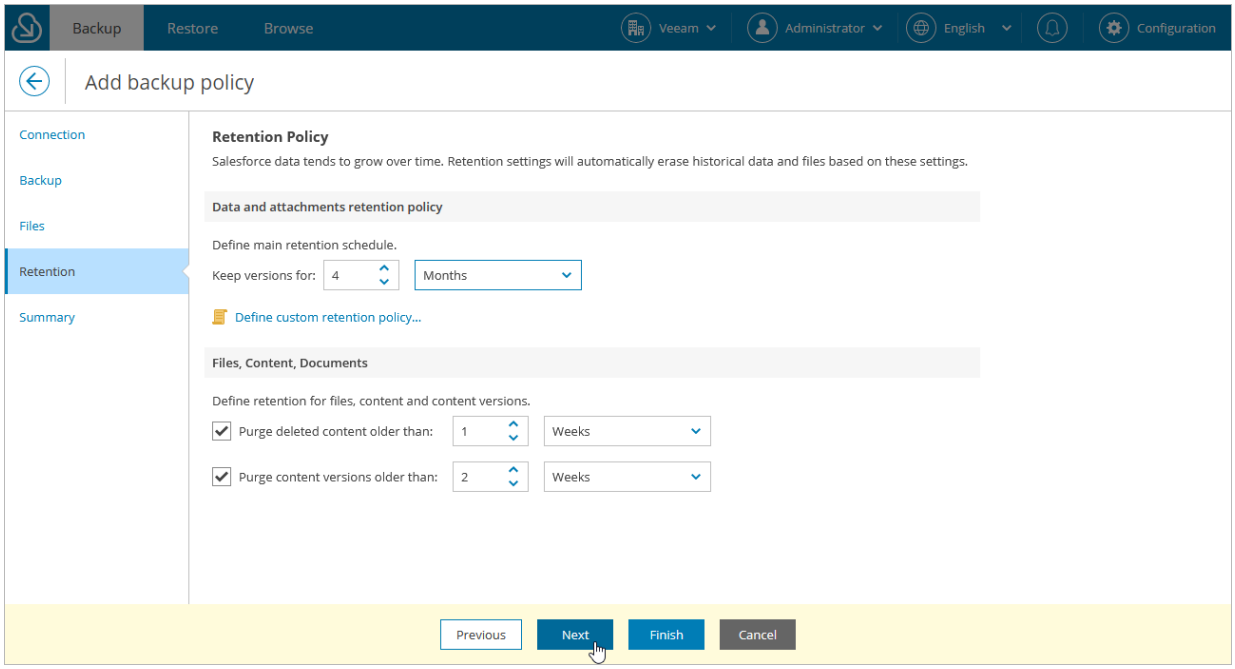
   b. If you want to configure specific retention settings for different objects protected by the backup policy, click the **Define custom retention policy** link.

      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 objects 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.

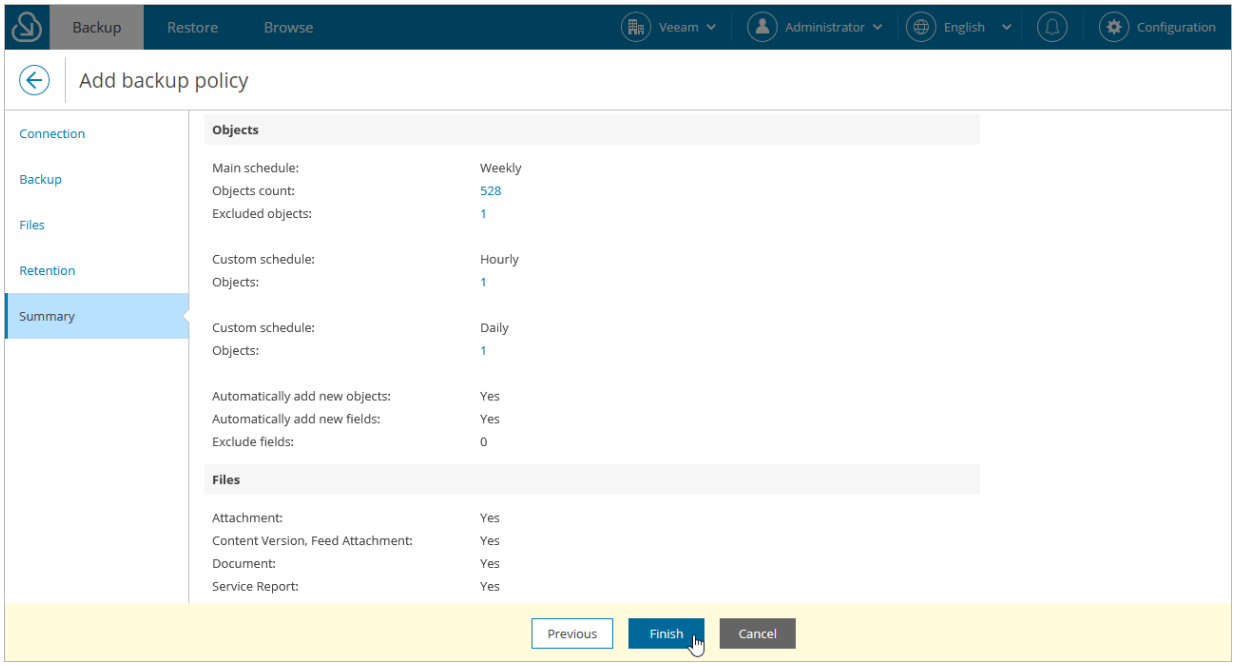
2. The settings specified in the **Data and attachments retention policy** section do not apply to backups of Files, Content and Documents created by the policy. If you want Veeam Backup for Salesforce to automatically delete these backups according to the retention policy, you must configure their own retention settings in the **Files, Content, Documents** section:
   - To instruct Veeam Backup for Salesforce to remove backups of files associated with object backups that have been already deleted 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 6. Finish Working with Wizard

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



Starting and Stopping Backup Policies

You can start a backup policy manually, for example, if you want to create an additional restore point 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, do the following:

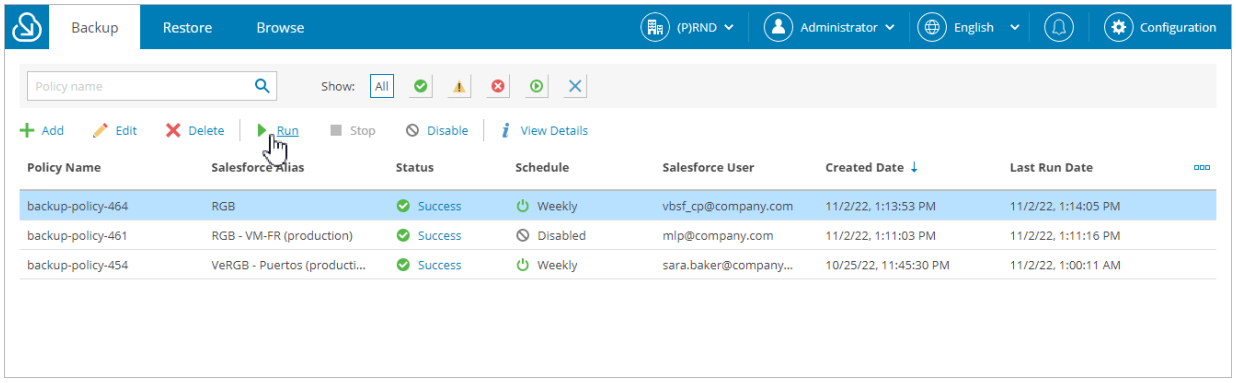
1. Navigate to the **Backup** tab.
2. Select the necessary backup policy.

> **NOTE**
>
> 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 set a filter, the settings apply to all companies and do 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 set.

3. 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

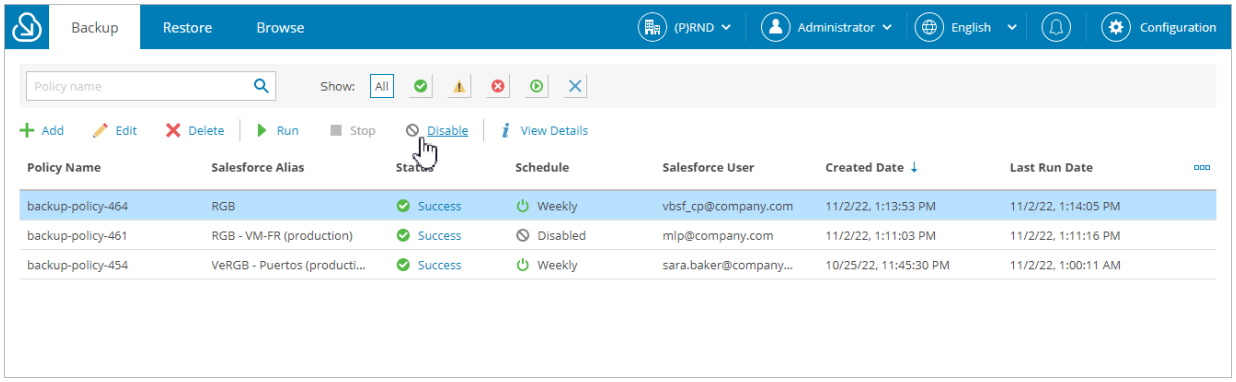
By default, Veeam Backup for Salesforce runs all created backup policies according to the specified schedules. However, you can temporarily disable a backup policy so that Veeam Backup for Salesforce does not run the backup policy automatically. You will still be able to manually start or enable the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

> **NOTE**
>
> 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 set a filter, the settings apply to all companies and do 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 set.

3. Click **Disable** or **Enable**.



Editing Backup Policies

You can edit backup policies created in Veeam Backup for Salesforce. For example, you may want to modify some settings for a backup policy, change the backup policy schedule and so on.

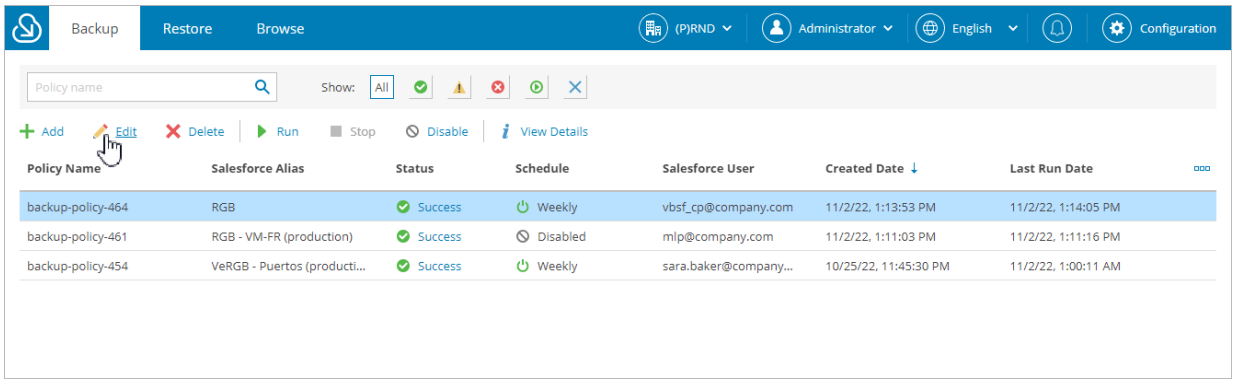
To edit backup policy settings, do the following:

1. Navigate to the **Backup** tab.
2. Select the necessary backup policy.

> **NOTE**
>
> 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 set a filter, the settings apply to all companies and do 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 set.

3. Click **Edit**. The **Edit Backup Policy** wizard will open.
4. Edit backup policy settings as described in section Creating Backup Policies.

> **IMPORTANT**
>
> If an error occurs when you reconnect to the Salesforce organization, check whether you specified the correct credentials of a user that belongs to the same Salesforce organization.



Removing Backup Policies

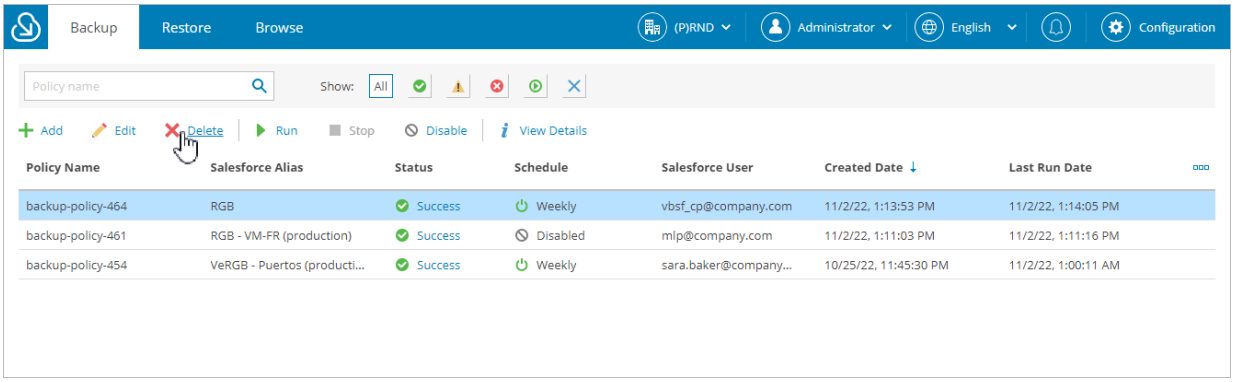
You can permanently remove a backup policy from Veeam Backup for Salesforce. Note that the backed-up data will not be automatically deleted when you remove the policy.

To remove a backup policy, do the following:

1. Navigate to the **Backup** tab.
2. Select the necessary backup policy.

> **NOTE**
>
> 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 set a filter, the settings apply to all companies and do 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 set.

3. 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 which data they have access to.

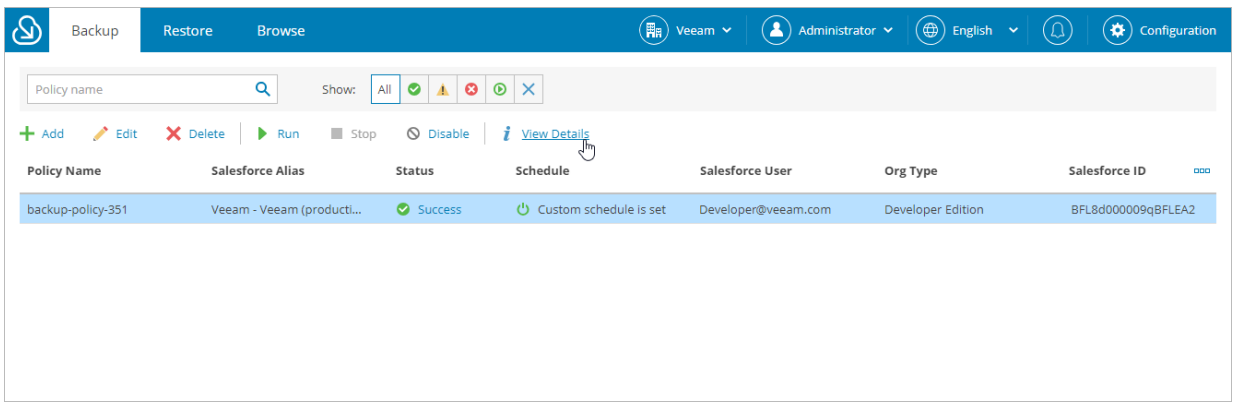
> **NOTE**
>
> You can filter backup policies displayed on the **Backup** tab by using the icons in the **Show** field at the top of the list. If you set a filter, the settings apply to all companies and do not change during the current user session. That is why if you do not see a policy in the list,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

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

- **Policy Name** — the name of the backup policy.
- **Salesforce Alias** — the alias of the Salesforce organization.
- **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 Policy Session Statistics.
- **Schedule** — the name or status of the schedule configured for the backup policy.
- **Salesforce User** — the name of an Salesforce account specified during policy configuration.
- **Org Type** — the type of the Salesforce 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 that includes the Salesforce organization.
- **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 Policy Sessions

When creating a backup policy, you configure the default backup schedule according to which Veeam Backup for Salesforce backs 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 4 different types:

- Data job — this type of job is used to back up data of objects of the protected Salesforce organization. Dedicated 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 type of job is used to back up metadata of the protected Salesforce organization. Metadata jobs run according to default backup schedules only.
- File job — this type of job 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.
- Validate job — this type of job is used to compare backed-up data in the product database with data currently stored in the Salesforce database, 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.

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

Backup Sessions

The **Backup Sessions** section 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 the backup job by which the session is launched.
- **Start** — the date and time when the session started.
- **Finish** — the date and time when the session ended.
- **Status** — the status of the session.
- **Message** — a message displayed in case the session has the Warning or Error status.
- **Processed Objects** — the number of backup policy objects processed during the session.
- **API Usage** — the number of API calls sent during the session.
- **Inserted** — the number of Salesforce records added compared to the previous session.
- **Updated** — the number of Salesforce records updated compared to the previous session.
- **Deleted** — the number of Salesforce records deleted compared to the previous session.
- **Failed** — the number of Salesforce records whose processing failed.
- **Total** — the number of Salesforce records processed.
- **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 is created.

Session Details

The **Session Details** section displays information on processing of all backup objects included in the selected policy session.

Each part of the backup session dedicated to an object is described with the following properties:

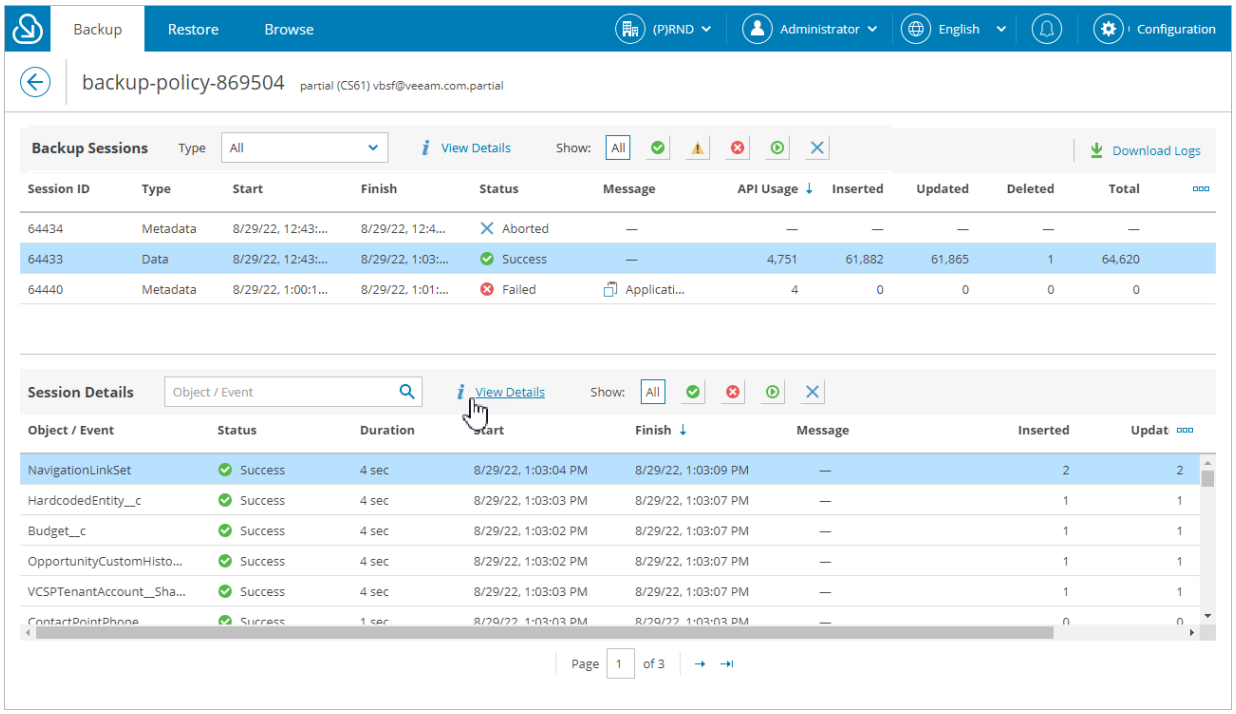
- **Object / Event** — the name of a backup object.
- **Status** — the status of the object processing.
- **Duration** — the duration of the object-related part of the session.
- **Start** — the date and time when the object-related part of the session started.
- **Finish** — the date and time when the object-related part of the session ended.
- **Message** — the additional information on object protection status.
- **Interval Start** — the start time of the interval during which changes in backup object are collected.
- **Interval End** — the end time of the interval during which changes in backup object are collected.
- **API Usage** — the number of API calls sent during the session.
- **Inserted** — the number of Salesforce records added compared to the previous session.

- **Updated** — the number of Salesforce records updated compared to the previous session.
- **Deleted** — the number of Salesforce records deleted compared to the previous session.
- **Failed** — the number of Salesforce records whose processing failed.
- **Total** — the number of Salesforce records processed.

TIP

Consider the following:

- You can download backup session logs. To do that, click **Download Logs**, Veeam Backup for Salesforce will collect the backup logs and save them to the default download folder on the local machine in a single `log.zip` archive.
- You can see the detailed information on an object-related part of the session: To do that, select the necessary backup session and click **View Details**.



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 object whose records you want to restore.

   Only Salesforce objects that have been backed up are displayed at this step. If you do not see the necessary object, the object 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.
   - The object does not contain any data.
   - 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 whether you want to search through the latest records or the history records of the selected object:

   - If you select *Latest Records*, Veeam Backup for Salesforce will perform search only through the latest versions of backed-up records.
   - If you select *History Records*, Veeam Backup for Salesforce will perform search through all record versions in the history table for the time period that you specify.
5. Click **Search**.

   Veeam Backup for Salesforce will display all records that match the search parameters. You can select records that you want to restore, click **Start Restore**, and choose whether you want to restore the entire record or specific fields. The restore job configuration wizard will open.

Configuring Additional Search Parameters

By default, Veeam Backup for Salesforce shows the search results in the table with the columns that match specific Salesforce fields. You can choose the displayed information and apply additional search conditions using specific filters. To do that:

1. In the **Filters and Display fields** field, click **Customize**. The **Data Filters and Display Fields** window will open.
2. To specify the fields that must be displayed in the table, switch to the **Display Fields** tab, select the necessary Salesforce fields in the **Available** section, click **Add**. You can change the order of columns in the table using the **Move Up** and **Move Down** buttons.

3. To filter search results, switch to the **Data Filters** tab, click **Add Condition**. Select a field, a conditional operator and the necessary value from the drop-down lists.

   Veeam Backup for Salesforce suggests a number of in-built conditional operators, such as *contains*, *equals*, *starts with*, *is null* and so on. These operators are used to make queries to databases. Note that the time required to process the request depends on the operator you are using, for example, processing a request with the equals operator will take less time than a request with the contains operator.

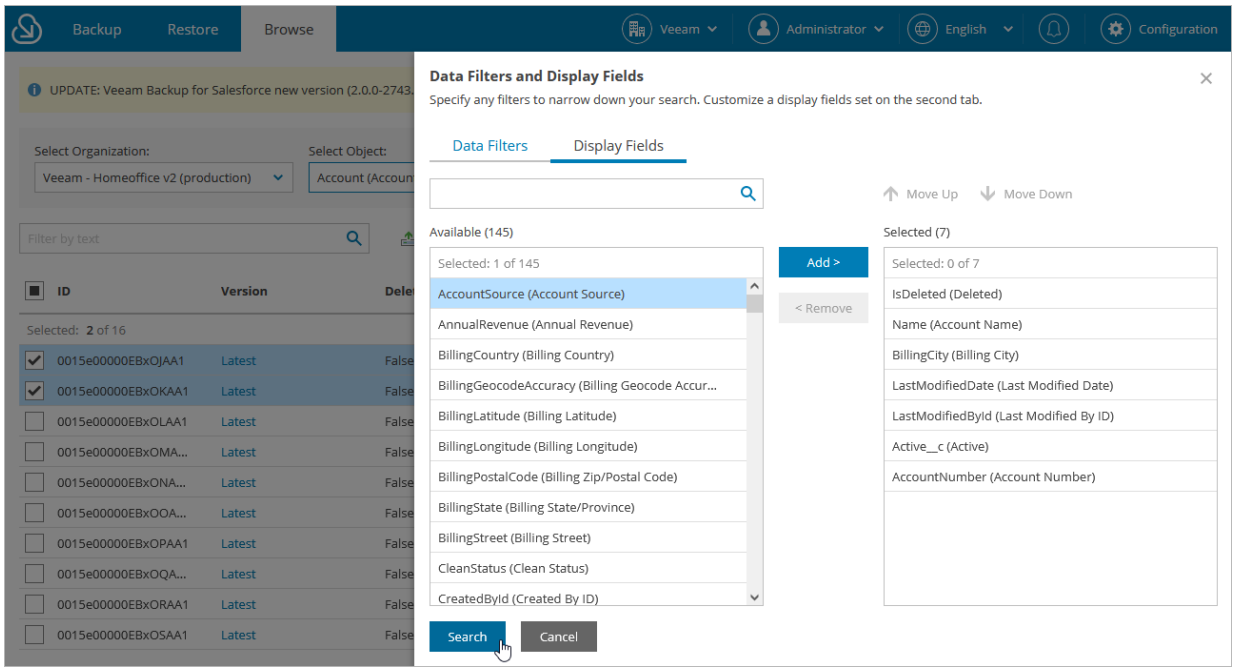
NOTE

When adding conditions, consider the following:

- To search for records with null field values, use the *is null* operator. Using the *equals* operator with an empty value is not supported.
- If you have a list of ID values, you can use the *in* operator and enter these IDs separated by a comma in the **Value** field.
- When you filter records using the lookup relationship fields, you must specify the correct ID in the **Value** field. It must be the ID of a record to which the lookup is linked.

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

4. To apply the configured settings, click **Search**.



Performing Salesforce Restore

Only users assigned the Administrator, Backup operator or Restore operator roles can perform restore operations in Veeam Backup for Salesforce. Users can perform restore operations within their permission scope — only for companies and organizations which data they have access to.

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.

In This Section

- Creating Restore Jobs
- Starting and Stopping Restore Jobs
- Cloning and 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.

Veeam Backup for Salesforce suggests you 4 restore options:

- Restore records — restores the complete records with all fields that are defined as *updatable* and *creatable* in Salesforce. You can also restore attachments associated with these records and the related objects hierarchy.
- Restore field value — restores specific field values of Salesforce records. Consider that you can only restore values of existing fields using this type of restore. If the fields were removed from Salesforce, you must perform the metadata restore first.
- Restore files — restores Salesforce files and attachments.
- Restore metadata — restores Salesforce 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:

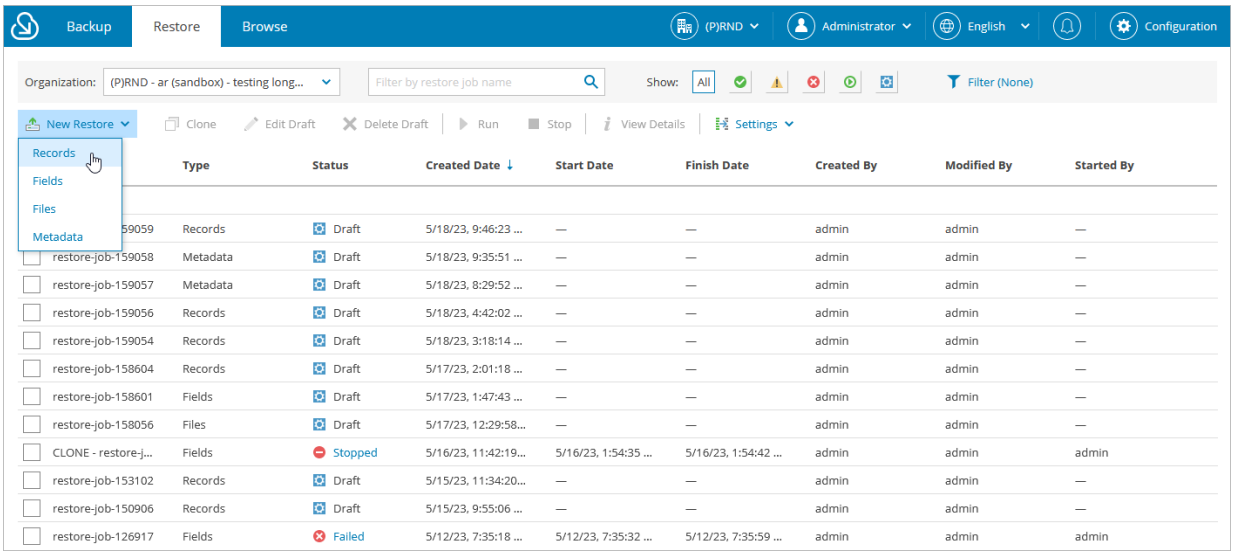
1. Launch the Restore Records wizard.
2. Specify a name and description for the restore job.
3. Select Salesforce organizations.
4. Choose the data that will be restored.
5. Choose what attachments associated with the specified records will be restored.
6. Enable restore of object hierarchy.
7. Configure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

Step 1. Launch Restore Records Wizard

To launch the **Restore Records** wizard:

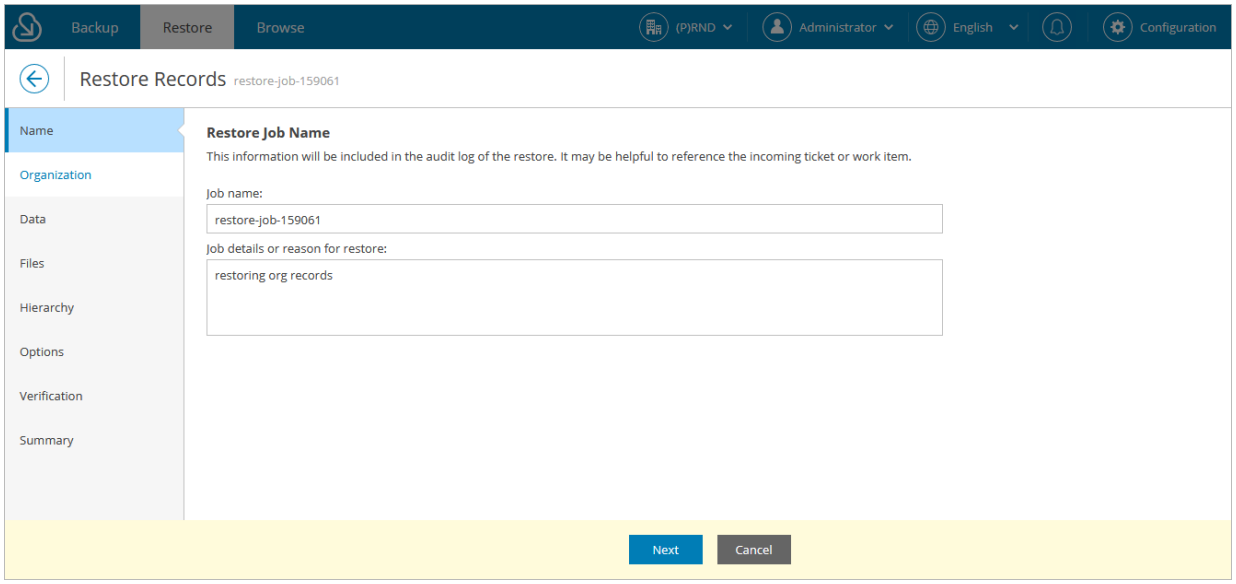
1. Navigate to the **Restore** tab.
2. Click **New Restore** > **Records**.

> **NOTE**
>
> If you have added multiple companies to Veeam Backup for Salesforce, before you launch the **Restore Records** wizard, select the company to which a Salesforce organization whose data you want to restore belongs from the company drop-down list at the top of the page.
>
> For a company to be displayed in the list, it must be added to Veeam Backup for Salesforce beforehand as described in section Adding Companies, and the user must have permissions to access the company. For more information on user permissions, see User Roles and Permissions.



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.

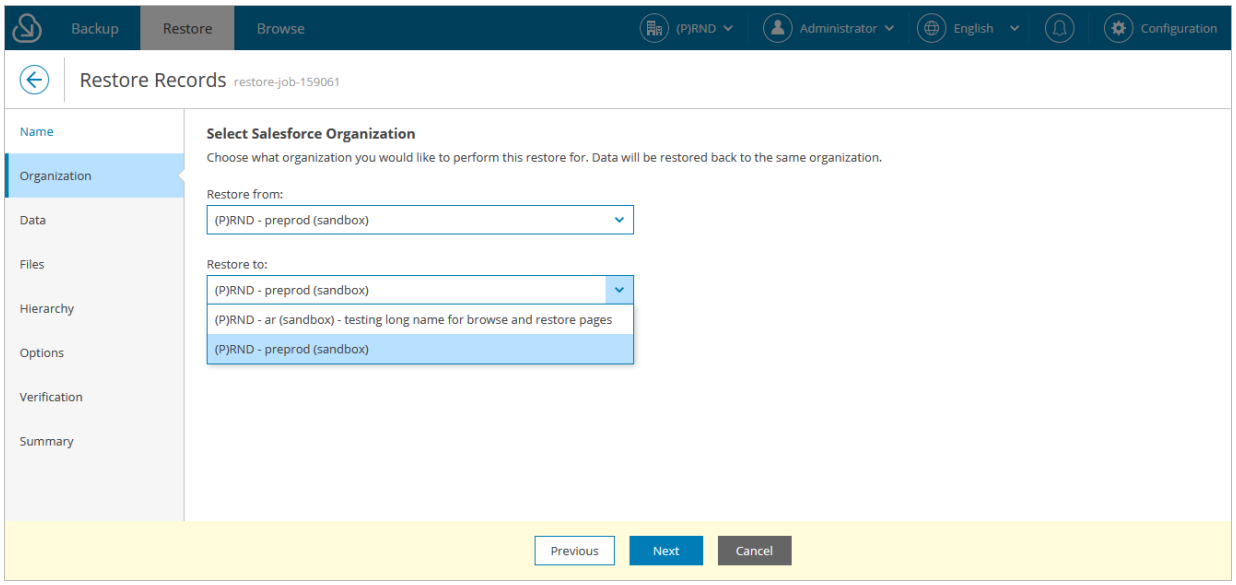


Step 3. Select Organization

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

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 populate (seed) a sandbox with backed-up data of your production or another Salesforce sandbox organization. To do that, select a Salesforce organization to which you want to restore the records from 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 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.



Step 4. Choose Data to Restore

At the **Data** step of the wizard, you can look through the backed-up data, as well as browse, filter, and choose data that you want to restore.

To choose Salesforce records for restore:

1. Specify the record search parameters.
   a. Select a Salesforce object whose records you want to restore.

      Only Salesforce objects that have been backed up are displayed at this step. If you do not see the necessary object, the object 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.
      - The object does not contain any data.
      - 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.

   b. Choose whether you want to search through the latest records or the history records of the selected object:

      - If you select *Latest records*, Veeam Backup for Salesforce will perform search only through the latest record versions.
      - If you select *History records*, Veeam Backup for Salesforce will perform search through all record versions in the history table for the time period that you specify.

   c. The records will be shown in the table with the columns that match specific Salesforce fields. To choose the displayed information, click **Customize** and select the necessary Salesforce fields on the **Display Fields** tab in the **Data Filters and Display Fields** window.
2. Apply additional search conditions using specific filters. To do that, click **Add Condition** on the **Data Filters** tab, select a field and a conditional operator from the drop-down lists, and enter the necessary value.

   Veeam Backup for Salesforce suggests a number of in-built conditional operators, such as *contains*, *equals*, *starts with*, *is null* and so on. These operators are used to make queries to databases. Note that the time required to process the request depends on the operator you are using, for example, processing a request with the *equals* operator will take less time than a request with the *contains* operator.

> **NOTE**
>
> When adding conditions, consider the following:
>
> - To search for records with null field values, use the *is null* operator. Using the *equals* operator with an empty value is not supported.
> - If you have a list of ID values, you can use the *in* operator and enter these IDs separated by a comma in the **Value** field.
> - When you filter records using the lookup relationship fields, you must specify the correct ID in the **Value** field. It must be the ID of a record to which the lookup is linked.

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

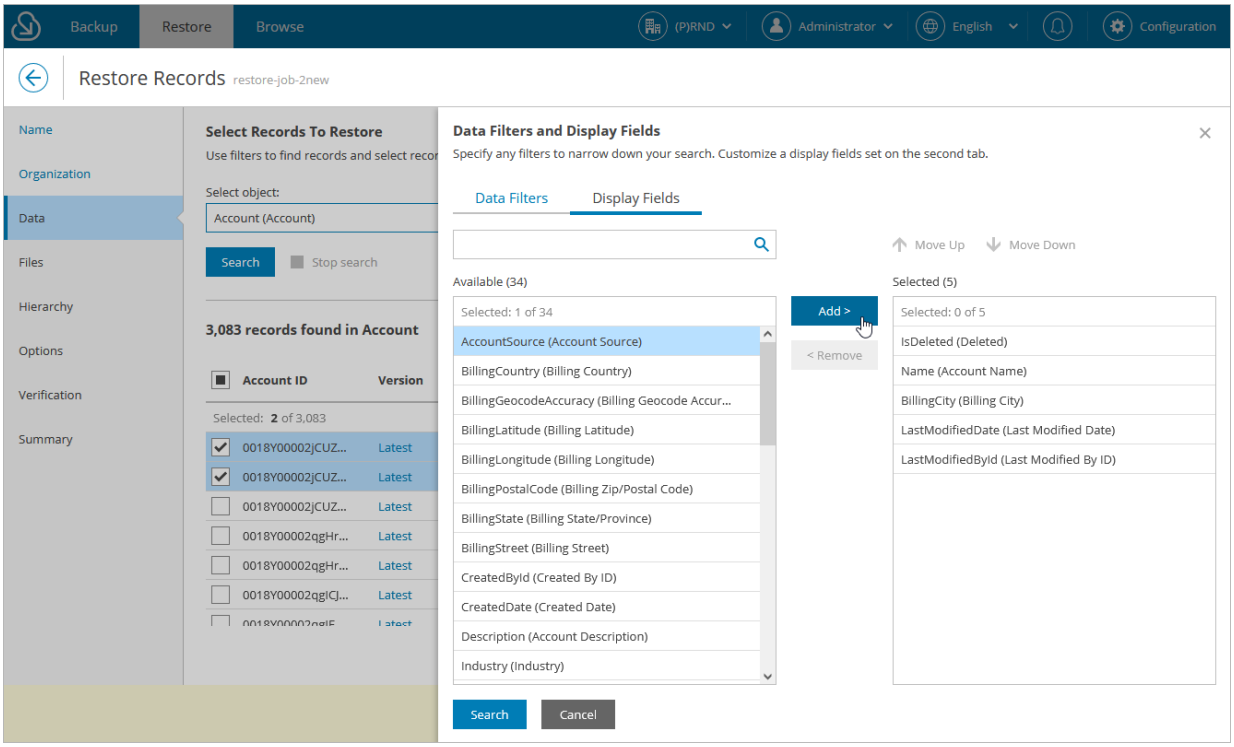
3. Click **Search**. Veeam Backup for Salesforce will show the results satisfying your search parameters in the **Records found** section.

   By design, 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 the records from the search results displayed in the **Records found** section. Consider that the section displays the maximum number of 500 records per page. It is recommended that you use filters to reduce the number of search results.

   You can 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 in the **Select Record Version to Restore** window. 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*.

> **TIP**
>
> By default, you can select up to 500,000 of records for this type of the restore job if hierarchy restore is disabled, and only up to 100 records if hierarchy restore is enabled. To change these limits, modify the `hierarchy.restore.off.max.input.records` and `hierarchy.restore.on.max.input.records` parameter values as described in section Configuring Advanced Settings.



Step 5. Choose Attachments to Restore

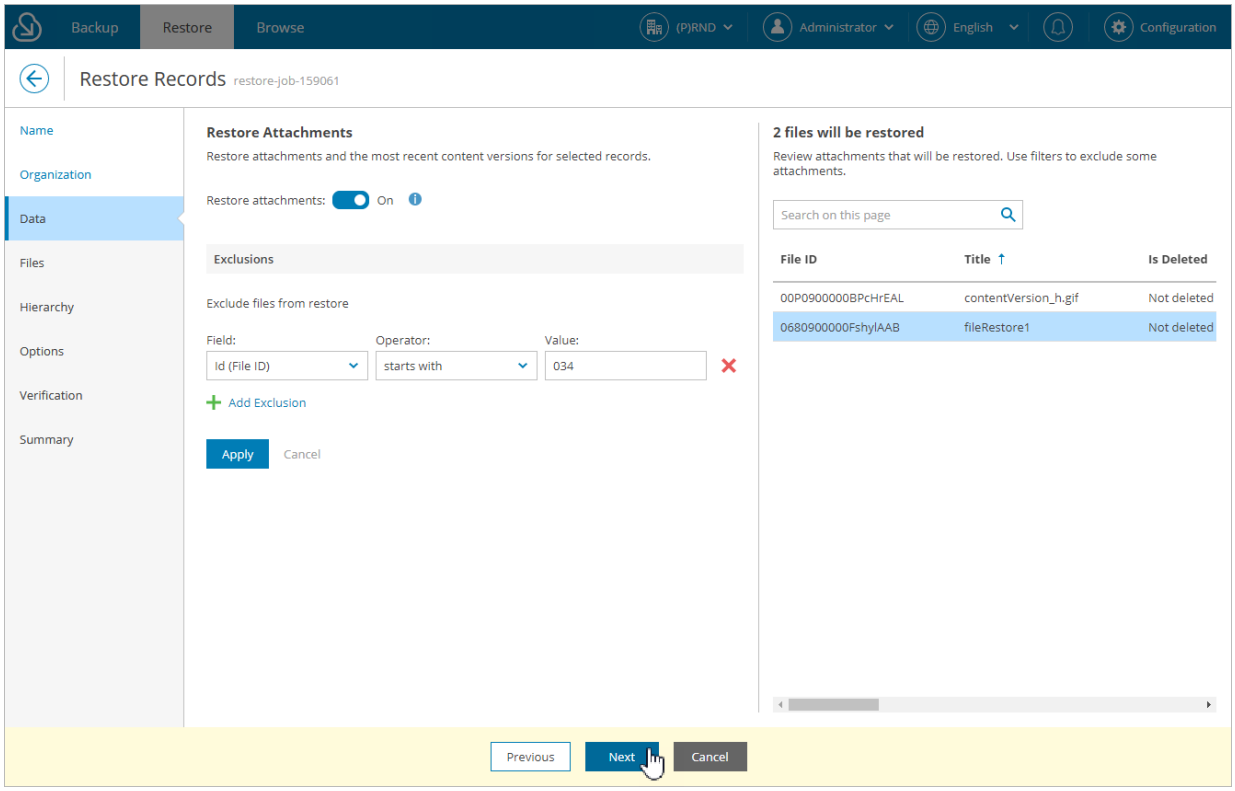
At the **Files** step of the wizard, you can instruct Veeam Backup for Salesforce to restore files associated with the selected records. Salesforce content and attachments will be displayed at this step only if the records that you restore have any associated content or attachments and these files have been backed up by Veeam Backup for Salesforce.

1. Set the **Restore attachments** toggle to *On*.

   Veeam Backup for Salesforce will display the backed-up files in the opened section.

2. You can exclude files from restore. To exclude the files, Veeam Backup for Salesforce uses filters. To add a data filter, click **Add Exclusion** in the **Exclusions** section, and specify a field, conditional operator and the necessary value. Then, click **Apply**.

   Veeam Backup for Salesforce will exclude all files that satisfy the specified filter from restore.



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, do the following:

1. Set the **Restore objects hierarchy** toggle to *On*.

> **NOTE**
>
> Hierarchy restore can affect hundreds or thousands of records in Salesforce, and restoring even a single record and validating results can be tedious. That is why if you enable the hierarchy restore functionality, you can select a maximum of 100 Salesforce records to recover in one restore session. To change this limit, modify the `hierarchy.restore.on.max.input.records` parameter value as described in section Configuring Advanced Settings.

2. To specify the child hierarchy that must be restored, do the following for each record added to the restore session:
   a. In the **Configure hierarchy for restore. Review all records.** section, select a record from the **Record** drop-down list.
   b. In the list of lookup relationships for the record, select check boxes next to the objects whose records you want to restore. Veeam Backup for Salesforce will restore records of the child objects that you have selected only — if you do not expand the object node, child objects under the node remain unselected and records of those objects will not be restored.

      You can click **Select All** at the top of the lookup relationships list to select all displayed objects. However, child objects under the closed nodes will remain unselected. To select all child objects, expand all nodes first, and then click **Select All**.

> **IMPORTANT**
>
> For the records that have not been reviewed in the Configure hierarchy for restore section, Veeam Backup for Salesforce will restore the child hierarchy to the default 1st level only. To edit the default level to which child records will be restored, modify the `hierarchy.restore.default.depth` parameter value as described in section Configuring Advanced Settings.

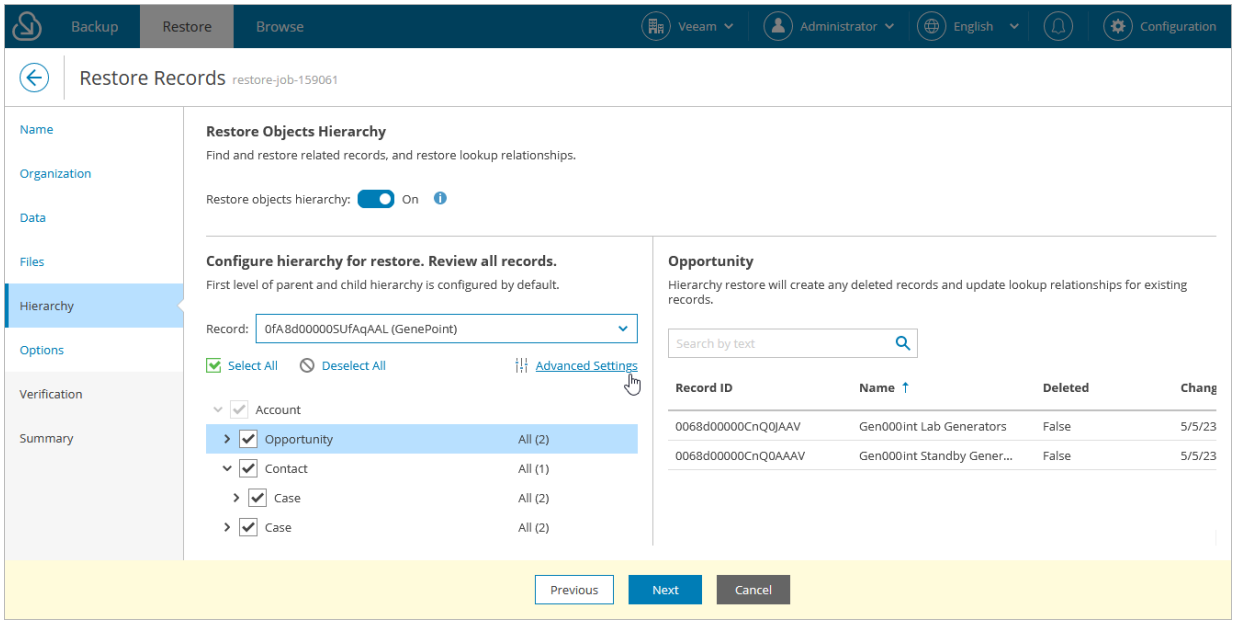
3. To configure hierarchy settings, click **Advanced Settings** in the **Configure hierarchy for restore. Review all records.** section and do the following:
   - From the **Overwrite fields** drop-down list, choose what fields will be updated for existing child records:
     - To update only the parent lookup fields of the existing child records, select *Parent lookup only*.
     - To update all fields of the existing child records, select *All fields*.

- Not to update fields of the existing child records, select *None*.

- From the **Stop processing hierarchy** 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 *Exists*. This child record will be the last updated record. Keep in mind that it will be updated according to the selected **Overwrite fields** 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 *Correct lookup*. This child record will be the last updated record. Keep in mind that it will be updated according to the selected **Overwrite fields** 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 *All fields match*.
  - To proceed with hierarchy restore until all the selected child records are updated, select *Never*.
- From the **Restore parent hierarchy** drop-down list, 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. To edit the default level, modify the `hierarchy.max.parents.restore` parameter value as described in section Configuring Advanced Settings.

  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.

> **NOTE**
>
> The product restores child and parent records of the versions that you selected at step 4.



How Veeam Backup for Salesforce Restores Object Hierarchy

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

- This record refers to another record in 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 in 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 1st level child records only (that is, 2 records in the **Case** object in our example). However, you can instruct Veeam Backup for Salesforce to restore child records of deeper hierarchy levels (records in the **CaseMilestone** object) 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.

Step 7. Configure Additional Restore Settings

At the **Options** step of the wizard, specify additional restore settings:

1. To allow Veeam Backup for Salesforce to overwrite field values of the existing records in Salesforce during restore, select the **Restore field values for records. Job setting applies to all restored records** check box.

   For the existing Salesforce records that contain values other than *null*, the product does not replace the values with *null*. To replace the values with *null*, select the **Restore empty field values. Empty field values from backup will replace current values on records** check box.

2. To manually override values of specific fields in all restored records, click the link in the **Override field values** field. In the **Override field values for selected records** window, click **Add Field**, select the field for which you want to specify value from the **Field** drop-down list, and provide the necessary value. Then, click **Apply**. For example, it can be used for sandbox seeding when you need to mask sensitive data.

   If you want to restore the value of the field saved in the restore point and add comments to it, you can use the following format: `<text> {value}`, where `<text>` — is the text that you want to add to the backed-up field value. For example, if the backed-up value of the **Name** field is *Account1*, and you select this field and specify the following value to override: *New {value}*, then the restored value of the field will be *New Account1*.

   Consider that Veeam Backup for Salesforce will override field values for the records selected at step 4 only.

> **IMPORTANT**
>
> When overriding time values, consider that you specify time in the UTC time zone and this value will be displayed in Salesforce according to the time zone set on the Salesforce site.

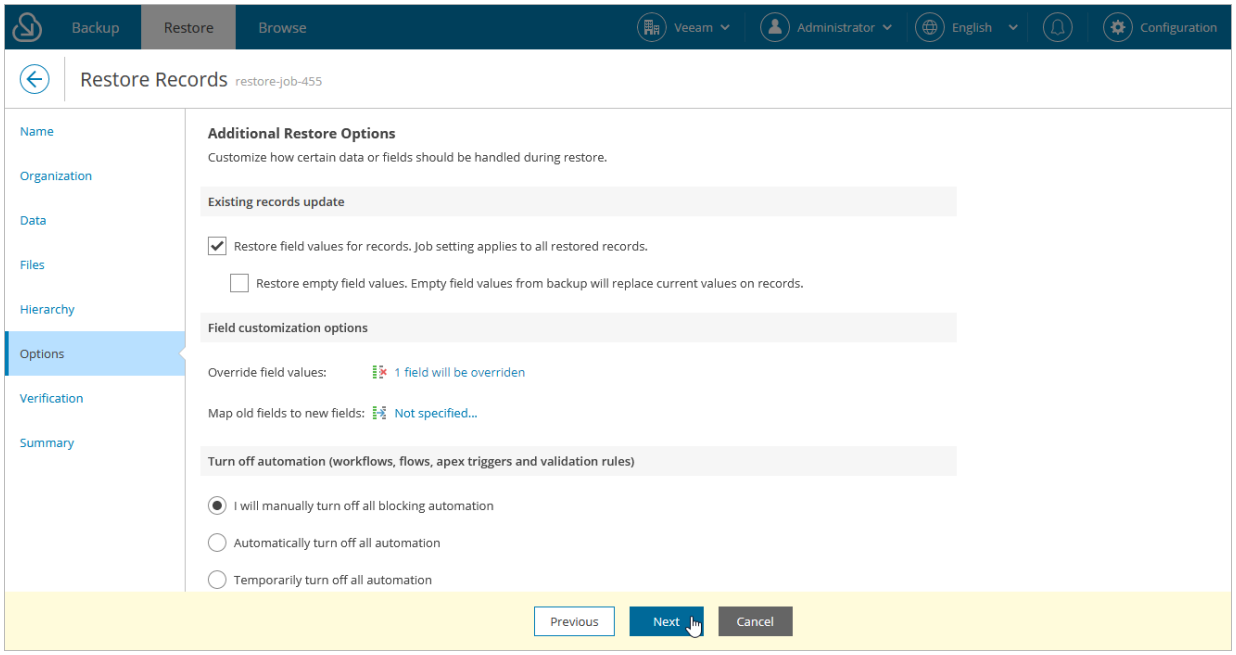
3. You can map fields to other Salesforce fields if you want to restore the values from the backup to the different fields. To do that, click **Map old fields to new fields**. In the **Map Fields** window, click **Add Field**, select the field from backup that you want to map to a new one, and specify the Salesforce field to which it will be mapped. Then, click **Apply**.

   Consider that you can configure mapping only for existing Salesforce fields of the records selected at step 4. If you removed a field from Salesforce, you cannot map it to another field.

4. 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.

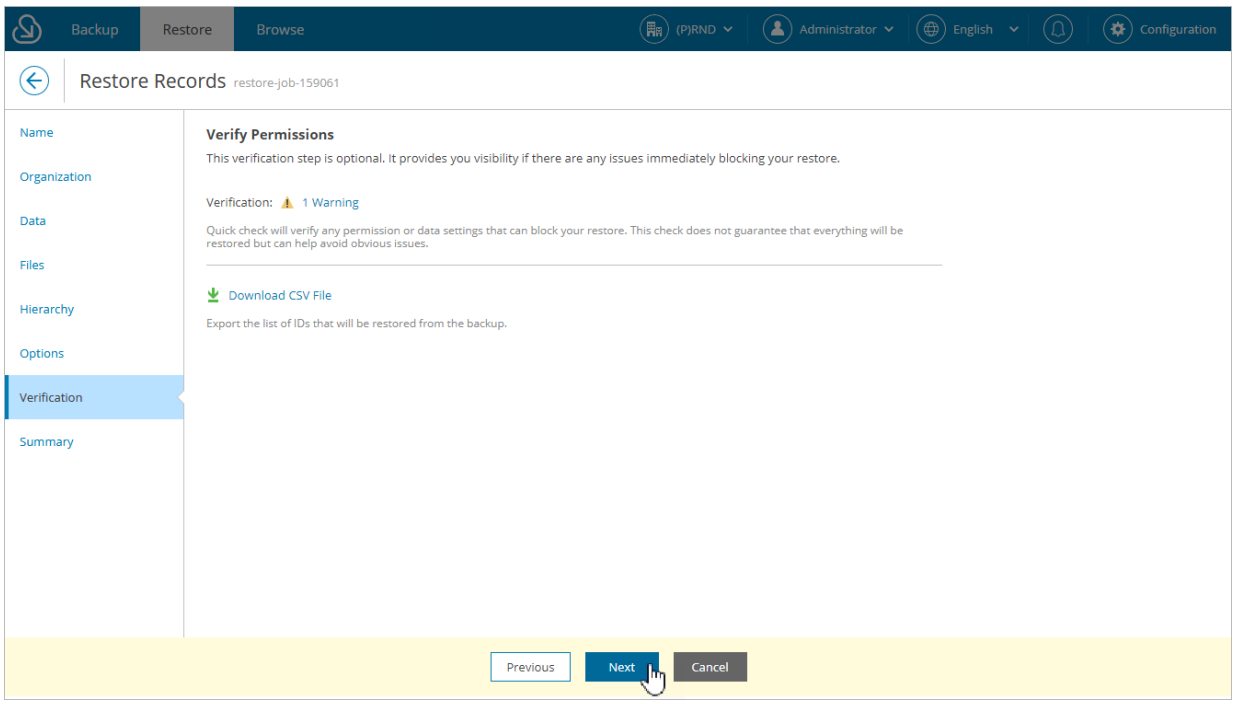
- Select the **Temporarily turn off all automation** option to automatically update Flows, Validation Rules and Apex Triggers so that they are bypassed while the product performs the current restore operation only without impacting the Salesforce functionality. All changes made by the product will be 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.



Step 8. Check Permissions

At the **Verification** step of the wizard, you can run an automated check for the user permissions and the Salesforce object selected for restore. To do that, click the **Not verified yet** link.

To export the list that contains all fields of the records selected at step 4 of the wizard, click **Download CSV File**. Veeam Backup for Salesforce will export all the record fields to a CSV file and download it to your local machine.

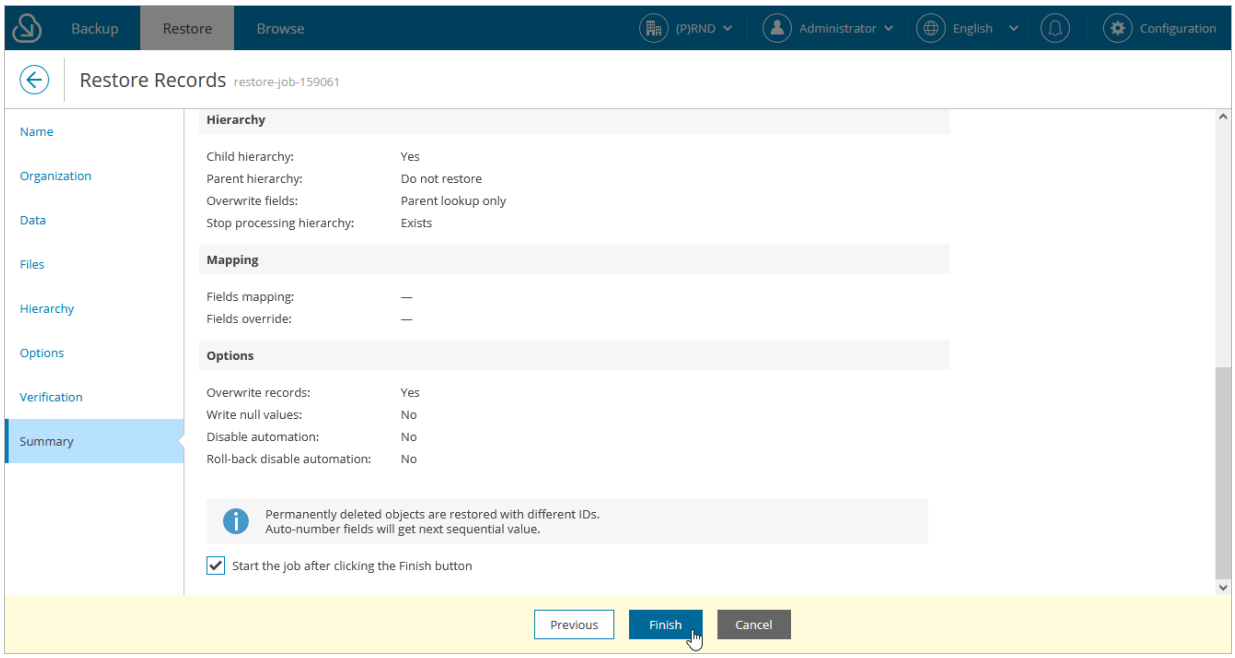


Step 9. Finish Working with Wizard

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.



Restoring Field Values

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

> **IMPORTANT**
>
> You can only restore values of existing fields using this type of restore. If the fields were removed from Salesforce, you must perform the metadata restore first.

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

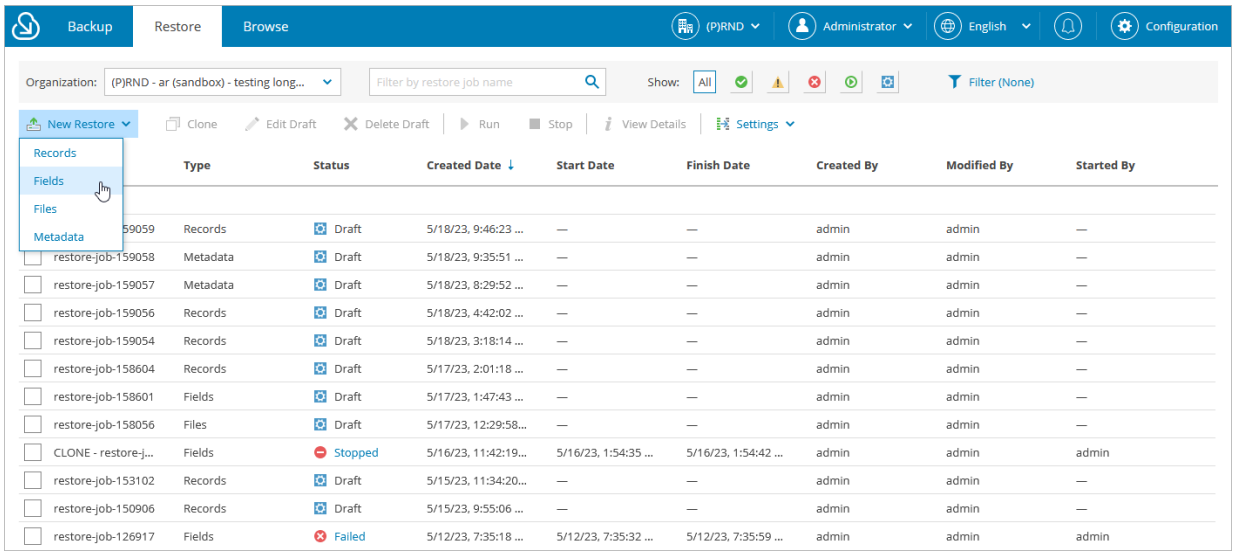
1. Launch the Restore Field Values wizard.
2. Specify a name and description for the restore job.
3. Select Salesforce organizations.
4. Select records whose field values you want to restore.
5. Select fields whose values will be restored.
6. Configure additional restore settings.
7. Check permissions.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

Step 1. Launch Restore Field Values Wizard

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

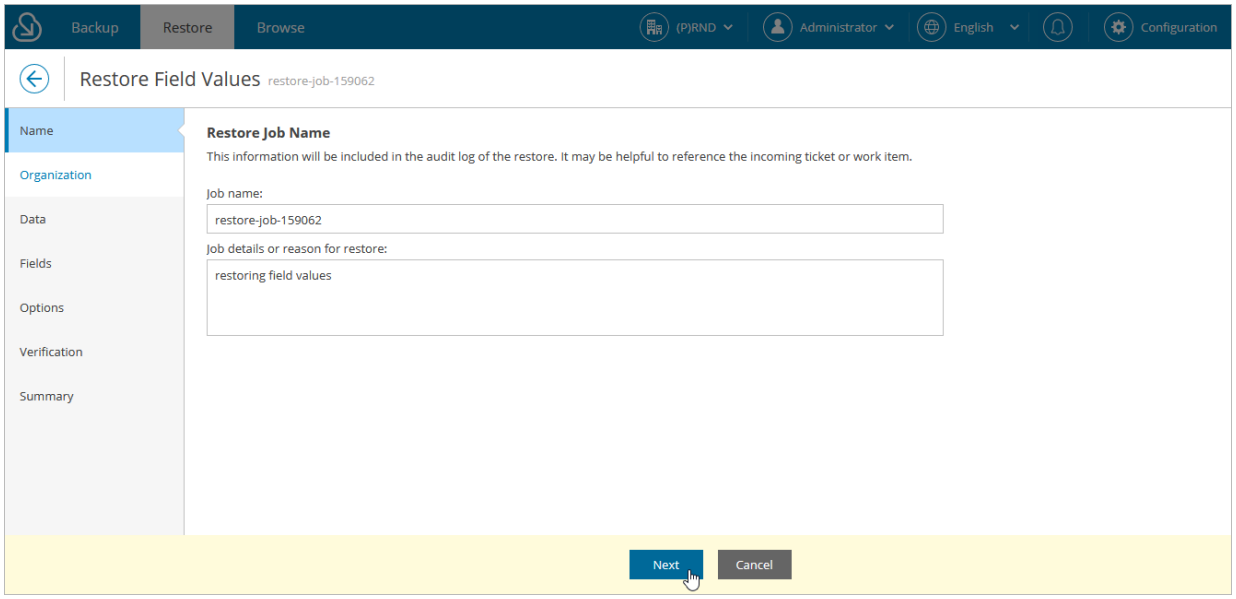
1. Navigate to the **Restore** tab.
2. Click **New Restore** > **Fields**.

> **NOTE**
>
> If you have added multiple companies to Veeam Backup for Salesforce, before you launch the **Restore Field Values** wizard, select the company to which a Salesforce organization whose data you want to restore belongs from the company drop-down list at the top of the page.
>
> For a company to be displayed in the list, it must be added to Veeam Backup for Salesforce beforehand as described in section Adding Companies, and the user must have permissions to access the company. For more information on user permissions, see User Roles and Permissions.



Step 2. Specify Restore Job Info

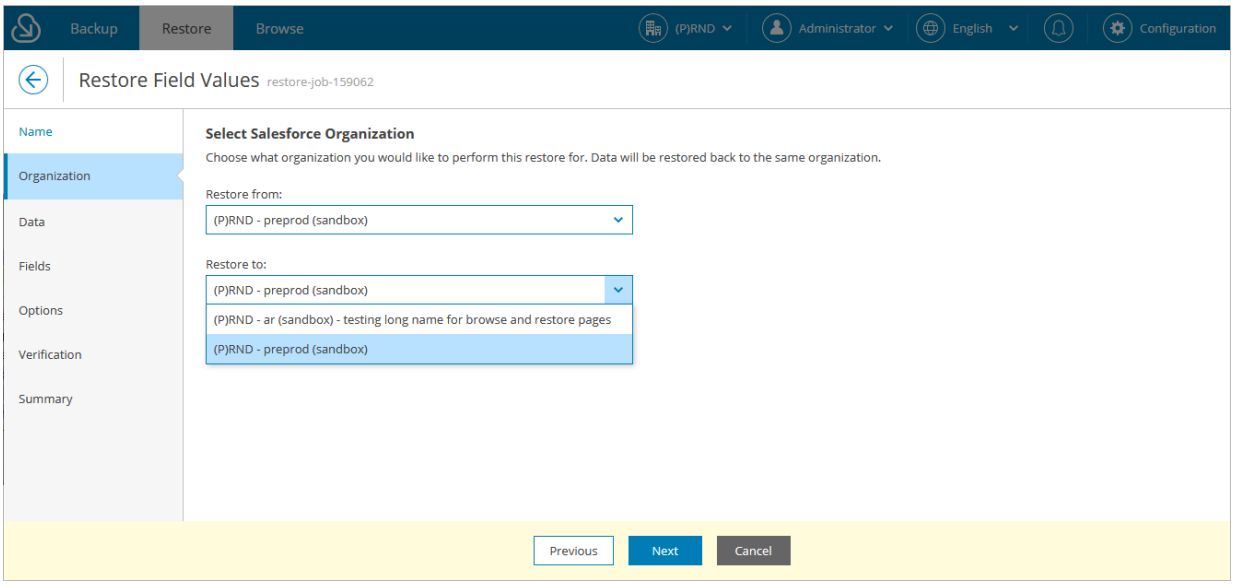
At the **Name** step of the wizard, use the **Job name** and **Job details or reason for restore** fields to specify a name for the new restore job and to provide a description for future reference.



Step 3. Select Organization

At the **Organization** step of the wizard, select a Salesforce organization whose field values you want to restore from the **Restore from** drop-down list. 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, select a Salesforce organization to which you want to restore the field values from 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.



Step 4. Choose Data to Restore

At the **Data** step of the wizard, you can look through the backed-up data, as well as browse, filter, and choose data that you want to restore.

To choose Salesforce records whose field values you want to restore:

1. Specify the record search parameters.
   a. Select a Salesforce object whose record fields you want to restore.

      Only Salesforce objects that have been backed up are displayed at this step. If you do not see the necessary object, the object 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.
      - The object does not contain any data.
      - 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.

   b. Choose whether you want to search through the latest records or the history records of the selected object:

      - If you select *Latest records*, Veeam Backup for Salesforce will perform search only through the latest record versions.
      - If you select *History records*, Veeam Backup for Salesforce will perform search through all record versions in the history table for the time period that you specify.

   c. The records will be shown in the table with the columns that match specific Salesforce fields. To choose the displayed information, click **Customize** and select the necessary Salesforce fields on the **Display Fields** tab in the **Data Filters and Display Fields** window.
2. Apply additional search conditions using specific filters. To do that, click **Add Condition** on the **Data Filters** tab, select a field and a conditional operator from the drop-down lists, and enter the necessary value.

   Veeam Backup for Salesforce suggests a number of in-built conditional operators, such as *contains*, *equals*, *starts with*, *is null* and so on. These operators are used to make queries to databases. Note that the time required to process the request depends on the operator you are using, for example, processing a request with the *equals* operator will take less time than a request with the *contains* operator.

> **NOTE**
>
> 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.
> - To search for records with null field values, use the *is null* operator. Using the *equals* operator with an empty value is not supported.
> - If you have a list of ID values, you can use the *in* operator and enter these IDs separated by a comma in the **Value** field.
> - When you filter records using the lookup relationship fields, you must specify the correct ID in the **Value** field. It must be the ID of a record to which the lookup is linked.

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

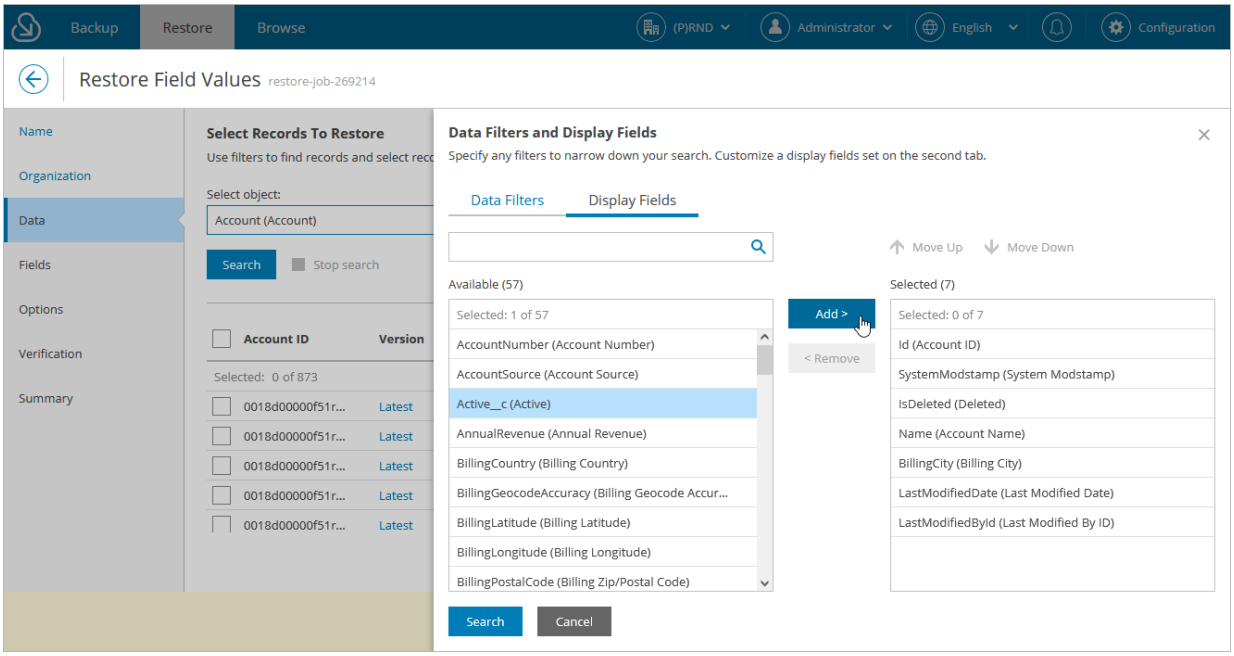
3. Click **Search**. Veeam Backup for Salesforce will show the results satisfying your search parameters in the **Records found** section.

   By design, 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 the records from the search results in the **Records found** section. Consider that the section displays the maximum number of 500 records per page. It is recommended that you use filters to reduce the number of search results.

   You can 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 with previous backed-up record versions and the version of the record currently stored in the Salesforce database, and select the necessary version in the **Select Record Version to Restore** window. 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*.

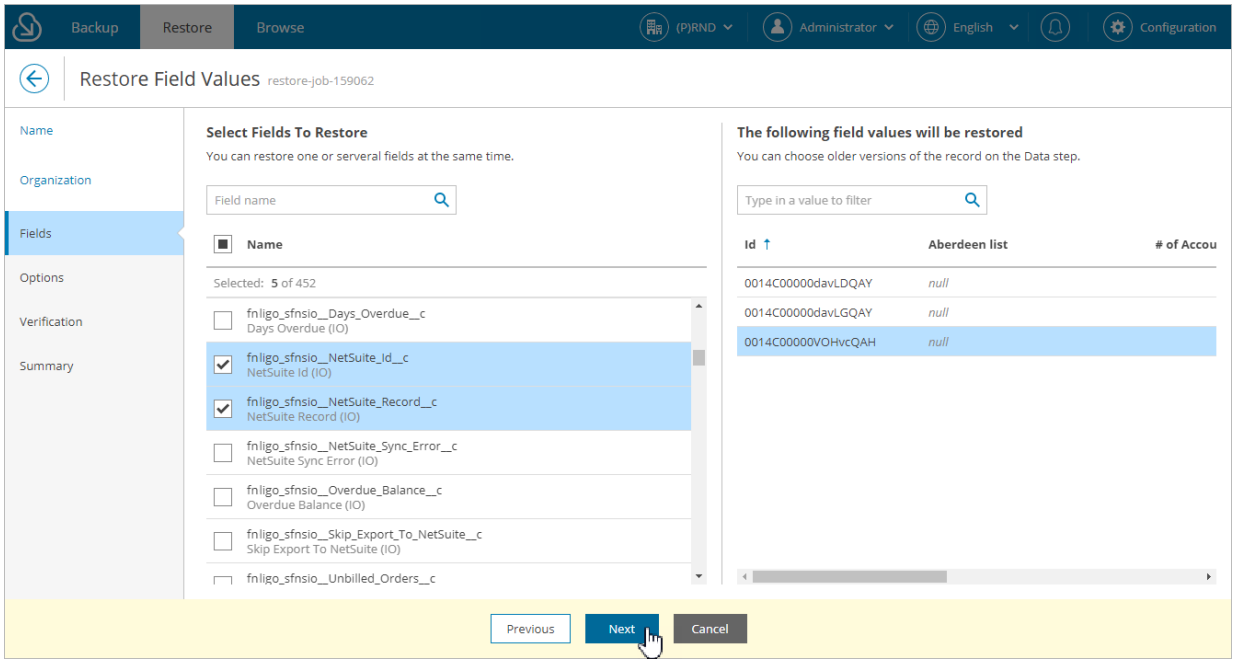
> **TIP**
>
> By default, you can select up to 500,000 of records for one field value restore session. To change this limit, modify the `fields.restore.max.input.records` parameter value as described in section Configuring Advanced Settings.



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, specify additional restore settings:

1. To allow Veeam Backup for Salesforce to overwrite field values during restore, select the **Restore field values for records. Job setting applies to all restored records** check box.

   For the existing Salesforce records that contain values other than *null*, the product does not replace the values with *null*. To replace the values with *null*, select the **Restore empty field values. Empty field values from backup will replace current values on records** check box.

2. To manually override values of specific fields in all restored records, click **Override field values**. In the **Override field values for selected records** window, click **Add field**, select the field for which you want to specify value from the **Field** drop-down list, and provide the necessary value. Then, click **Apply**.

   If you want to restore the value of the field saved in the restore point and add comments to it, you can use the following format: `<text> {value}`, where `<text>` — is the text that you want to add to the backed-up field value. For example, if the backed-up value of the **Name** field is *Account1*, and you select this field and specify the following value to override: *New {value}*, then the restored value of the field will be *New Account1*.

> **IMPORTANT**
>
> When overriding time values, consider that you specify time in the UTC time zone and this value will be displayed in Salesforce according to the time zone set on the Salesforce site.

3. You can map fields to other Salesforce fields if you want to restore the values from the backup to the different fields. To do that, click **Map old fields to new fields**. In the **Map Fields** window, click **Add Field**, select the field from backup that you want to map to a new one, and specify the Salesforce field to which it will be mapped. Then, click **Apply**.

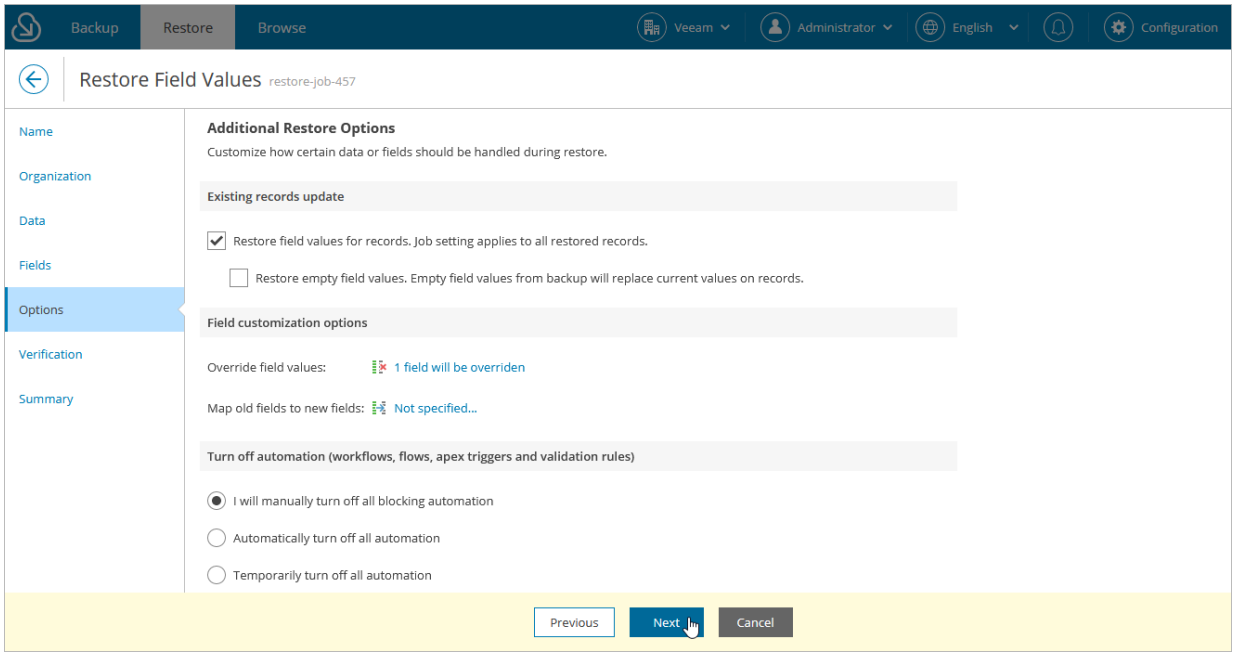
   Consider that you can configure mapping only for existing Salesforce fields. If you removed a field from Salesforce, you cannot map it to another field.

4. Business logic and automated rules configured in Salesforce can block Veeam Backup for Salesforce restore operations or trigger undesirable side processes. You can choose to manually handle the Salesforce automation exceptions or to let the product permanently or temporarily disable all triggered automation for the user that is executing the backup and restore operations. To do that, select one of the automation modes in the **Turn off automation** section:

   - Select the **I will manually turn off all blocking automation** option, if you want to disable Flows and inactivate Validation Rules and Apex Triggers on the Salesforce side or add the Salesforce user whose permissions are used to perform backup and restore operations to exclusions manually.
   - Select the **Automatically turn off all automation** option, to automatically disable all blocking automation for the Salesforce user whose permissions are used to perform backup and restore operations. The user will be added to exclusions for all configured automation functionality without specifying any time period.

     This functionality will be disabled in Veeam Backup for Salesforce during the restore operation only, and then it will be enabled again. When you select this option again, it will take less time to disable automation because all the changes have been already saved in the Salesforce medatada.

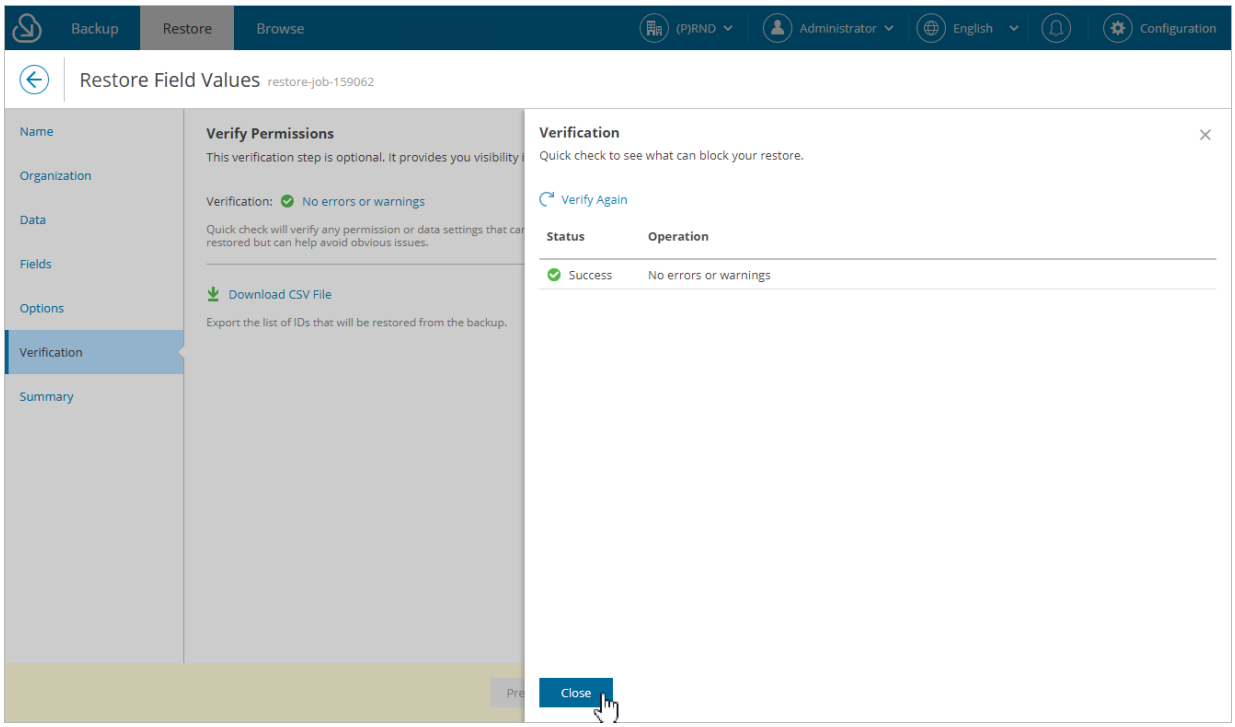
- Select the **Temporarily turn off all automation** option, to temporarily disable all blocking automation for the Salesforce user whose permissions are used to perform backup and restore operations. The automation functionality will be disabled only for the restore operation duration, and then it will be enabled again. Note that each operation of disabling and enabling of automation my take significant time to complete.



Step 7. Check Permissions

At the **Verification** step of the wizard, you can run an automated check for the user permissions and the Salesforce object selected for restore. To do that, click the **Not verified yet** link.

To export the list that contains all fields of the records selected at step 4 and included in the restore job, click **Download CSV File**. Veeam Backup for Salesforce will export all the record fields to a CSV file and download it to your local machine.

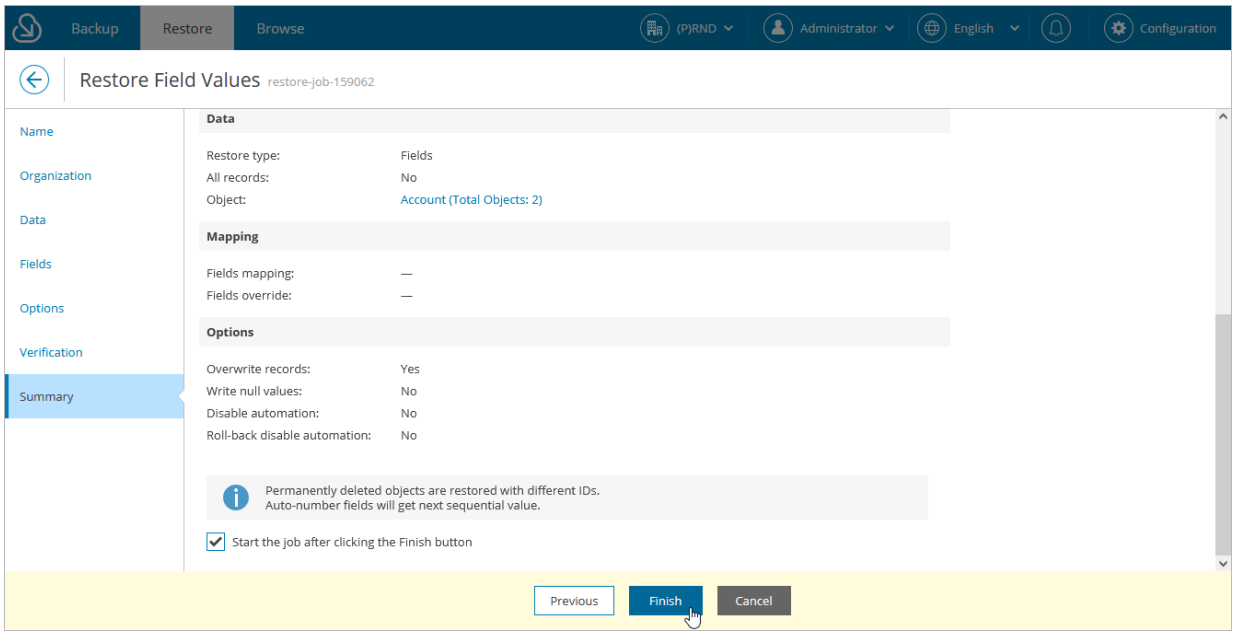


Step 8. Finish Working with Wizard

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.



Restoring Files

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

> **IMPORTANT**
>
> Consider the following:
>
> - When you restore a content version, Salesforce will create a new version for this Content Document.
> - When you restore an attachment, Veeam Backup for Salesforce will create a new file with the same file name and new ID. If the source file still exists, the file content will be 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:

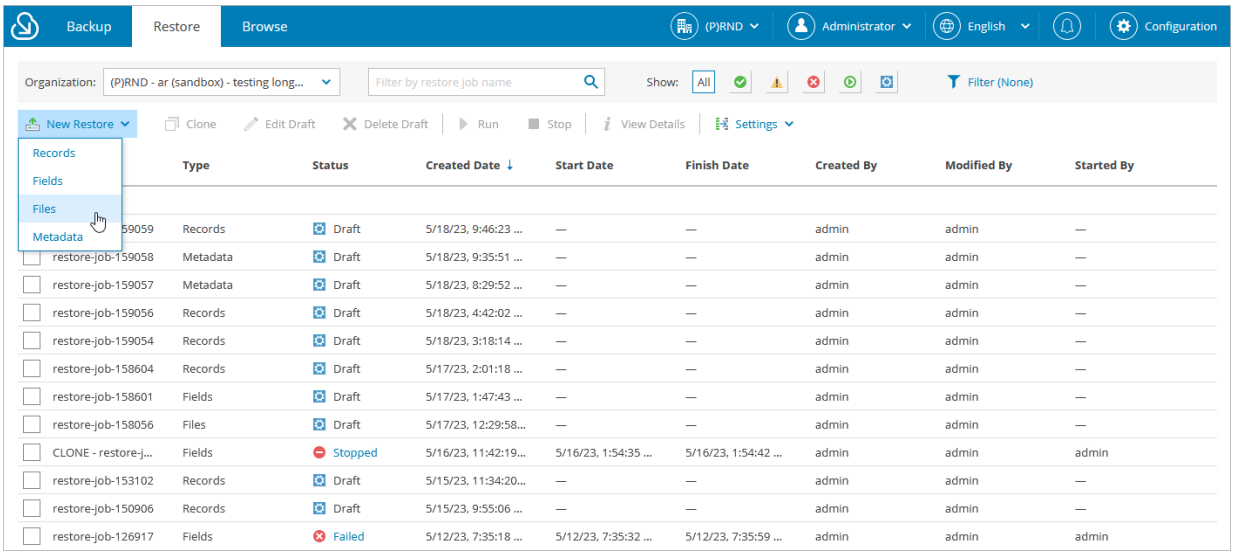
1. Launch the Restore Files wizard.
2. Specify a name and description for the restore job.
3. Select Salesforce organizations.
4. Select files and attachments to restore.
5. Finish working with the wizard.

Step 1. Launch Restore Files Wizard

To launch the **Restore Files** wizard:

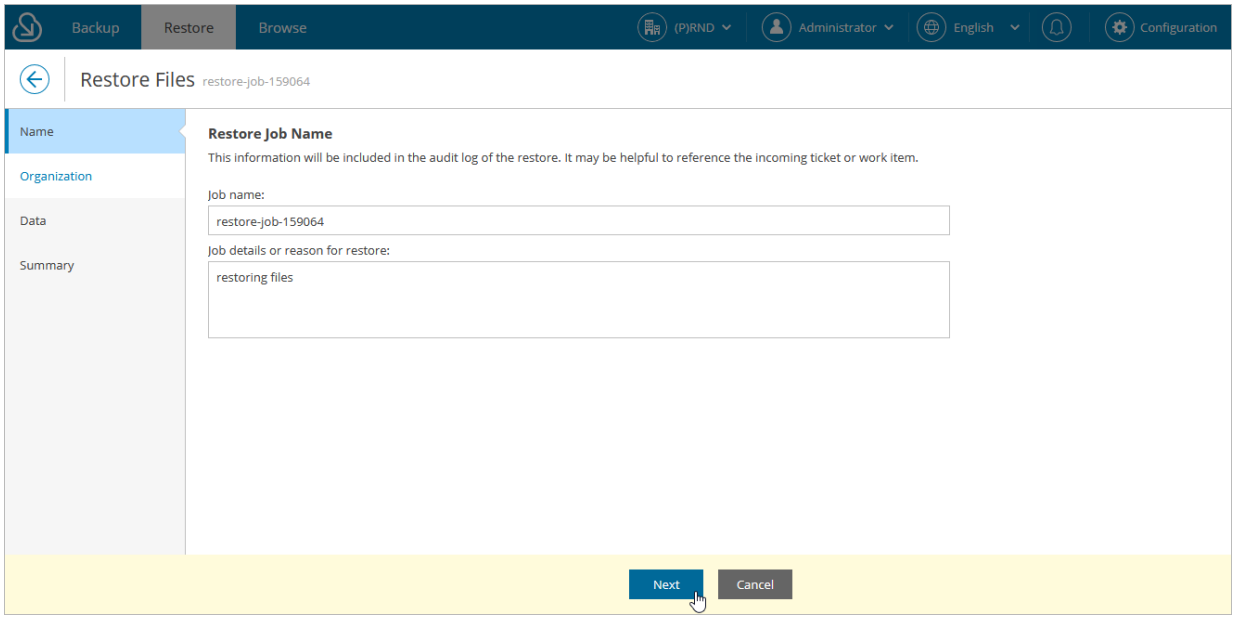
1. Navigate to the **Restore** tab.
2. Click **New Restore** > **Files**.

> **NOTE**
>
> If you have added multiple companies to Veeam Backup for Salesforce, before you launch the **Restore Files** wizard, select the company to which a Salesforce organization whose data you want to restore belongs from the company drop-down list at the top of the page.
>
> For a company to be displayed in the list, it must be added to Veeam Backup for Salesforce beforehand as described in section Adding Companies, and the user must have permissions to access the company. For more information on user permissions, see User Roles and Permissions.



Step 2. Specify Restore Job Info

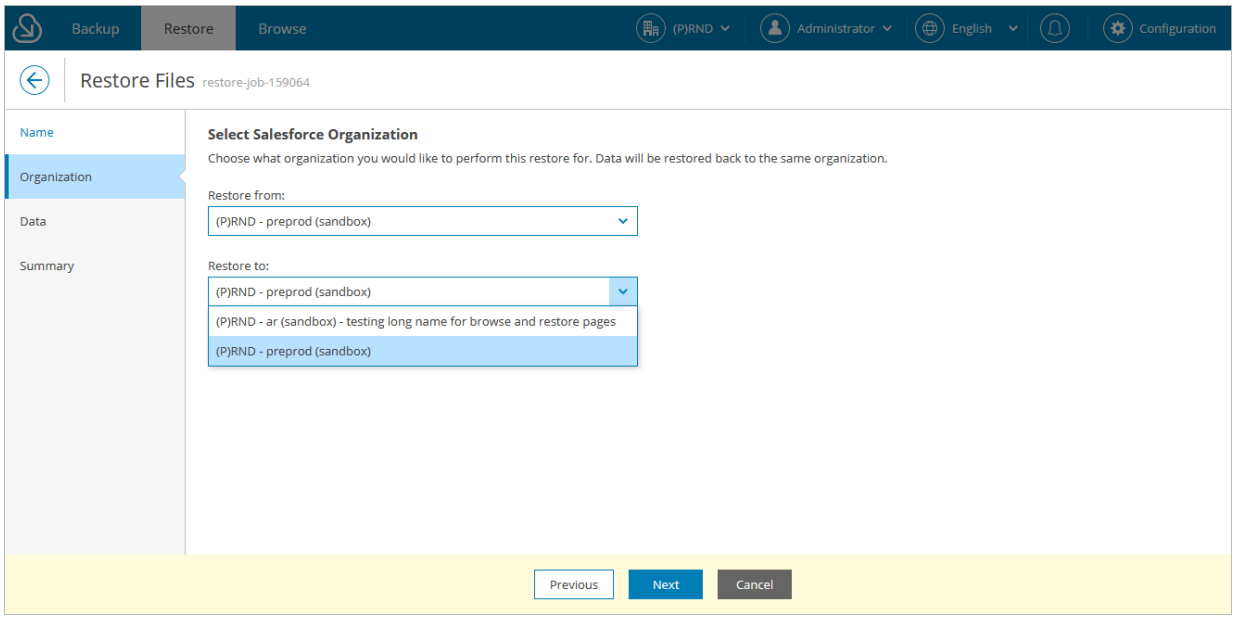
At the **Name** step of the wizard, use the **Job name** and **Job details or reason for restore** fields to specify a name for the new restore job and to provide a description for future reference.



Step 3. Select Organization

At the **Organization** step of the wizard, select a Salesforce organization whose files and attachments you want to restore from the **Restore from** drop-down list. 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, select a Salesforce organization to which you want to restore files and attachments from 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.



Step 4. Select Files to Restore

At the **Data** step of the wizard, you can look through the backed-up data, as well as browse, filter, and choose data that you want to restore. Only files that have been backed up are displayed at this step.

To choose files for restore:

1. Specify the file search parameters.

   a. From the **Search in** drop-down list, select a type of the restored files. If you select the *Attachment* or *Content Version* type of files, you will be able to specify an object with which the files must be associated.

   For a type of files to be displayed in the list, it must be backed-up by a backup policy for the organization selected at step 3 of the wizard.

   c. The results will be shown in the table with the columns that match specific Salesforce fields. To choose the displayed information, click **Customize** and select the necessary Salesforce fields on the **Display Fields** tab in the **Data Filters and Display Fields** window.

2. Apply additional search conditions using specific filters. To do that, click **Add Condition** on the **Data Filters** tab, select a field and a conditional operator from the drop-down lists, and enter the necessary value.

   Veeam Backup for Salesforce suggests a number of in-built conditional operators, such as *contains*, *equals*, *starts with*, *is null* and so on. These operators are used to make queries to databases. Note that the time required to process the request depends on the operator you are using, for example, processing a request with the *equals* operator will take less time than a request with the *contains* operator.

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

3. Click **Search**. Veeam Backup for Salesforce will show the results satisfying your search parameters in the **Records found** section.

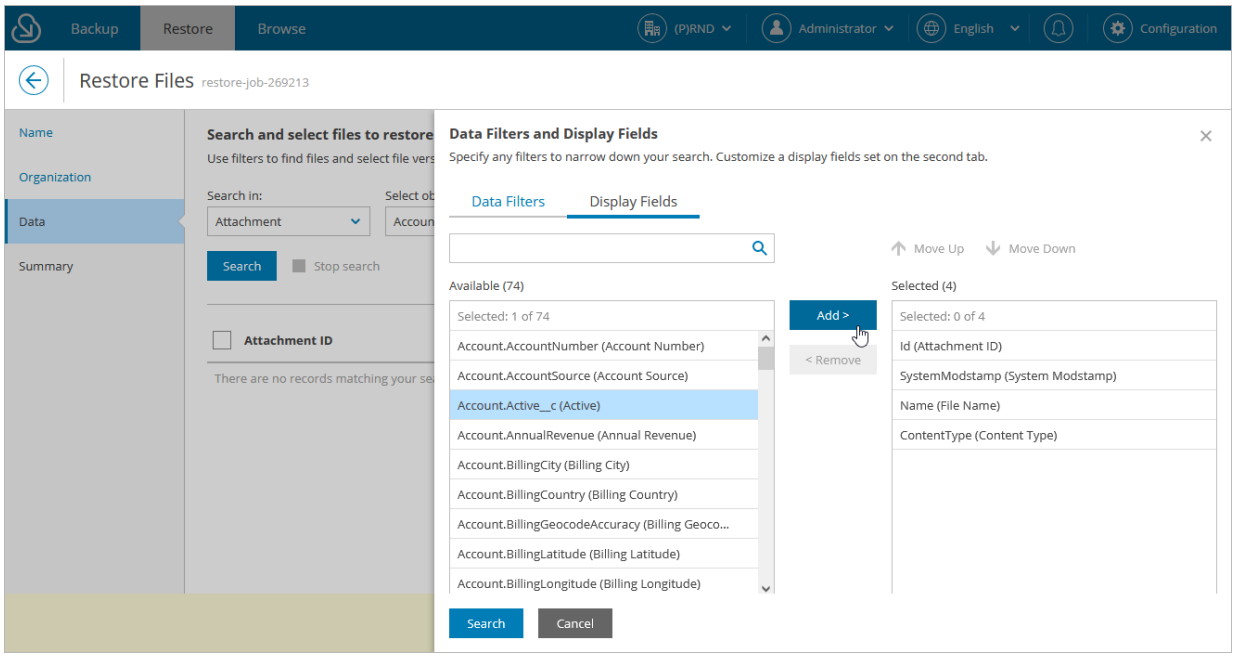
   By design, the search results will be displayed on the same pages where the records were originally shown. To make sure that you have seen all the results, look through all the pages.

4. Select the files from the search results displayed in the **Records found** section. Consider that the section displays the maximum number of 500 records per page. You cannot select and add files to the restore session from different pages. That is why it is recommended that you use filters to reduce the number of search results.

   For the *Content Version* type of files, you can 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 with previous backed-up file versions and the version of the file currently stored in the Salesforce database, and select the necessary version in the **Select Record Version to Restore** window. 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**.

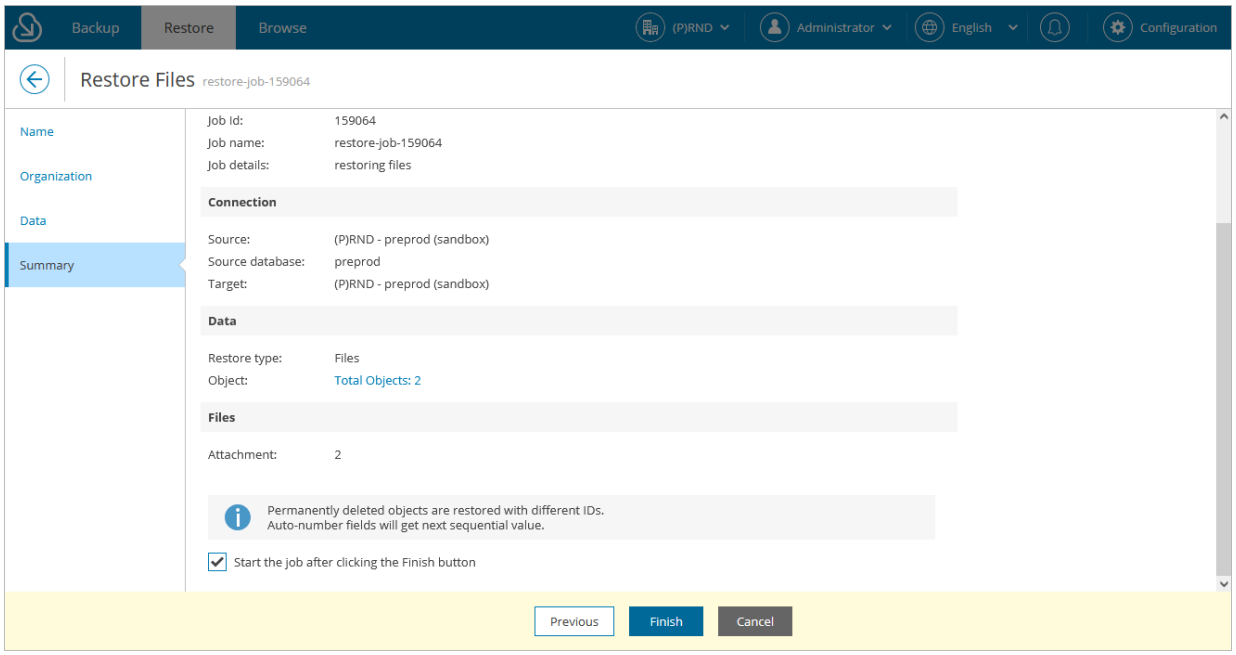


Step 5. Finish Working with Wizard

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.



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:

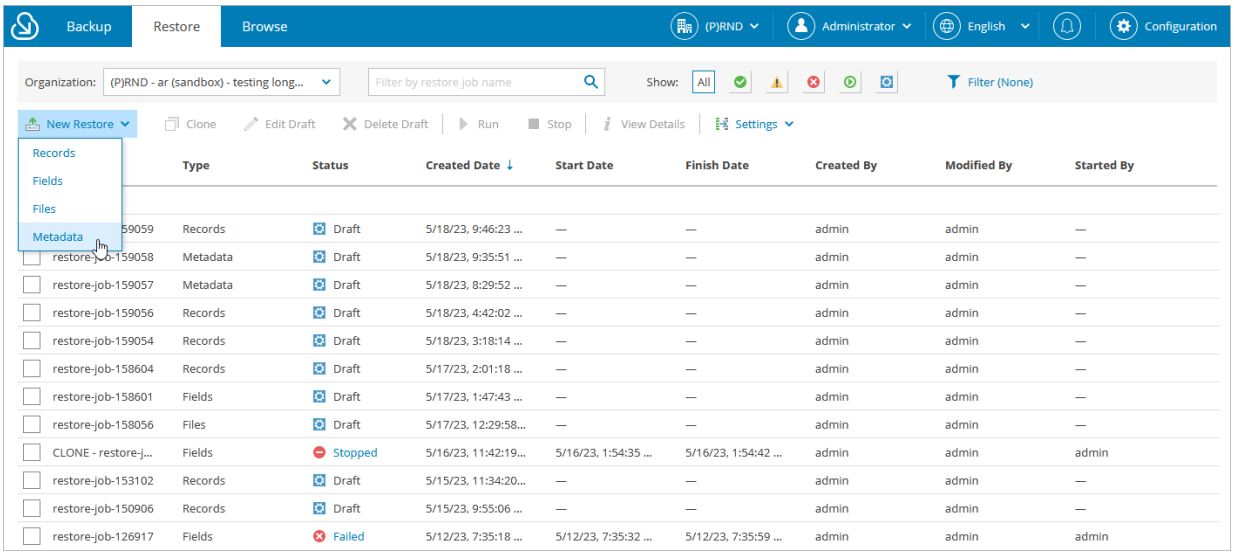
1. Launch the Restore Metadata wizard.
2. Specify a name and description for the restore job.
3. Select Salesforce organizations.
4. Select objects whose metadata will be restored.
5. Review the restore list.
6. Finish working with the wizard.

Step 1. Launch Restore Metadata Wizard

To launch the **Restore Metadata** wizard:

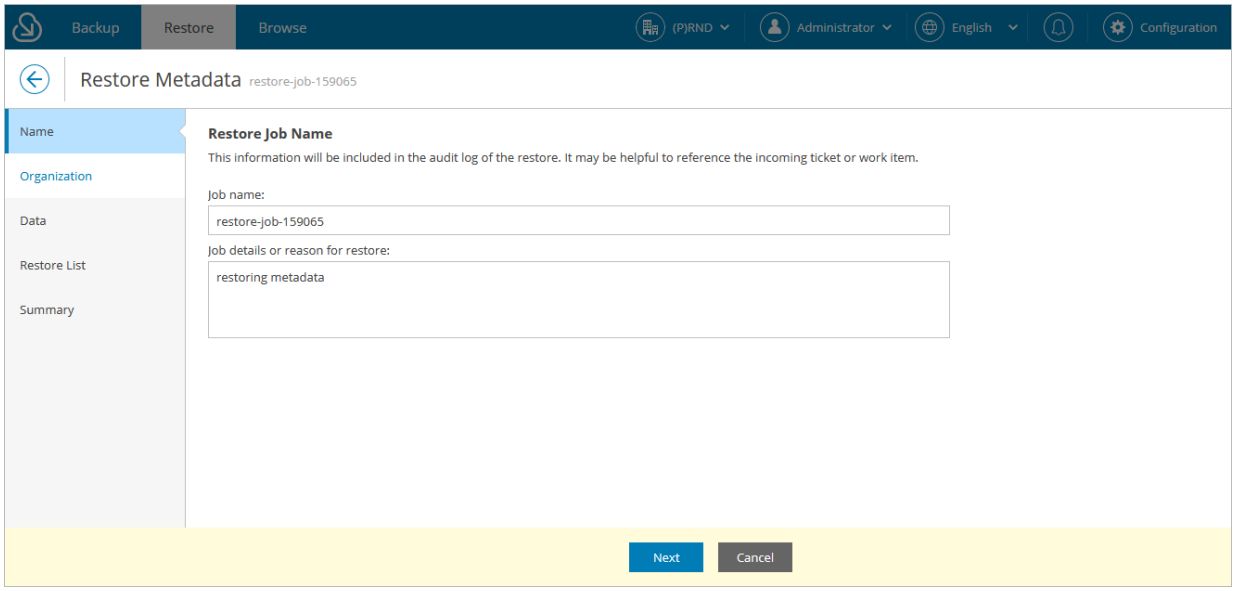
1. Navigate to the **Restore** tab.
2. Click **New Restore** > **Metadata**.

> **NOTE**
>
> If you have added multiple companies to Veeam Backup for Salesforce, before you launch the **Restore Metadata** wizard, select the company to which a Salesforce organization whose data you want to restore belongs from the company drop-down list at the top of the page.
>
> For a company to be displayed in the list, it must be added to Veeam Backup for Salesforce beforehand as described in section Adding Companies, and the user must have permissions to access the company. For more information on user permissions, see User Roles and Permissions.



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.

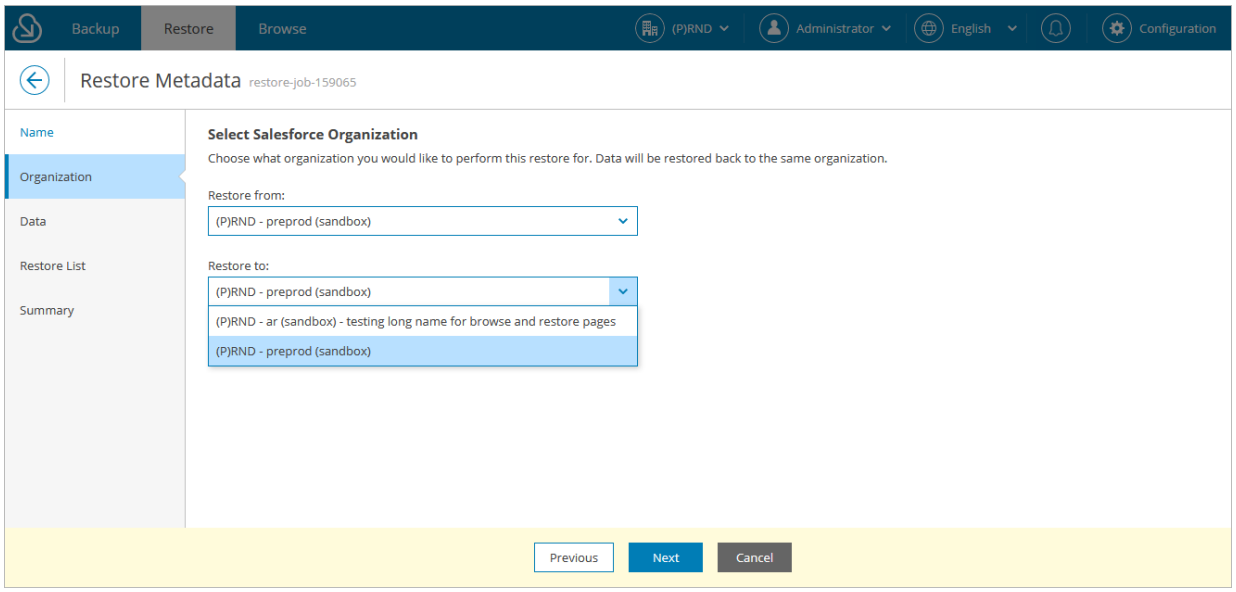


Step 3. Select Organization

At the **Organization** step of the wizard, select a Salesforce organization whose metadata you want to restore from the **Restore from** drop-down list. 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, select a Salesforce organization to which you want to restore metadata from 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.



Step 4. Select Metadata to Restore

At the **Data** step of the wizard, you can look through the backed-up data, as well as browse, filter, and choose data that you want to restore. Only metadata objects that have been backed up are displayed at this step.

Some metadata objects may have references to other objects. To restore all metadata objects successfully, you must analyze the relationships between the objects and restore the referenced objects first. This may require executing multiple jobs.

To choose metadata objects for restore:

1. From the **Metadata type** drop-down list, select the type of metadata.
2. Apply additional search conditions using specific filters. To do that, click **Customize**. In the **Metadata Filters** window, click **Add Condition**, select a field and a conditional operator from the drop-down lists, and enter the necessary value.

   Veeam Backup for Salesforce suggests a number of in-built conditional operators, such as *contains*, *equals*, *starts with*, *is null* and so on. These operators are used to make queries to databases. Note that the time required to process the request depends on the operator you are using, for example, processing a request with the *equals* operator will take less time than a request with the *contains* operator.

   By default, filters are linked by the AND logical operator. That is, a record is displayed in the search results when all specified conditions are met. You can change this behavior by linking filters with different operators. To do this, set the **Use filter logic** toggle to *On*, and specify the filter logic expression using condition ordinal number, brackets and logical operators, for example: 1 AND (2 OR 3) AND NOT 4.
3. Click **Search**. Veeam Backup for Salesforce will show the results satisfying your search parameters in the **Objects found** section.

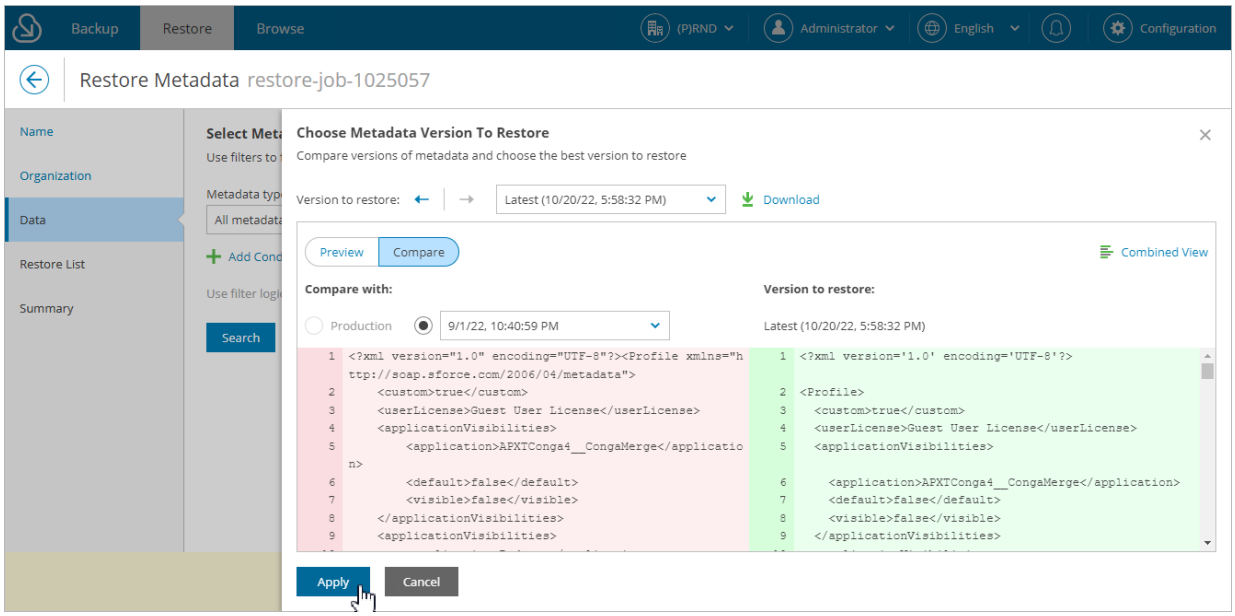
   By design, the search results will be displayed on the same pages where the records were originally shown. To make sure that you have seen all the results, look through all the pages.
4. Choose the files from the search results displayed in the **Objects found** section:
   a. Select check boxes next to the metadata files that you want to restore.
   b. To choose the version of a metadata file that will be restored, click the link in the **Version** column, and in the **Choose Metadata Version to Restore** window, compare the latest version of the backed-up metadata file with previous backed-up file versions and the version of the file currently stored in the Salesforce database, and select the necessary version.

> **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.

TIP

Consider the following:

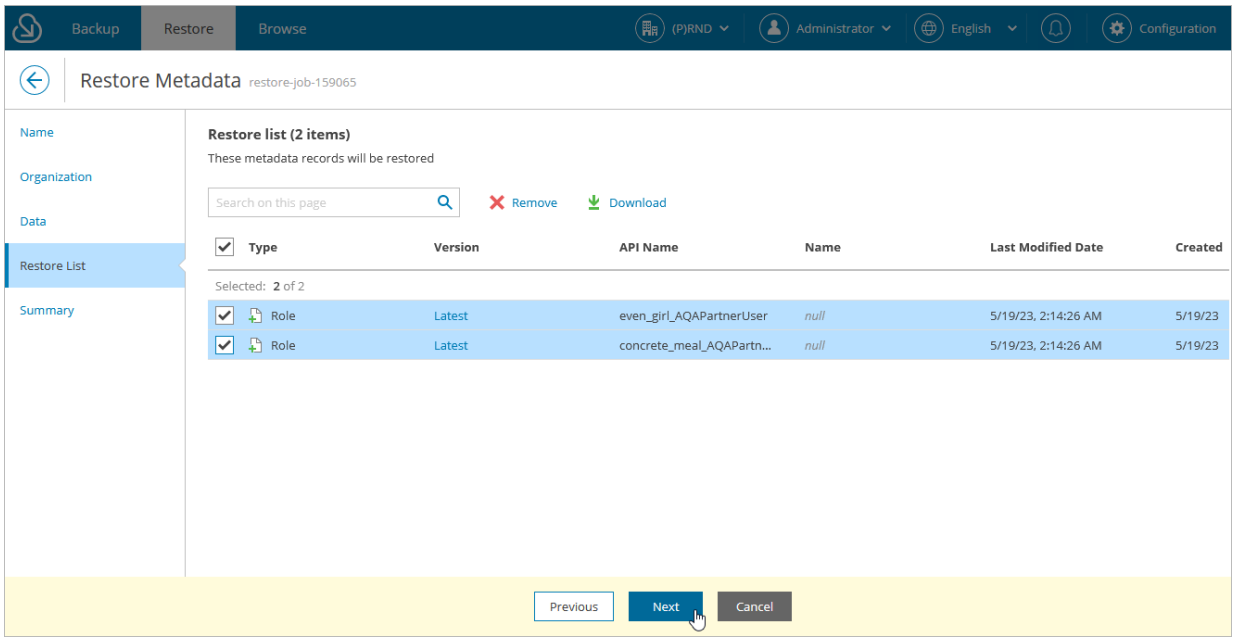
- By default, you can download up to 100 metadata files to the local machine. To do that, select the necessary objects, and click **Download**.
- For metadata of custom objects that was permanently deleted from Salesforce, you must restore metadata of the following types: *CustomObject*, *CustomTab*,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



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**.



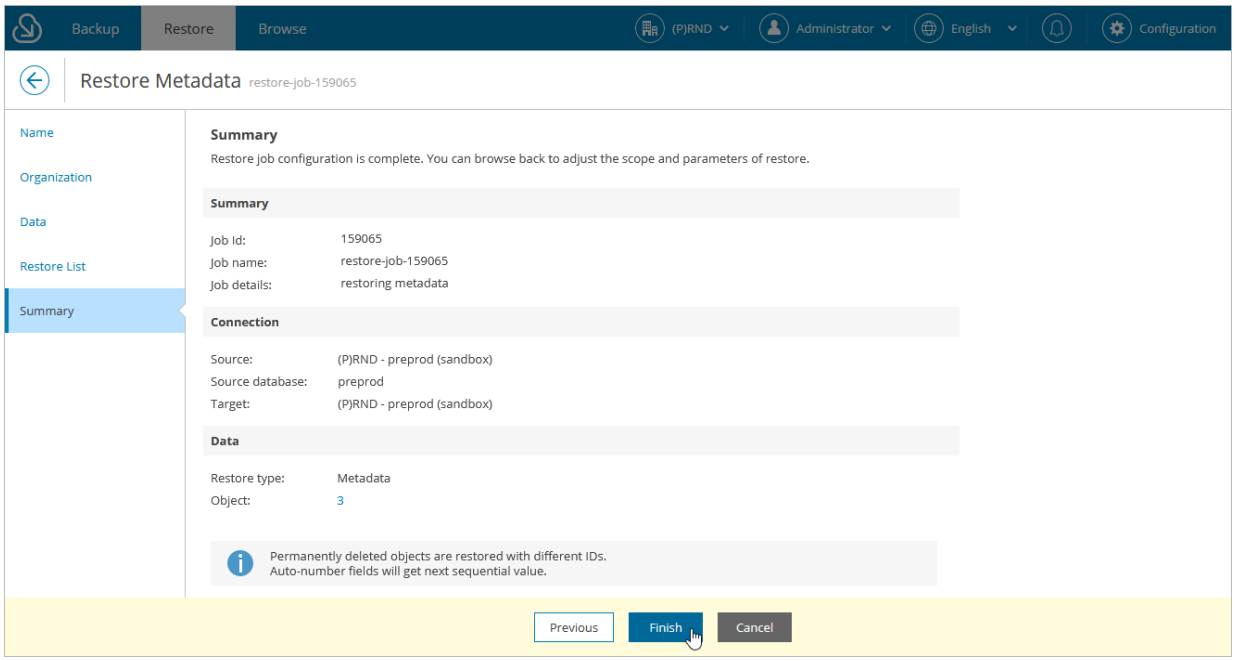
Step 6. Finish Working with Wizard

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.



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:

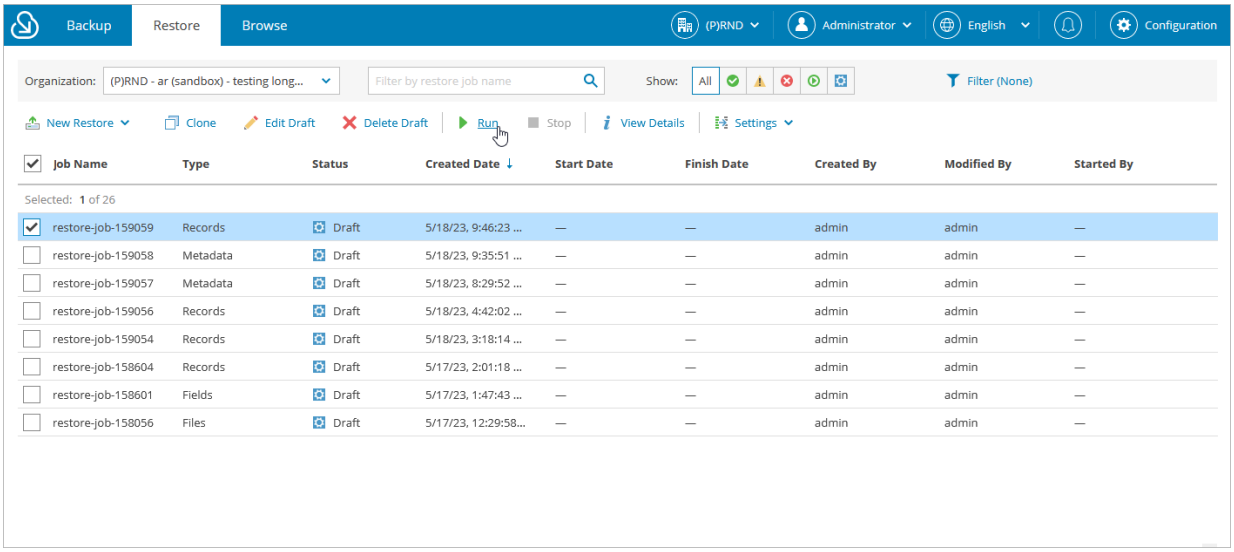
1. Navigate to the **Restore** tab.
2. From the **Organization** drop-down list, select a Salesforce organization for which the restore job has been created.
3. Select the necessary job.

> **NOTE**
>
> 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 set a filter, the settings apply to all companies and do 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 set.

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.



Cloning and Editing 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.

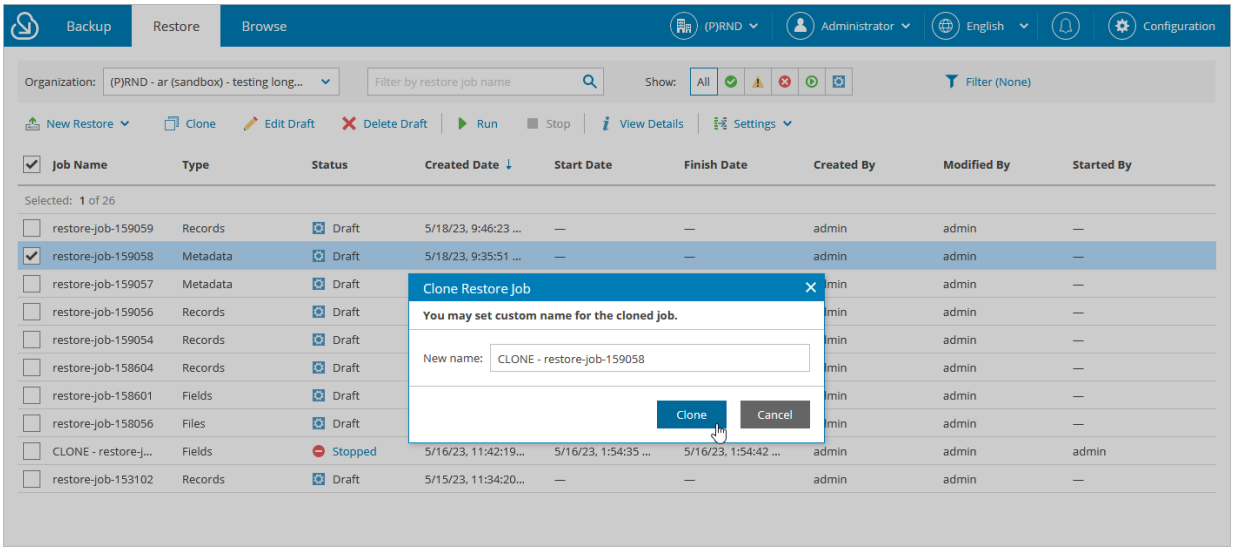
To clone a restore job:

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.

> **NOTE**
>
> 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 set a filter, the settings apply to all companies and do 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 set.

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.



Editing Restore Jobs

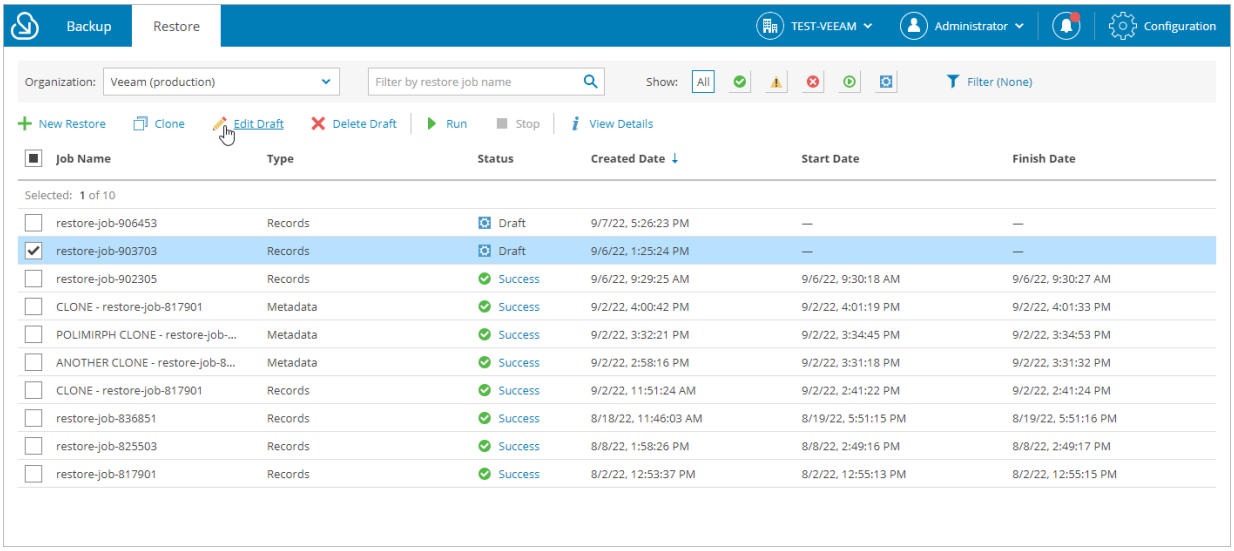
You can edit restore jobs created in Veeam Backup for Salesforce that were not launched yet and have the *Draft* status. For example, you may want to modify some settings specified in a restore job, change the chosen object and fields, and so on.

To edit restore job settings, do the following:

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.

> **NOTE**
>
> 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 set a filter, the settings apply to all companies and do 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 set.

4. Click **Edit Draft**. The restore job wizard will open.
5. Edit the job settings as described in sections Restoring Records, Restoring Field Values, Restoring Files or Restoring Metadata.



Removing Restore Job Drafts

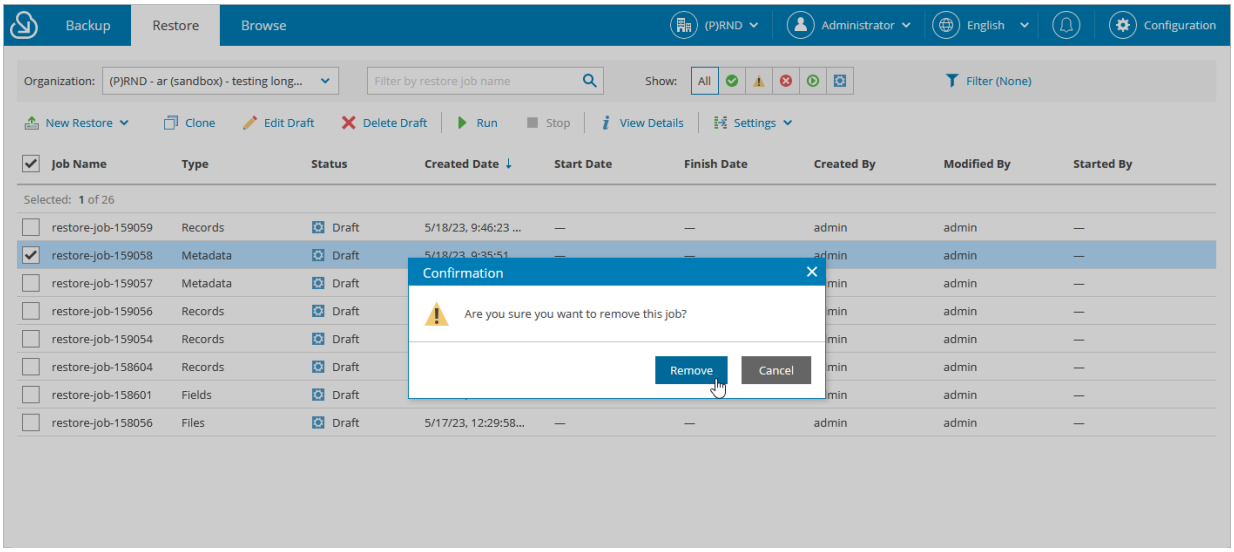
You can manually remove a draft of a restore job that is no longer needed. However, you cannot remove restore jobs that have been already launched.

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.

> **NOTE**
>
> 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 set a filter, the settings apply to all companies and do 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 set.

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



Configuring Restore Mapping Settings

You can configure restore mapping settings for a specific organization if it is protected by a backup policy. These settings will be applied to all restore jobs launched for this organization.

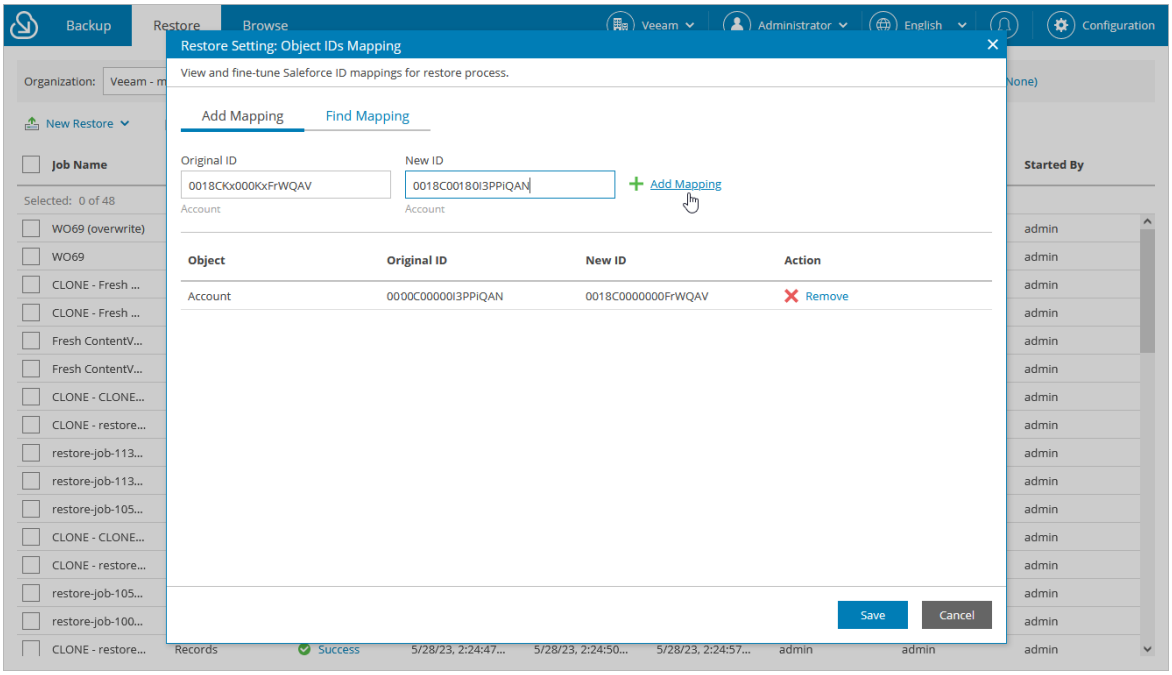
Object Mapping by Record IDs

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 saved in the backup file. To associate the newly created record with the backed-up record, the product creates in its organization database a default rule that maps the ID of the backed-up record with the ID of the record created in Salesforce. In addition to the default rule, you can create custom object mapping rules, for example, if you want to restore the deleted record data to an existing Salesforce record.

To create a custom rule, 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 create the rule.
3. Click **Settings** > **Object IDs Mapping**.
4. In the **Restore Setting: Object IDs Mapping** window, do the following:
    a. On the **Add Mapping** tab, specify the ID of the record saved in the backup file and the ID of the existing Salesforce record, and click **Add Mapping**.
    b. To save the configured mapping settings, click **Save**.

> **TIP**
>
> To find a mapping rule created for a record, switch to the **Find Mapping** tab, 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**.



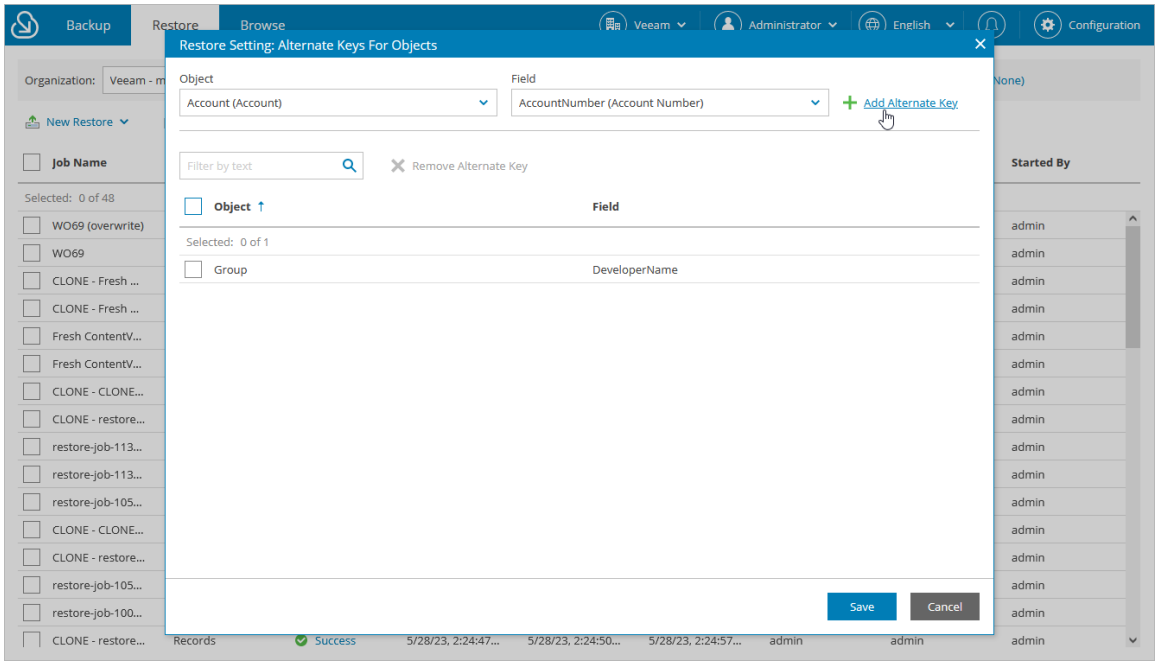
Mapping by Alternate Keys

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**.

> **NOTE**
>
> Consider the following:
>
> - 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

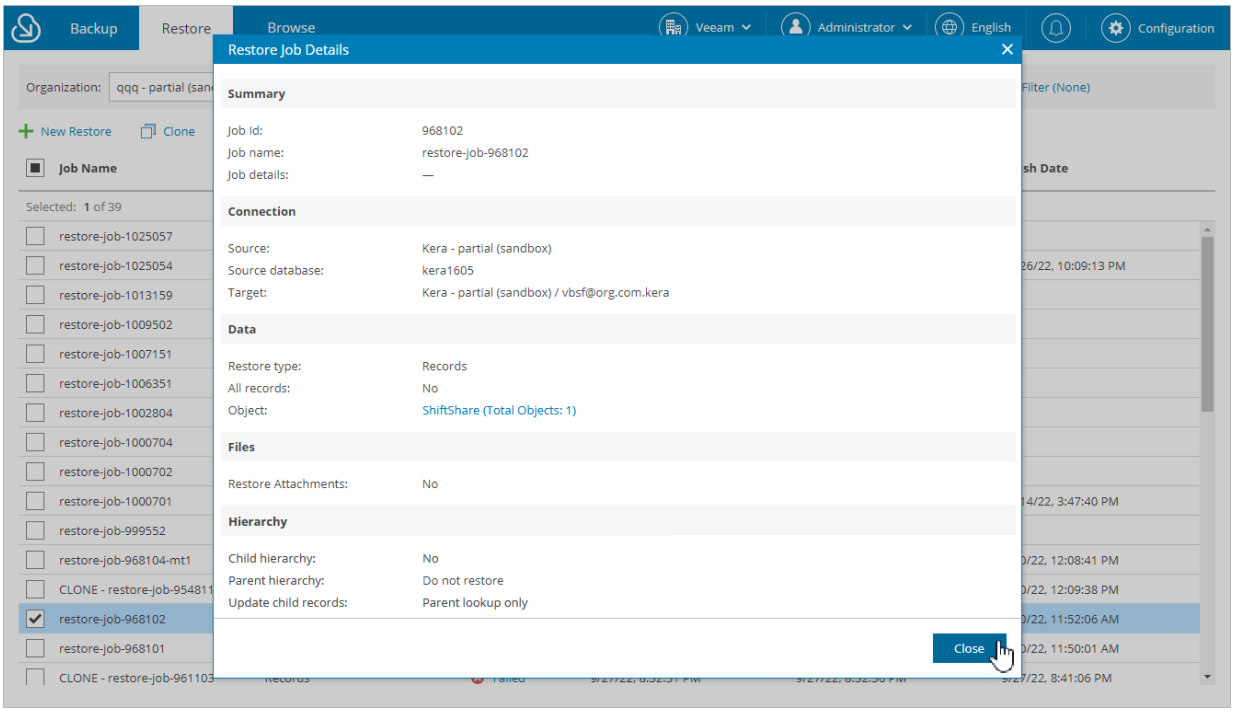
Veeam Backup for Salesforce displays all restore jobs and restore job drafts on the **Restore** tab. After you run a restore job, it cannot be edited or removed anymore. Users can only view the job details and restore session statistics. Users assigned any role can see information on restore jobs created for Salesforce organizations which data they have access to.

> **NOTE**
>
> 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 set a filter, the settings apply to all companies and do not change during the current user session. That is why if you do not see a restore job in the list, make sure that the **All** filter is set.

To view settings configured for a specific restore job:

1. Select the necessary restore job policy.
2. Click **View Details**.

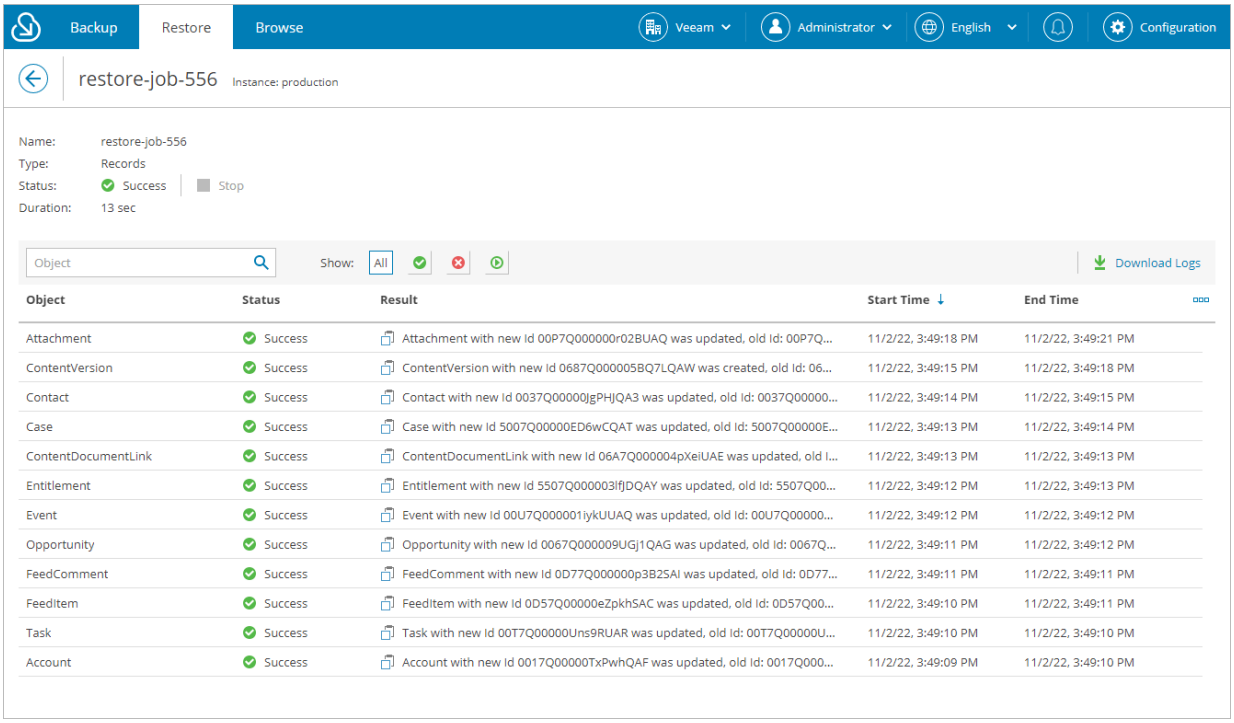
   The **Restore Job Details** window will open.



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 from 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.



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 following information:

   - **Build version** — the currently installed version of Veeam Backup for Salesforce.
   - **Management Console version** — the currently installed version of the Management Console service.
   - **Restore module version** — the currently installed version of the Veeam restore service.
   - **Backup module version** — the currently installed version of the Veeam backup service.
   - **Instance ID** — the unique identification number of the default protected Salesforce organization.

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 to Veeam Backup for Salesforce 2.0 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 2.0, consider the following:

- If the management server is running the CentOS 7, Oracle Linux 7 or RedHat Linux 7 operating system, you must reboot the server after the upgrade process completes. To do that, you can either select the **Reboot automatically after install if required** check box on the Veeam Updater page or run the `sudo systemctl restart veeam-updater` command from the server console.
- 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 2.0 supports API version 57.0, while Veeam Backup for Salesforce 1.0 supported API version 55.0. 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 2.0 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 2.0 will store backed-up data in the `/opt/vbsf/data` folder. However, if you upgrade from version 1.0 to 2.0, 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.

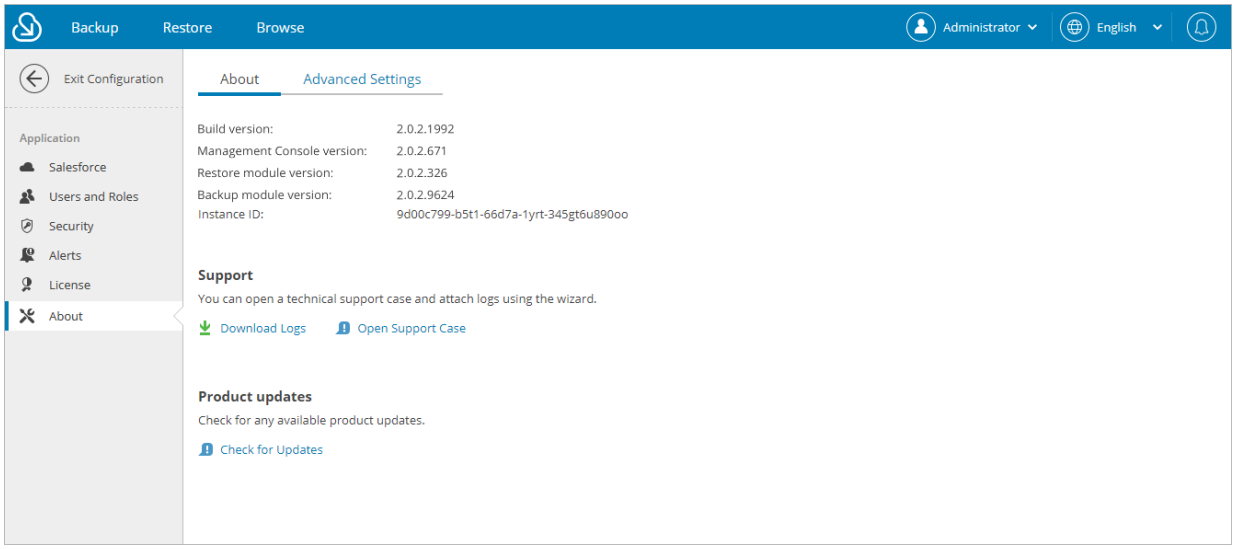
For more information on the issues that you may encounter while upgrading the product, see the Veeam Backup for Salesforce Release Notes.

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 **Product updates** 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 **Product updates** 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

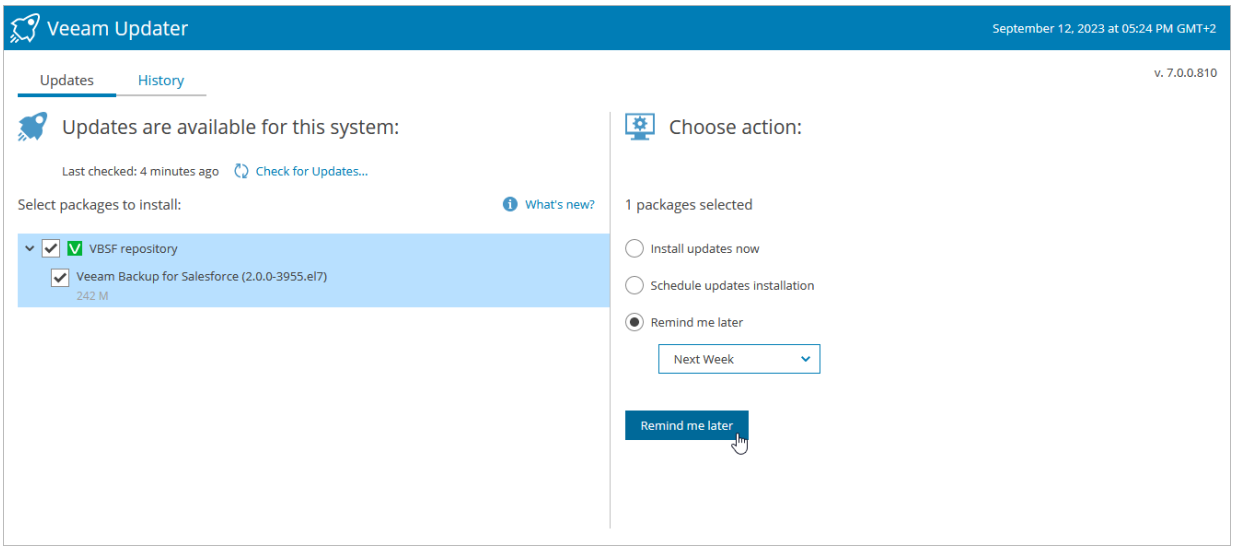
If you have not decided when to install updates, you can set an update reminder — instruct Veeam Backup for Salesforce to send an update notification later.

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**.



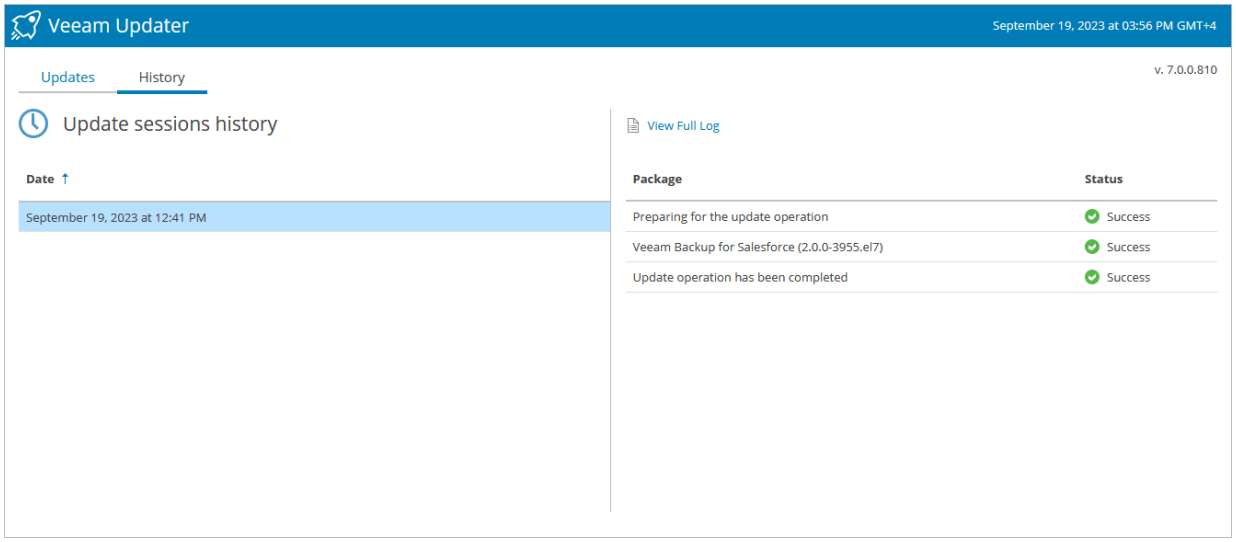
Viewing Updates History

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.



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:

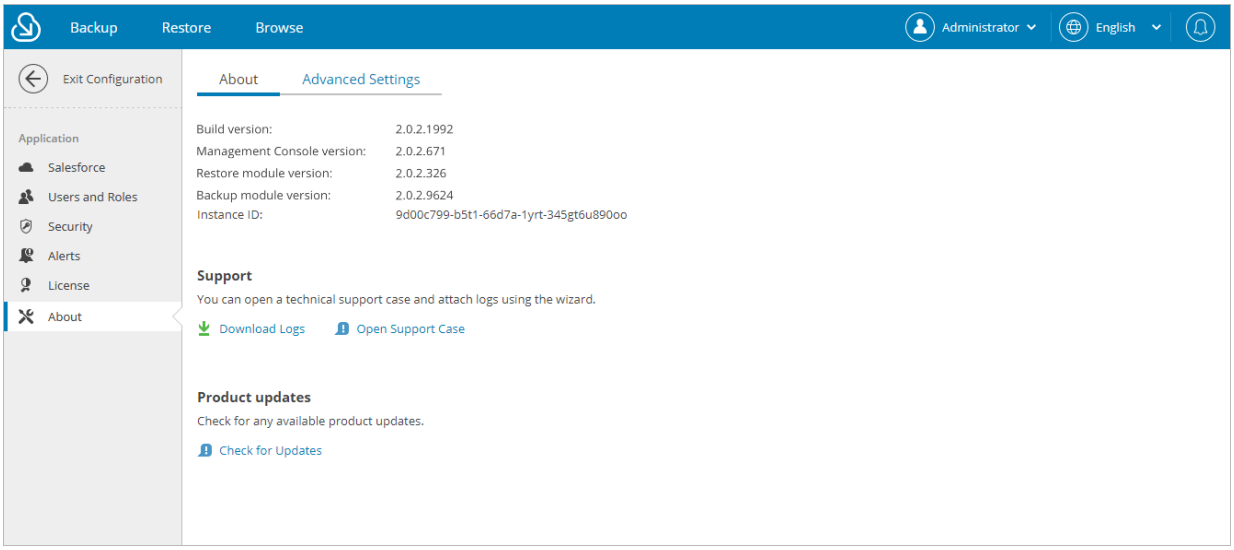
- Version information for the product and its infrastructure components
- The error message or an accurate description of the problem you are facing
- Log files

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.



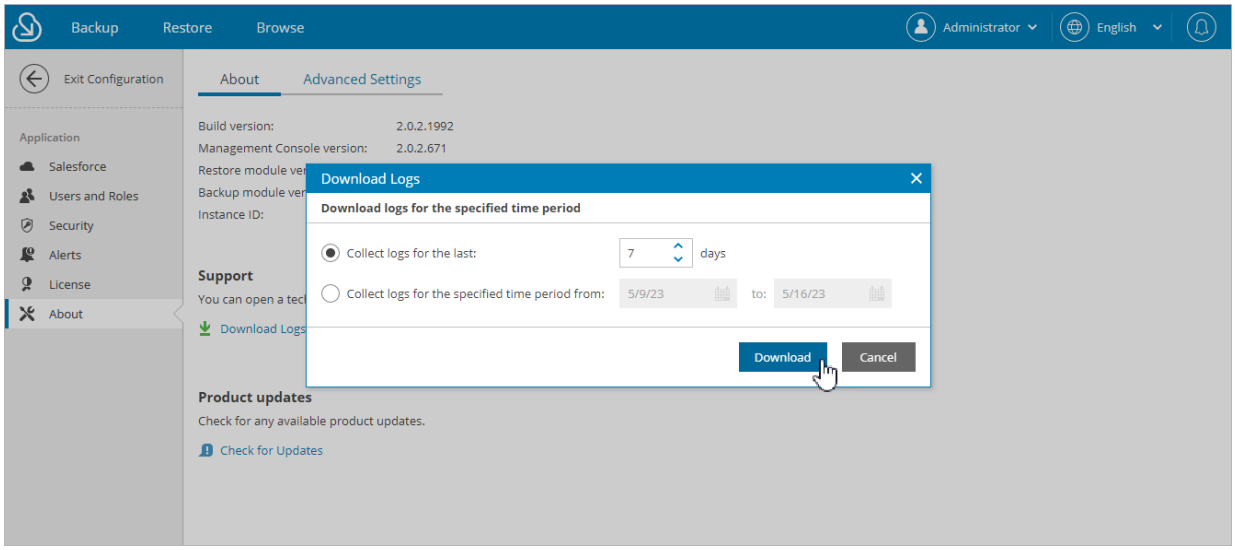
Downloading Product Logs

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 57 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.

Additionally, Veeam Backup for Salesforce does not support backup of the following Salesforce objects:

- *_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

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).