Veeam

Backup & Replication

13.0.1.2067

Integration Guide

ESKM

8.54.0

utimaco®

Imprint

Copyright 2026	Utimaco IS GmbH Krefelder Straße 220 52070 Aachen Germany
Phone	AMERICAS +1-844-UTIMACO (+1 844-884-6226) EMEA +49 800-627-3081 APAC +81 800-919-1301
Internet	https://support.hsm.utimaco.com/
e-mail	support@utimaco.com
Document Version	2.0.0
Date	2026-05-15
Status	PUBLISHED
Document No.	IG-2025-0033

All rights reserved	No part of this documentation may be reproduced in any form (printing, photocopy or according to any other process) without the written approval of Utimaco IS GmbH or be processed, reproduced or distributed using electronic systems. Utimaco IS GmbH reserves the right to modify or amend the documentation at any time without prior notice. Utimaco IS GmbH assumes no liability for typographical errors and damages incurred due to them. All trademarks and registered trademarks are the property of their respective owners.

Table of Contents

1 Introduction

This integration guide is part of the information and support provided by Utimaco. It outlines the process for integrating ESKM with Veeam Backup & Replication to enable secure and encrypted backup functionality. Together, Veeam Backup & Replication and ESKM deliver a comprehensive solution for secure, compliant, and resilient data protection. The guide contains the necessary steps to configure the integration.

1.1 About This Guide

This guide describes how to enable ESKM integration with Veeam Backup & Replication to enable backup encryption. It equips users with the key data to facilitate effortless communication and authentication between ESKM and Veeam Backup & Replication, implementing Key Management Interoperability Protocol (KMIP) and certificate-based authentication.

1.2 Target Audience

This guide is intended for Veeam Backup & Replication and ESKM administrators.

1.3 Purpose of the Integration

The integration of Veeam Backup & Replication with ESKM enhances the security and compliance of your data protection strategy. While Veeam ensures reliable backup and recovery across virtual, physical, Network-Attached Storage (NAS), and cloud-native environments, ESKM provides robust encryption key lifecycle management including generation, storage, access control, and auditing.

The primary objectives of this integration are to:

- Enhance data security by ensuring all backups are encrypted during storage and transmission.
- Leverage Veeam's encryption capabilities within the ESKM environment.

1.4 Abbreviations

Abbreviation	Meaning
ESKM	Enterprise Secure Key Manager
KMIP	Key Management Interoperability Protocol
CDP	Continuous Data Protection
API	Application Programming Interface
CA	Certificate Authority
P12	PKCS#12 or PFX (Personal Information Exchange)
KMS	Key Management System
UI	User Interface
URL	Uniform Resource Locator
VM	Virtual Machine
RSA	Rivest, Shamir, Adleman
GUI	Graphical User Interface
NAS	Network-Attached Storage

Table 1: List of Abbreviations

1.5 Document Conventions

The following conventions are used in this guide:

Convention	Use	Example
Bold	Items of the Graphical User Interface (GUI), e.g., menu options	Select **Details** and click on **Properties** button
`Monospaced`	Code that is given for explanation or as an example, file paths	`certreq.exe -new request.inf IISCertRequest.csr`
Italic	References and important terms	Operating system listed in *Tested Versions*

Table 2: Document Conventions

We use special icons to highlight the most important notes and information.

Here you will find important safety information that should be followed.

Here you will find additional notes or supplementary information.

This message marks the result expected after the successful execution of an instruction.

2 Product Overview

2.1 Veeam Backup & Replication

Veeam Backup & Replication is a proven data protection solution that offers efficient and reliable backup and recovery for virtual, physical, NAS, and cloud-native environments. It provides comprehensive security for critical business data. With Veeam Backup & Replication, you can create image-level backups of virtual, physical, and cloud machines and restore from them. Technology used in the product optimizes data transfer and resource consumption, which helps to minimize storage costs and the recovery time in case of a disaster.

2.2 ESKM (Enterprise Secure Key Manager)

The ESKM is a complete solution for generating, storing, serving, controlling, and auditing access to encryption keys. It enables you to protect and preserve access to business-critical, sensitive, data-at-rest encryption keys, either locally or remotely. ESKM is offering industry-certified KMIP with market-leading support for partner applications and pre-qualified solutions, integrating out-of-the-box with varied deployments, as well as custom integrations.

2.3 Joint Value Proposition

The integration of Veeam Backup & Replication with ESKM delivers a comprehensive and secure data protection solution that combines industry-leading backup and recovery capabilities with advanced encryption key management. This joint solution empowers organizations to:

- Ensure end-to-end data security by encrypting backups both at rest and in transit.
- Simplify compliance with regulatory standards through centralized key lifecycle management, including generation, storage, access control, and auditing.
- Maximize operational efficiency by seamlessly leveraging Veeam's encryption features within the ESKM environment.
- Strengthen resilience against data breaches and unauthorized access.

3 Integration Requirements and Prerequisites

Ensure that the system environment you will be using meets the following hardware and software requirements.

This guide assumes that the user has already installed and configured required software.

3.1 Tested Versions

The integration has been successfully tested with the ESKM with Veeam Backup & Replication.

Operating System	Veeam Backup & Replication Version	ESKM Version
Windows Server 2025 Datacenter Edition	13.0.1.2067	8.54.0
Rocky Linux release 9.4 (Blue Onyx)	13.0.1.2067	8.54.0

Table 3: List of Tested Versions

3.2 Supported Platforms

- ESKM hardware appliance
- ESKM virtual/cloud appliance

3.3 Software Requirements

Software	Software Requirements
ESKM	8.54.0
Veeam Backup & Replication	13.0.1.2067

Table 4: List of Software Requirements

3.4 Prerequisites

Before you begin, please ensure that you have installed/set up:

- **Veeam Backup & Replication**: Ensure that the latest version is installed and properly configured.
- **Licensing**: A valid Veeam license that supports API access and integration features.
- **ESKM:** Ensure that the latest version of ESKM is available.
- The operating system listed in *Tested Versions*.
- A valid SSL server certificate that meets the following requirements:
    - The Subject extension must be equal to the fully qualified domain name (FQDN) of the KMS server. For example: kms.domain.local.
    - The server certificate must have valid CRL distribution points specified in the CRL Distribution Points extension.

4 Installation and Configuration

The following section outlines the procedures required to configure both ESKM and Veeam Backup & Replication components for seamless integration.

4.1 Setting Up ESKM

The initial phase involves configuring ESKM before proceeding to Veeam Backup & Replication. For detailed configuration steps, refer to the installation guide *"ESKM_Installation and Replacement_Guide_8.54.0"*.

After successful installation and configuration, log in to ESKM.

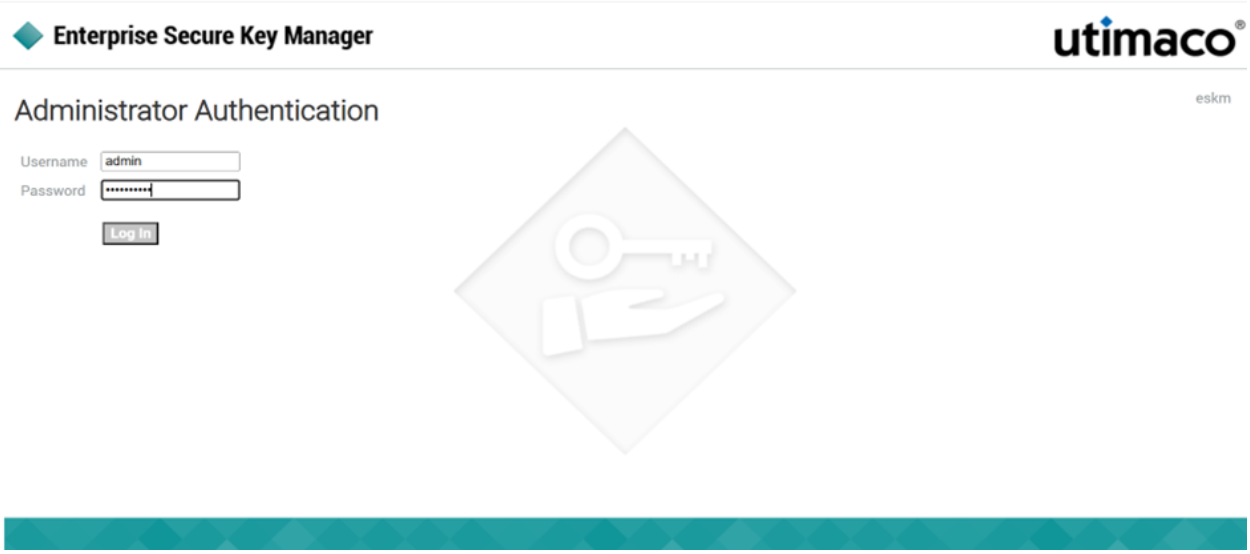

Figure 1 : ESKM Login

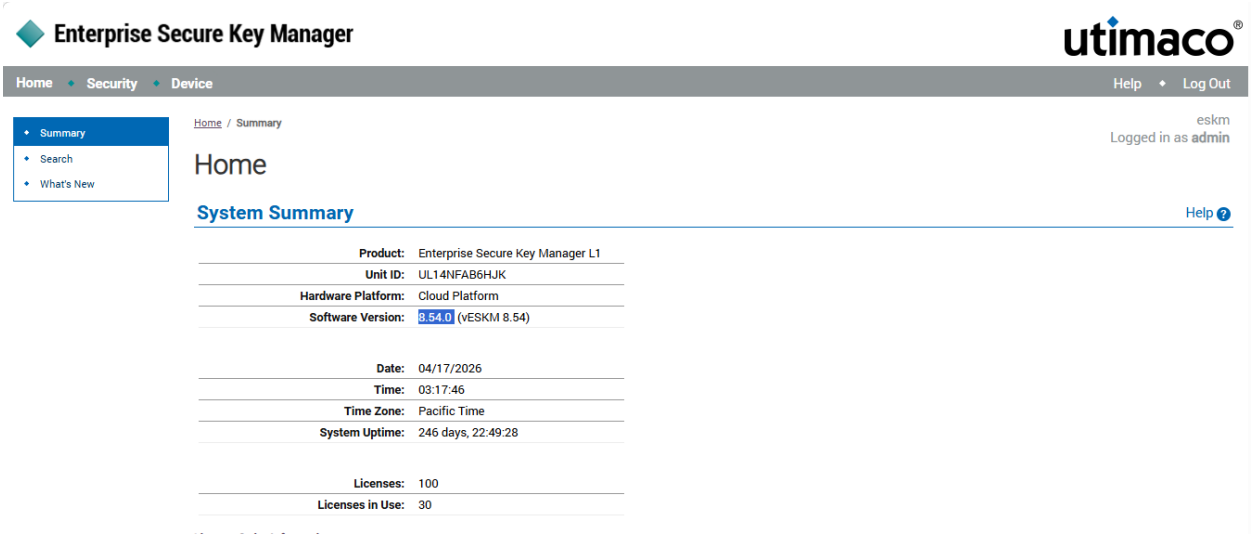

Figure 2 : ESKM Home Page

4.2 Setting up Veeam Backup & Replication

4.2.1 Setting up Veeam Backup & Replication on Windows

Download the Veeam Backup & Replication image from the official Veeam Product Download Page. For detailed installation instructions to ensure a smooth deployment, please refer to the installation guide *Veeam Backup & Replication Installation Guide*.

After the successful installation, launch the application and log in.

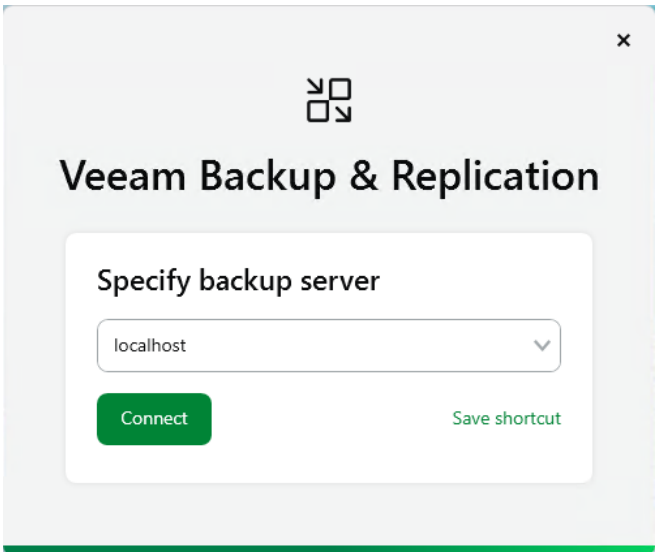

Figure 3 : Veeam Backup & Replication - Specify Backup Server

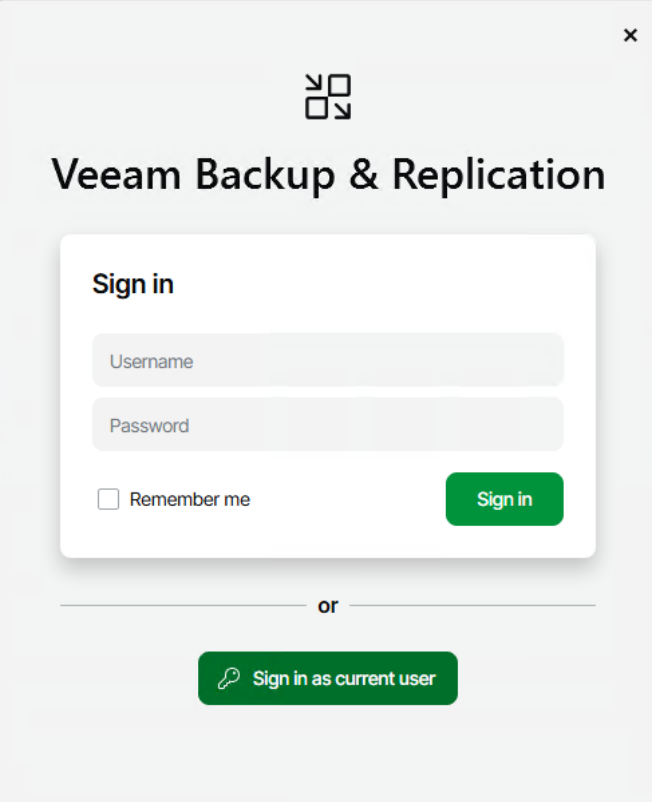

Figure 4 : Veeam Backup & Replication - Sign-in Page

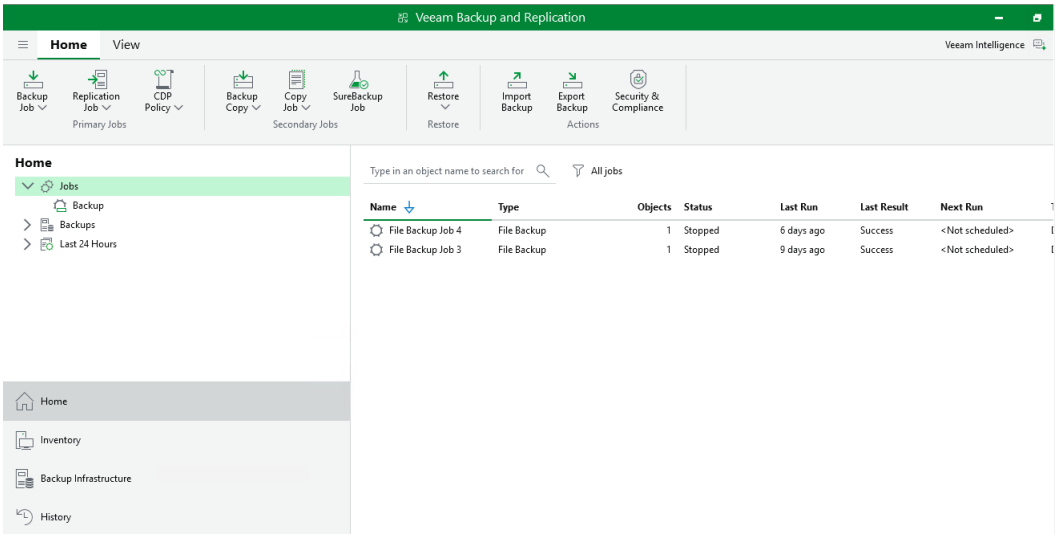

Figure 5 : Veeam Backup & Replication Main Page

4.2.2 Deploying Veeam Backup & Replication on Linux (Using ISO)

For Linux-based deployments, Veeam Backup & Replication is installed using the provided ISO image (for example, the Rocky Linux-based appliance ISO). The ISO is mounted to the target virtual machine, and the installation is performed following the official Veeam installation procedure.
Please follow the installation and deployment guide *Installing Veeam Infrastructure Appliance with ISO - Veeam Backup & Replication User Guide.*

While the Linux Web UI supports standard management and backup operations, certain advanced configurations, such as KMIP/KMS integration, are not currently available through the Web UI. For these configurations, and for all subsequent setup steps, use the Windows-based Veeam Backup & Replication console following the standard Windows workflow.

The Windows console can be connected to the Linux backup server by specifying the Linux backup server IP address in the **Specify backup server** screen.

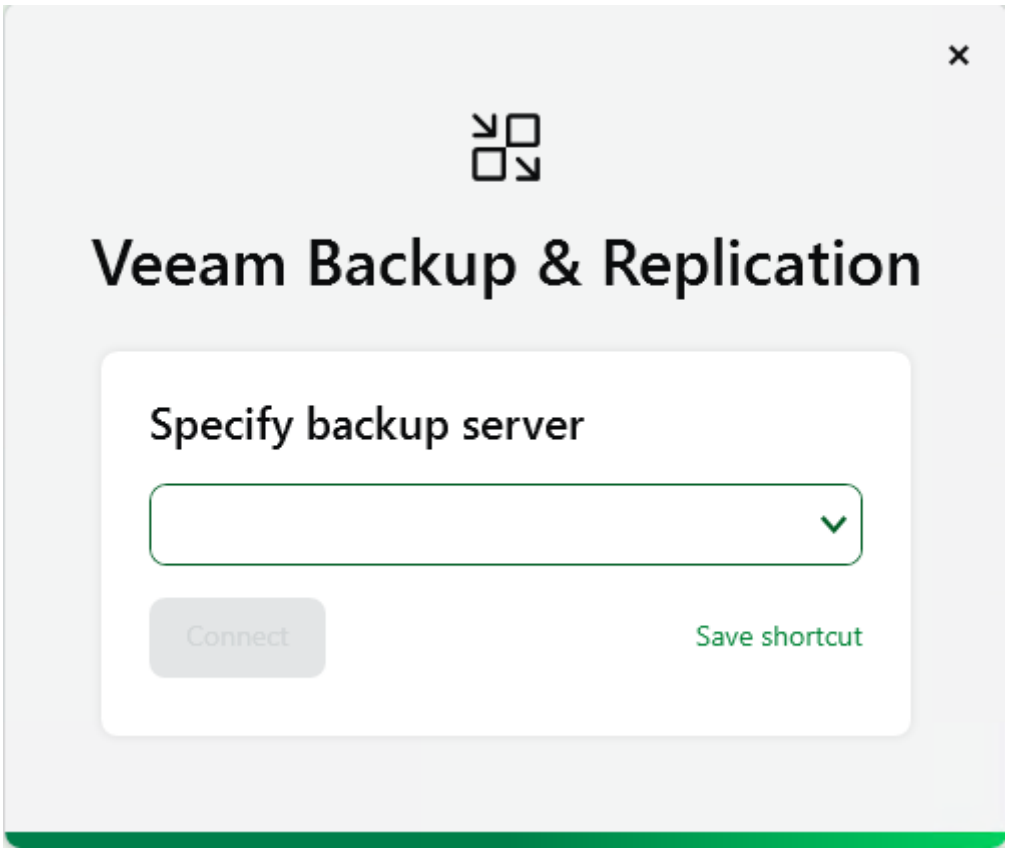

Figure 6 : Veeam Backup & Replication - Specify Backup Server

After connecting to the Linux server, log in using the administrative credentials configured during installation.

5 Integration Steps

To support a robust and secure backup infrastructure, integrating a KMS is a critical step. In environments where data protection and encryption are paramount, configuring a KMS ensures that encryption keys are managed securely and in compliance with organizational policies. As part of the setup process for Veeam Backup & Replication, it is essential to register ESKM as a KMS. This registration enables secure key handling and seamless encryption workflows, ensuring that sensitive data remains protected throughout the backup and recovery lifecycle.

5.1 Configuration on ESKM

It is essential to configure ESKM to ensure secure and efficient key management. This section guides you through the necessary steps to configure ESKM for Veeam Backup & Replication integration.

5.1.1 Local CA Creation

Inside ESKM, create a local CA by following the steps below:

1. Go to the **Security** tab.
2. Click on the **Certificates** option listed under **Certificates & CAs**.
3. Scroll down to the **Local CAs** section.
4. Enter a **Certificate Authority Name** and **Common Name**. These may have the same value (e.g., ESKM Local CA).
5. Enter your organization's details.
6. Select the **Algorithm** (e.g., RSA-2048).
7. Click on **Self-signed Root CA** and enter the **CA Certification Duration** and **Maximum User Certificate Duration**. These values determine when the certificate must be renewed and should be set in accordance with your company's security policies. The default value for both is 3650 days or 10 years.
8. Click on **Create**.

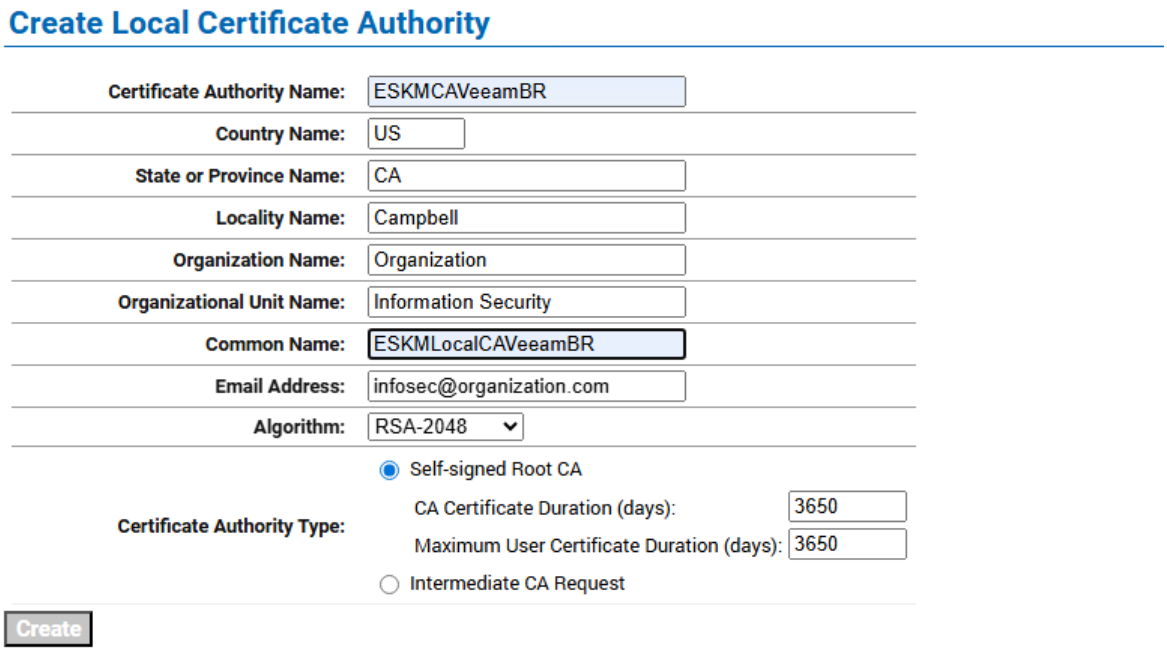

Figure 7 : Local CA Creation Page

9. Click on the **Local CAs** option listed under **Certificates & CAs** to view the created local CA certificate.

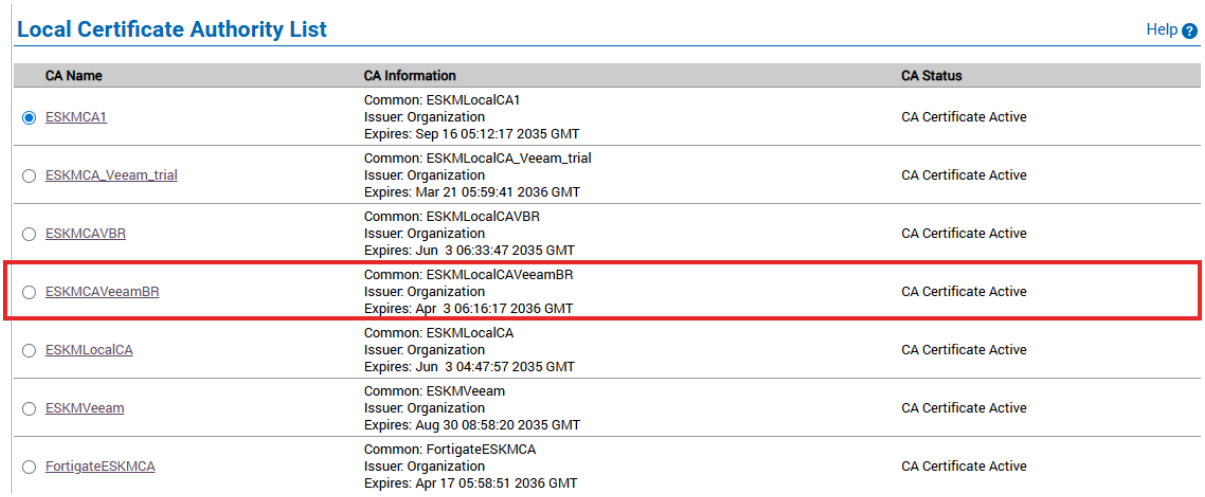

Figure 8 : Created Local CA Certificate

5.1.2 Import Server Certificate

This certificate serves as the server certificate for accessing the ESKM. The certificate must be a valid SSL server certificate meeting the requirements mentioned in the prerequisites.

Perform the following steps:

1. Go to ESKM **Management Console**.
2. Go to the **Security** tab and in the **Certificates & CA**, click **Certificates**.
3. In the **Import Certificate** section, select **Upload from browser** and **Choose File**.
4. Enter the **Certificate Name** and **Private Key Password**.

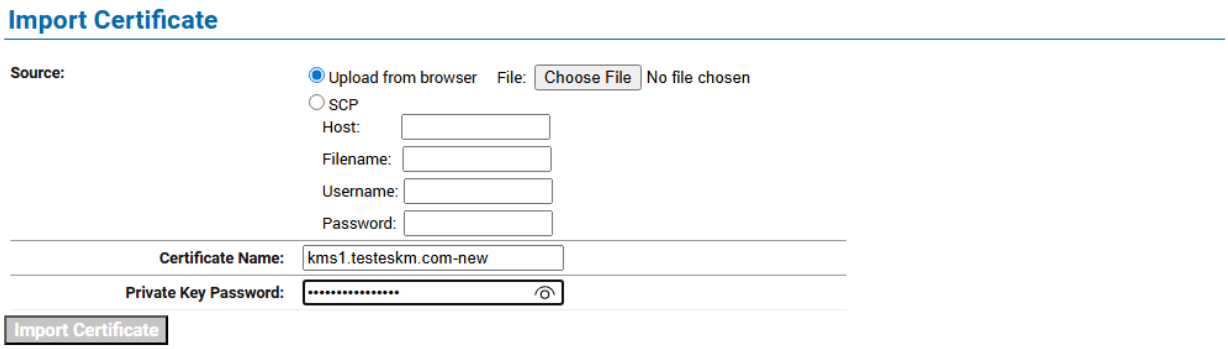

Figure 9 : Import Certificate

5. Click **Import Certificate.**

Figure 10 : Certificate Imported

5.1.3 Client Certificate Creation

This certificate functions as the client certificate used to authenticate and securely connect to the ESKM system. It is essential for establishing mutual TLS communication, where both the client and server verify each other's identities. The client certificate must be uploaded and

registered in Veeam Backup & Replication to enable secure access and enforce identity-based access control.

The following steps outline the process for generating the client certificate:

1. Go to the **Security** tab.
2. Click on the **Certificates** option listed under **Certificates & CAs**.
3. Scroll down to the **Create Certificate** section.
4. Enter a **Certificate Name** and **Common Name** (e.g., KMIPClientVeeamBR).
5. Enter your organization's details.
6. Enter a **Subject Alternative Name**.
7. Select the **Algorithm** (e.g., RSA-2048).
8. Choose the **Creation Type** as **Certificate Signed by Local CA**. Select the CA name you created in Local CA Creation (e.g., ESKMCAVeeamBR).
9. Select the **Certificate Purpose** as **Client**.
10. Click **Create**.

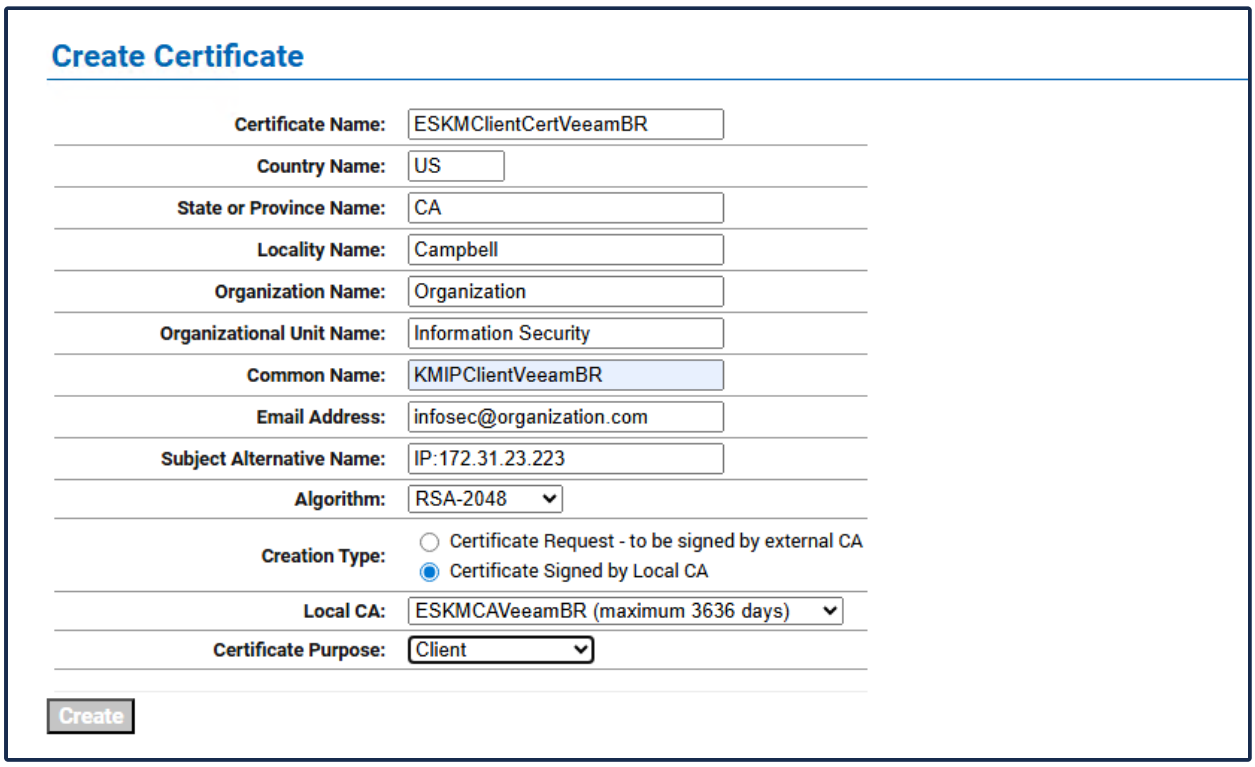

Figure 11 : Client Certificate Creation

11. Open the created client certificate and export it by providing a password.

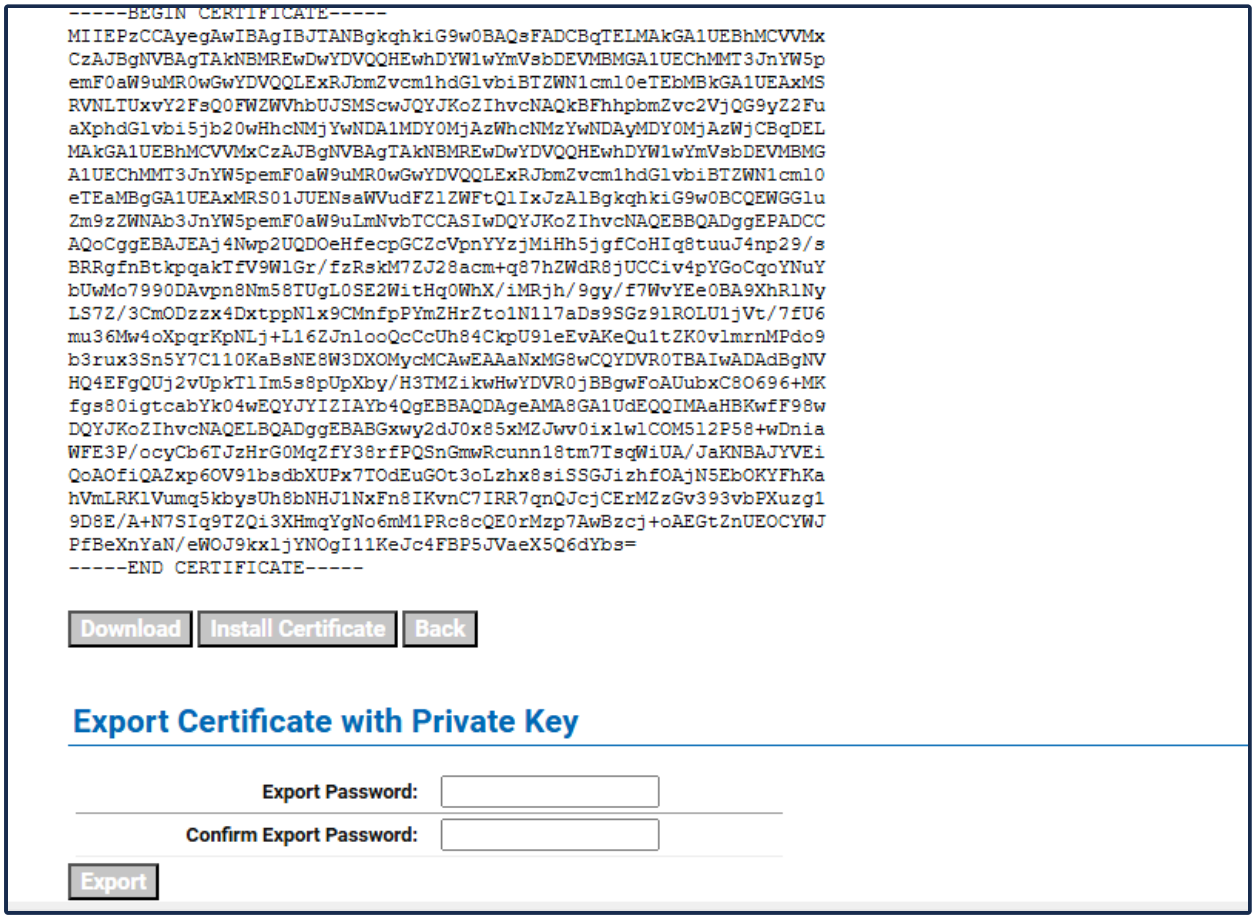

Figure 12 : Exporting Client Certificate

12. The certificate will be downloaded in p12 format.

13. Click the **Download** button to save the certificate content for local user creation.

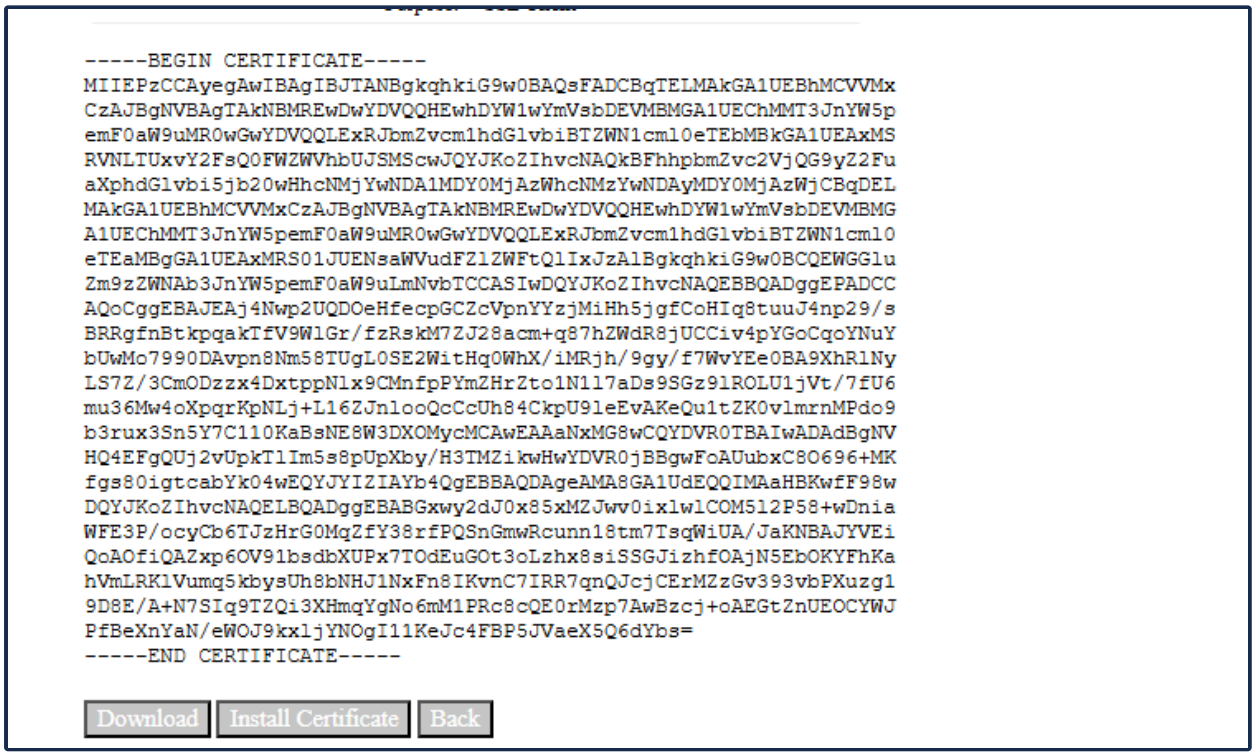

Figure 13 : Downloading Client Certificate

5.1.4 Local User Creation

Perform the following steps to create a local user in the ESKM:

1. Go to the **Security** tab.
2. Select **Local Users** from **Users & Groups > Local Users & Groups**.
3. Scroll down and click **Add**.
4. Enter the **Username**, which is the same as the **Common Name** provided during client certificate creation (e.g., KMIPClientVeeamBR).
5. Select **Enable KMIP**.
6. Select the **License Type** as **KMIP**.
7. Paste the downloaded client certificate in **KMIP Client Certificate Contents**.
8. Click **Create**.

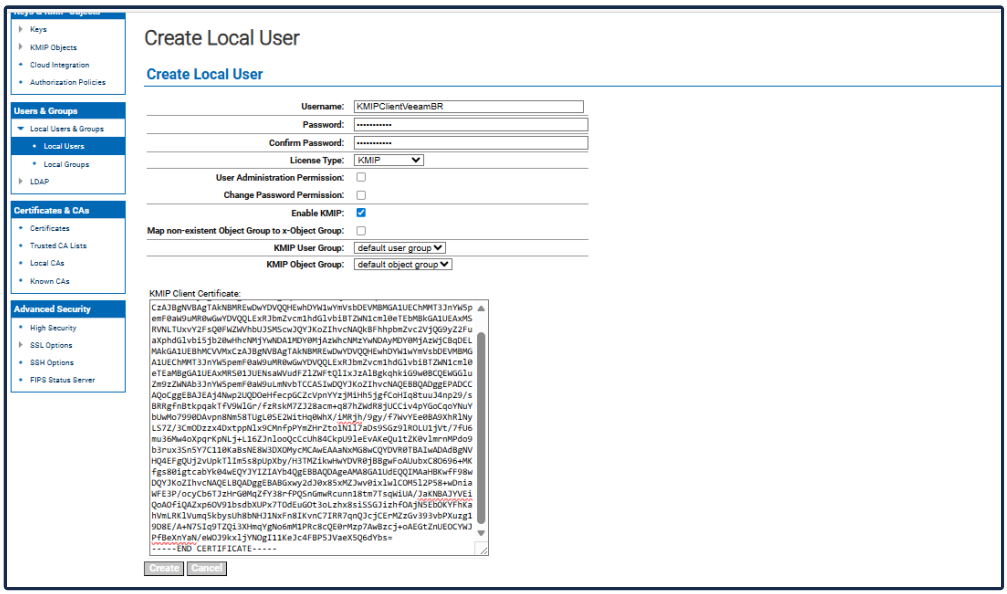

Figure 14 : Local User Creation

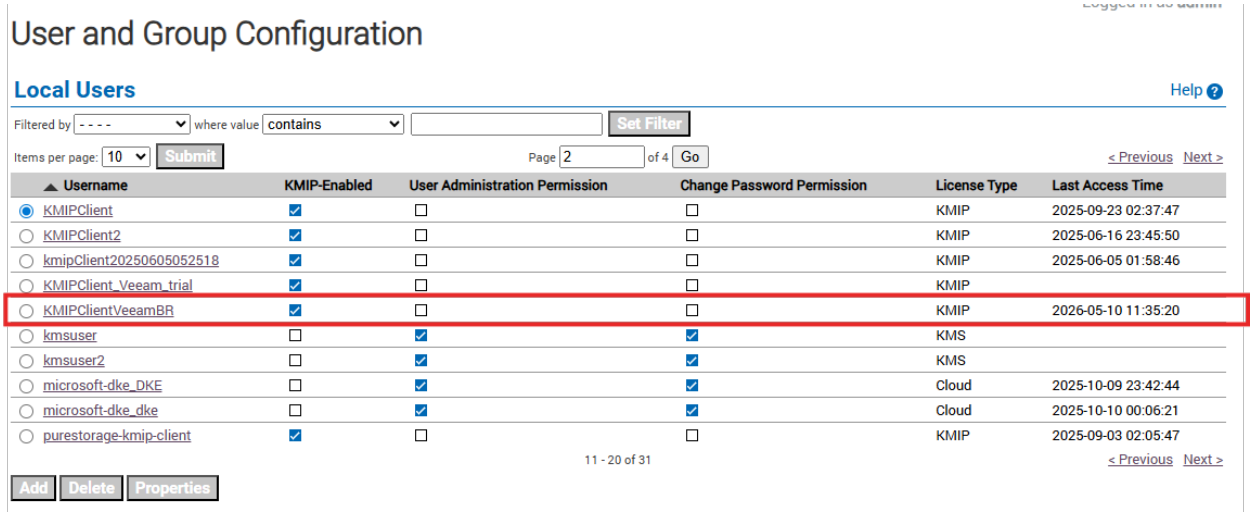

Figure 15 : Created Local User

5.1.5 KMIP Server Configuration

Configure the KMIP server.

1. Go to the **Device** tab.
2. From the left side panel, click on the **KMIP Server** option listed under **Device Configuration**.

3. Click the **Edit** button on the main page.
4. Choose the imported server certificate as the server certificate for KMIP server.
5. Click the **Save** button.

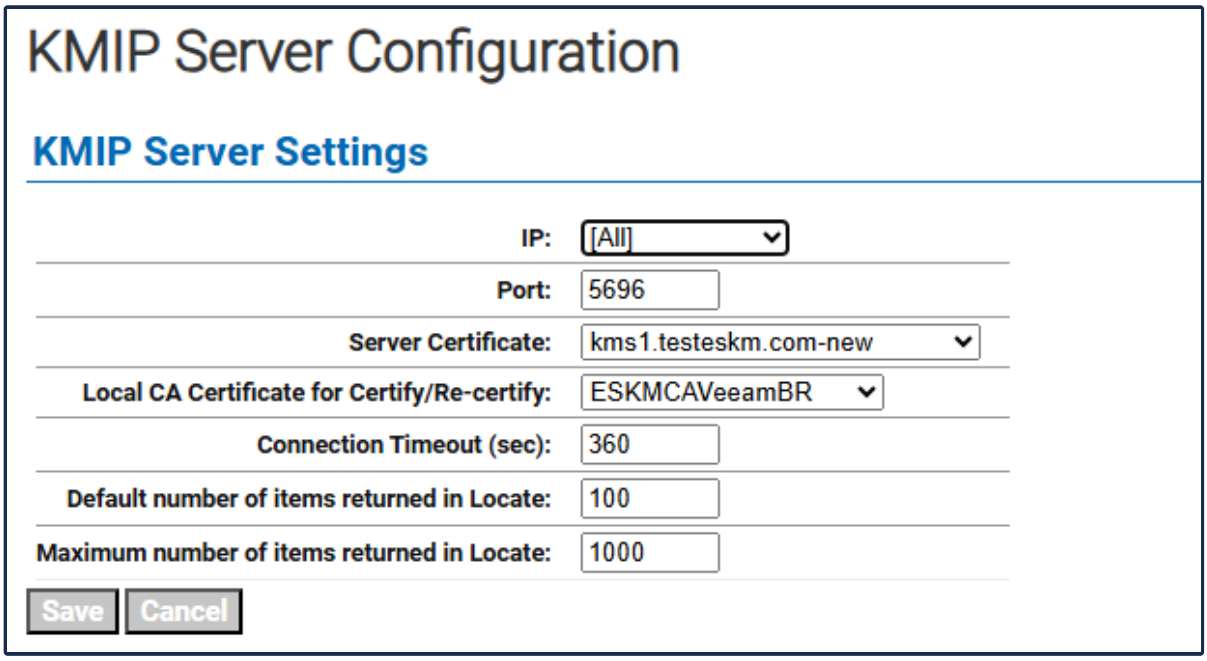

Figure 16 : KMIP Server Configuration

5.2 Configuration on Veeam Backup & Replication

Properly configuring Veeam Backup & Replication is essential to ensuring seamless integration with ESKM. This section walks you through the necessary steps to prepare Veeam Backup & Replication. Follow the instructions below to complete the setup efficiently and securely.

5.2.1 Register ESKM as a Key Management Service

To enable this integration, follow the steps outlined below within the Veeam UI.

1. Log in to the Veeam Backup & Replication interface.

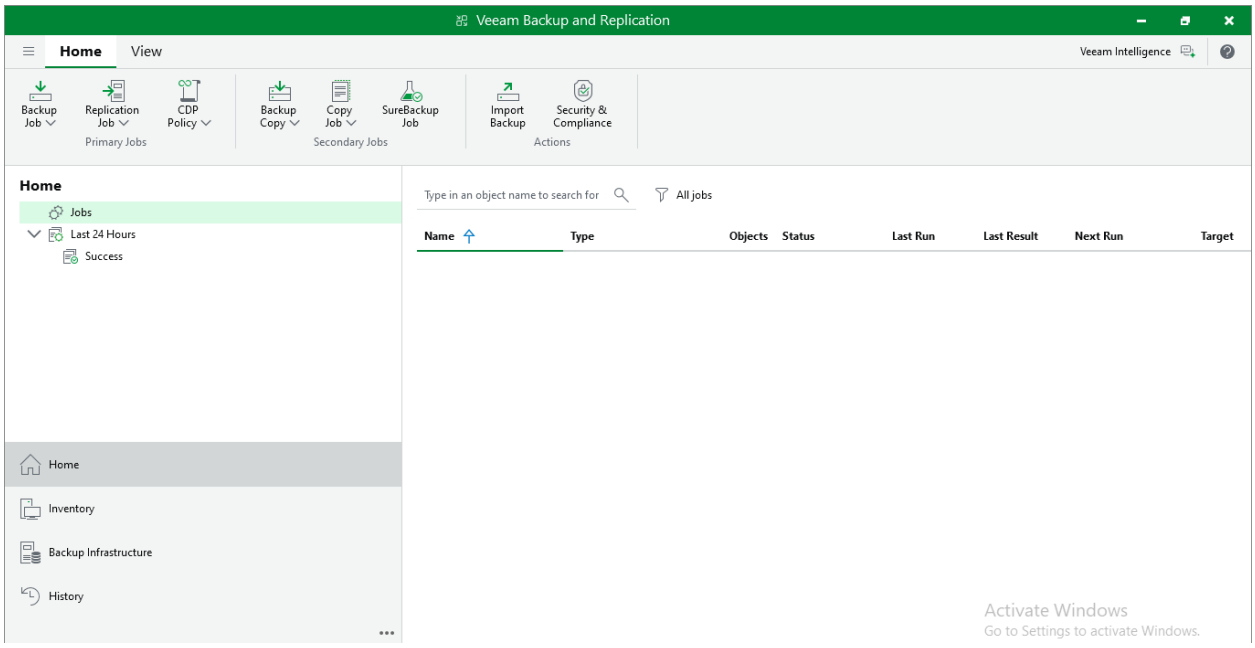

Figure 17 : Veeam Backup & Replication Home Page

2. Navigate to **Credentials & Password** and select the **Key Management Servers**.

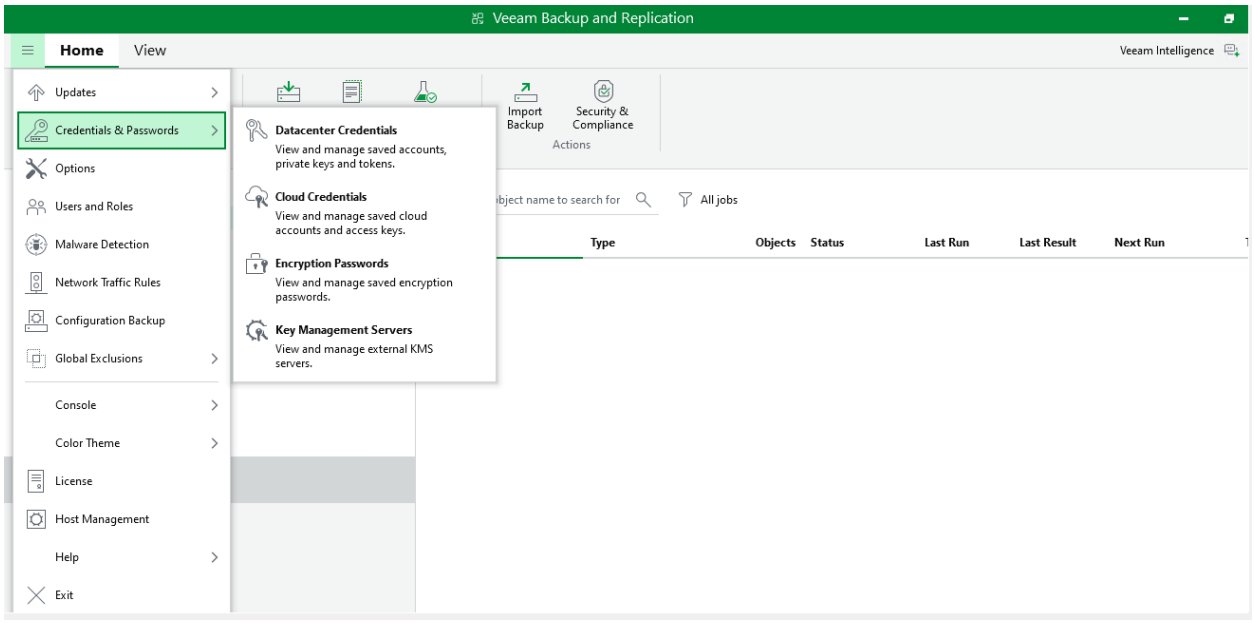

Figure 18 : Credentials and Passwords Page

3. Click **Add** and fill out the server URL, server certificate, and client certificate.

Ensure that the default port number 5696 is correctly set.

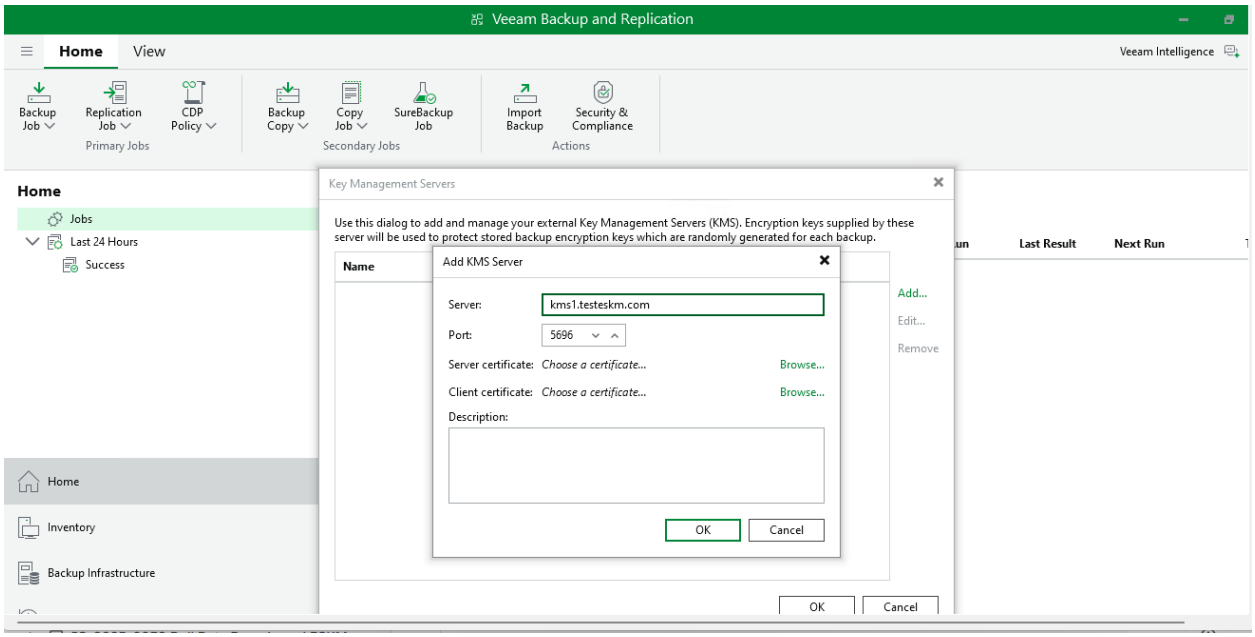

Figure 19 : Server Name Added

4. Upload the server and client certificates generated in sections *Import Server Certificate* and *Client Certificate Creation*.

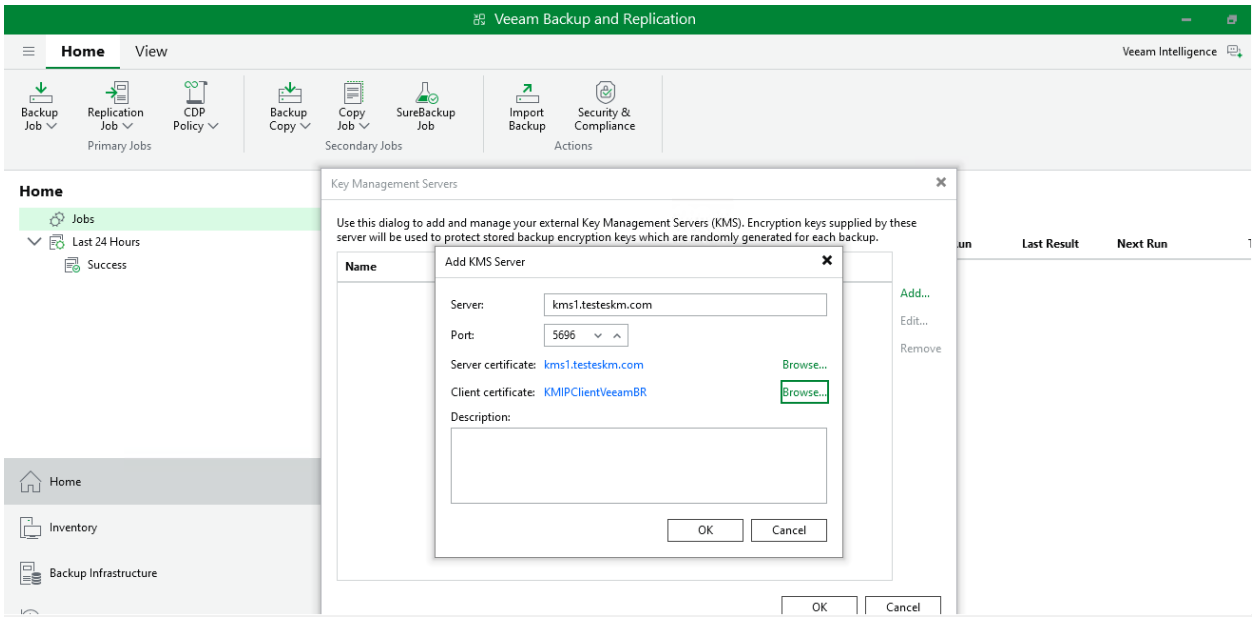

Figure 20 : Server and Client Certificates Added

5. After providing the required information, click **OK**.

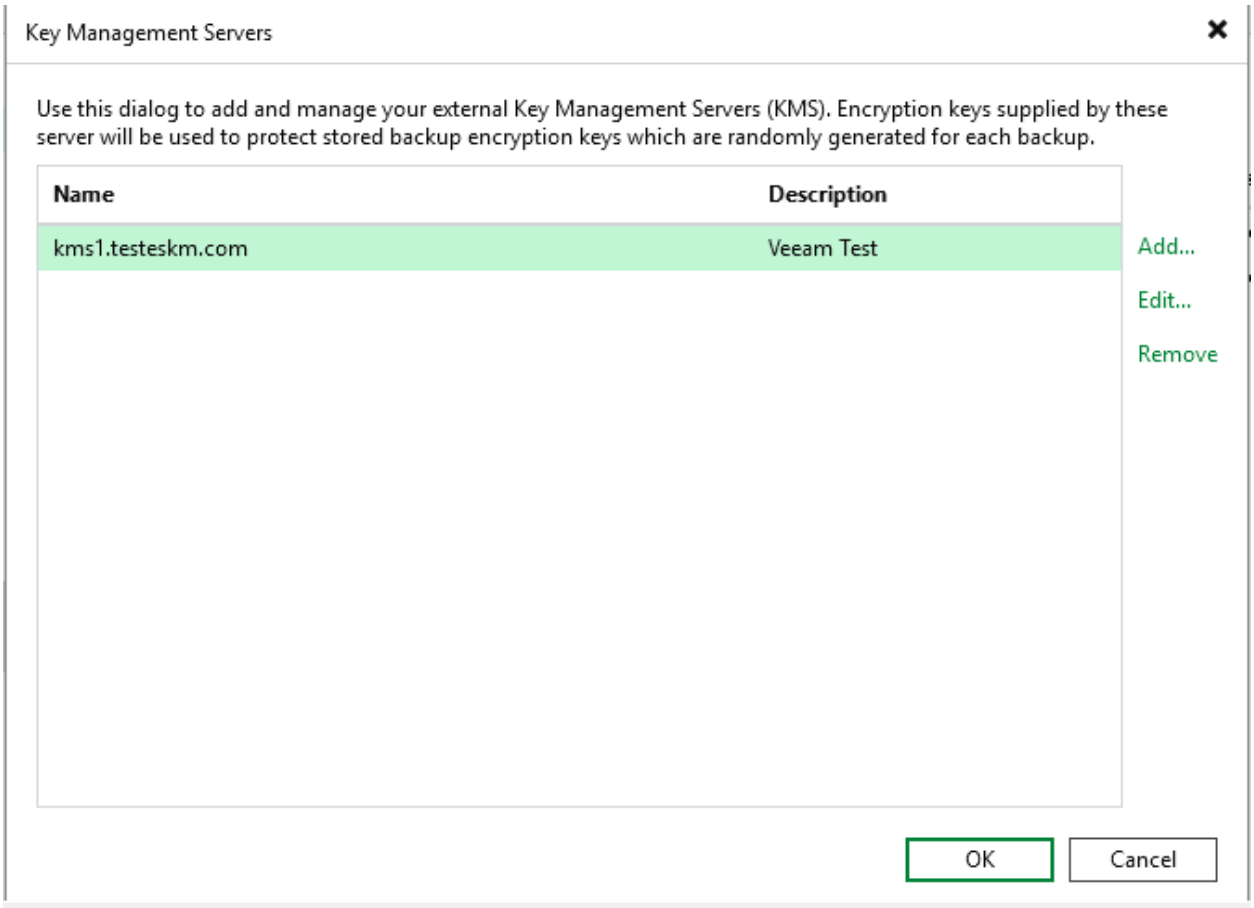

Figure 21 : Configured Key Management Server

5.2.2 Managing Protection Groups

To manage Veeam agents in Veeam Backup & Replication, begin by creating a **Protection Group** in the **Inventory**. Then, define the computers you want to protect within the group settings.

Create a protection group by following the steps described in *Creating Protection Group*.

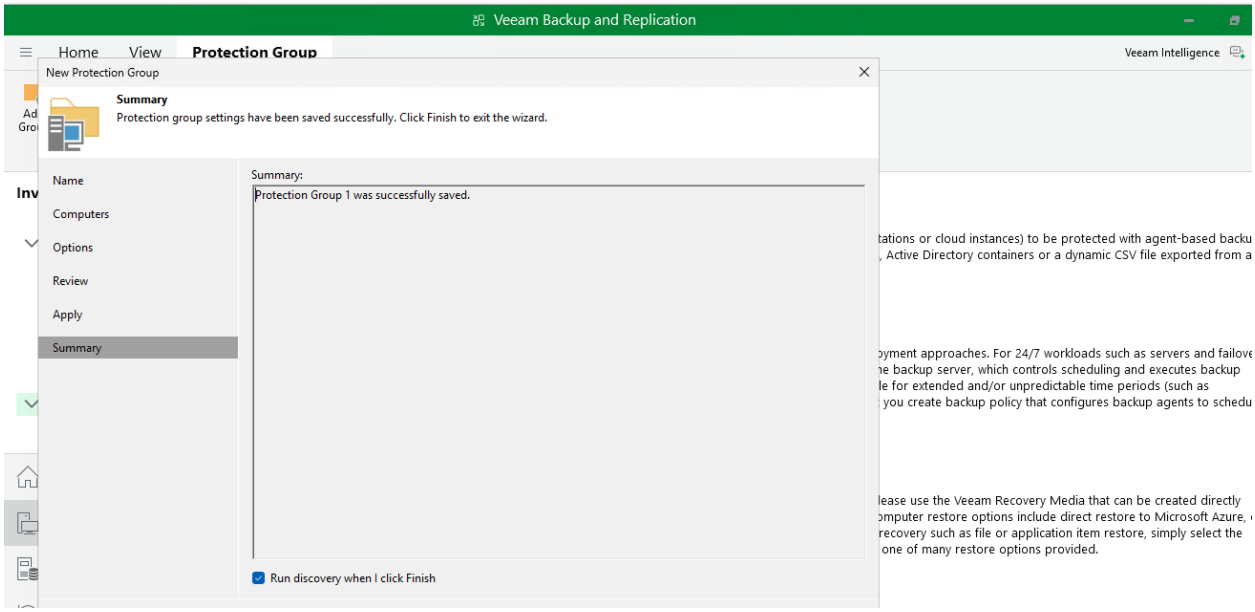

Figure 22 : Created Protection Group

In Veeam Backup & Replication, a **Protection Group** is a logical container that organizes protected computers (virtual machines, physical servers, etc.) for easier management. It allows for grouping computers with similar backup requirements or deployment strategies. These groups are then used to simplify backup job creation and maintenance.

Once a protection group is created, Veeam Backup & Replication launches a rescan job session to establish connections with the computers in the group and carry out the required operations on them.

6 Verification and Testing

In this chapter, we will verify whether the integration between ESKM and Veeam Backup & Replication is functioning as expected. This includes checking connectivity, validating encryption workflows, and ensuring that both systems are communicating correctly. By the end of this section, you should be able to confirm that the integration is successfully established and operational.

6.1 Functional Testing - Creating Backup Jobs

This section outlines the procedures for creating backup jobs for both the entire system and Unstructured Data Backup to Tape.

6.1.1 For the Entire System

To back up VMs, you need to set up a backup job. This involves choosing how, where, and when the VM data will be backed up. Each job can include one or more VMs. Users can run these jobs manually or schedule them to run automatically at set times.

Follow the steps below:

1. Launch the Veeam Backup & Replication application.
2. In the Veeam Backup & Replication console, select the **Backup Jobs** option from the navigation menu and select the required backup job option, such as **Windows Computer**.

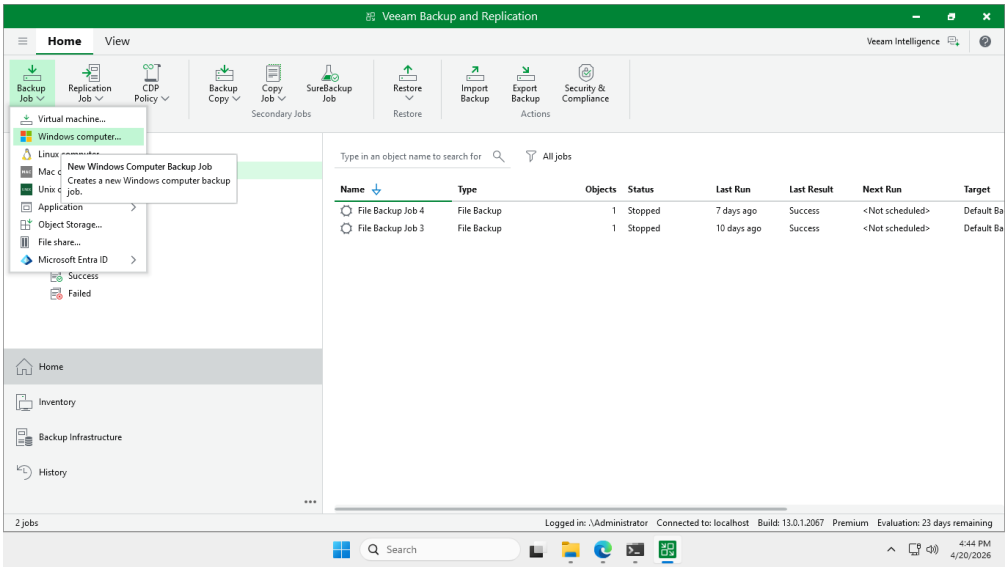

Figure 23 : Backup Job Option is Windows Computer

On the **New Agent Backup Job** page, perform the following actions:

1. In the **Job Mode** section, select the **Type** as **Server** and **Mode** as **Managed by backup server**.

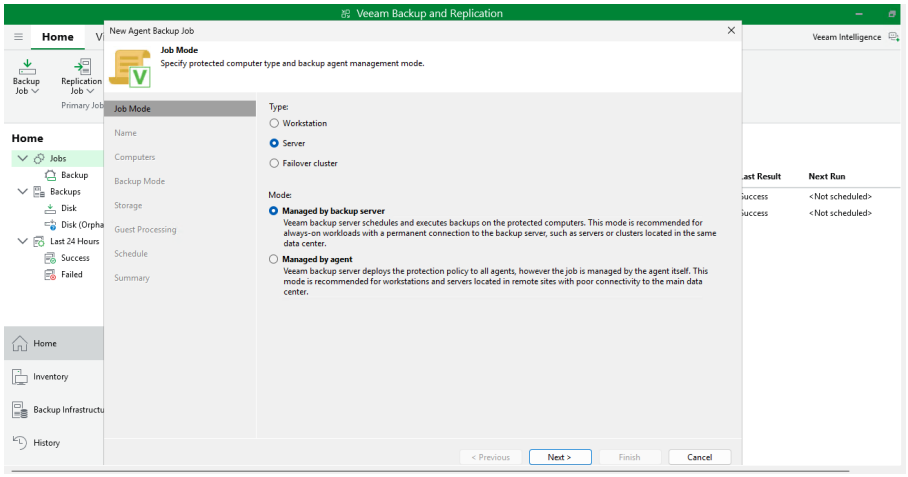

Figure 24 : Choose the Type and Mode

2. In the **Name** section, enter the required name and description of the job. Click **Next** to proceed.

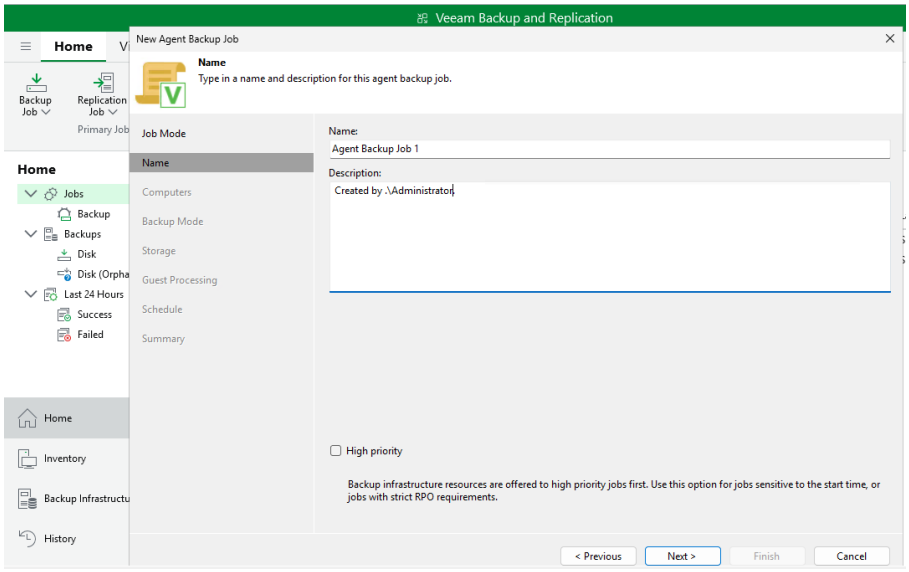

Figure 25 : Add Details

3. In the **Computers** section, click the **Add** > **Protection Group**. Select the required protection group from the list. Click **Next** to proceed.

4. Click **OK**.

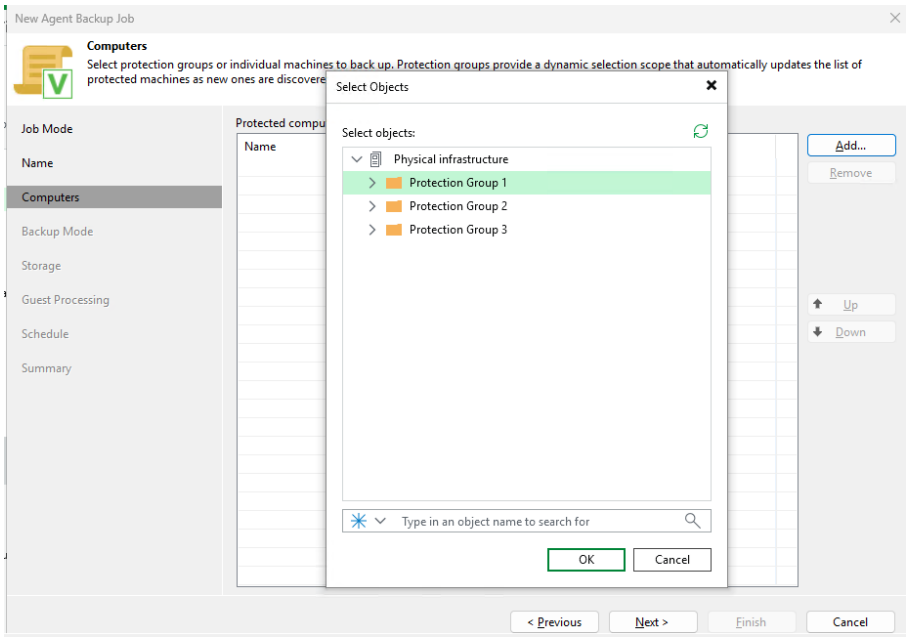

Figure 26 : Choose the Protection Group

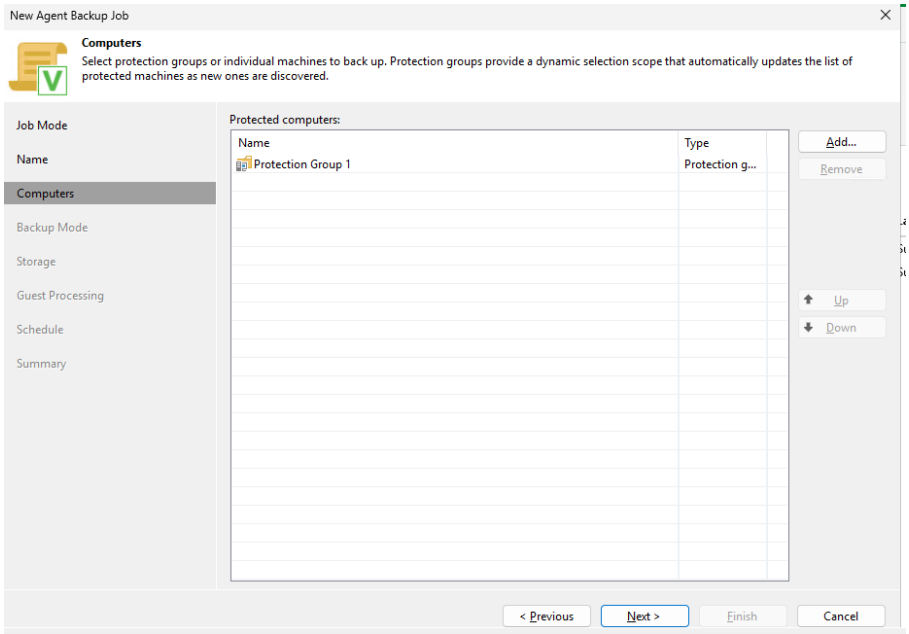

Figure 27 : Protection Group Added

5. In the **Backup Mode** section, select the **Entire computer** radio button to back up the computer image. Click **Next** to proceed.

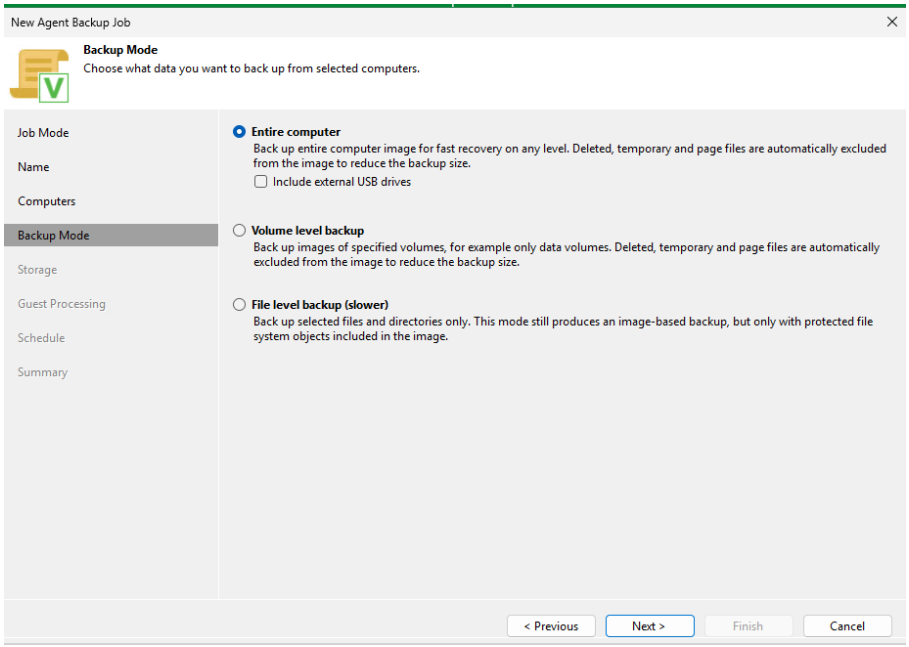

Figure 28 : Select Backup Mode

6. In the **Storage** section, enter the required information in the available field, and then click **Advanced** to encrypt the Backup using ESKM. Click **Next** to proceed.

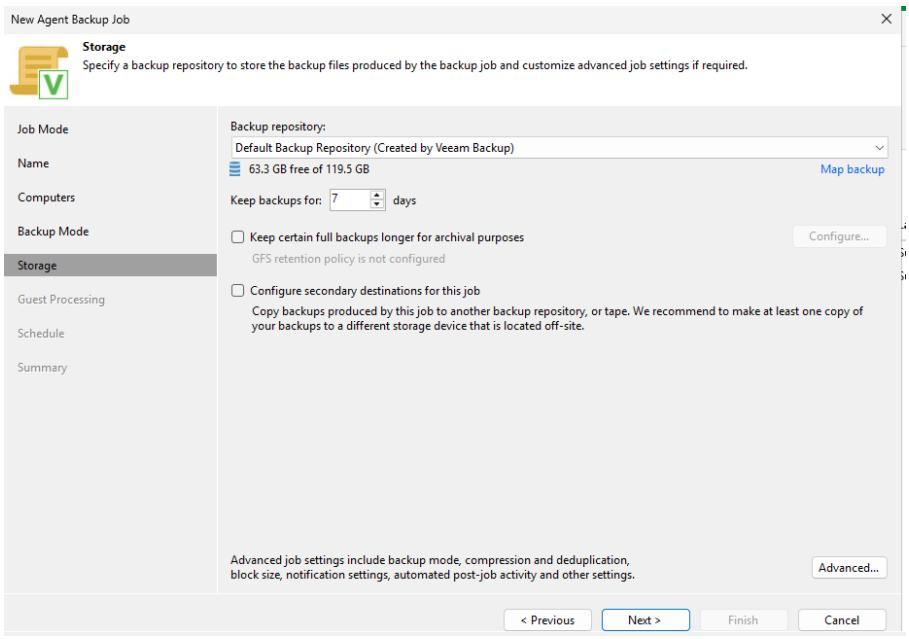

Figure 29 : Configure Storage

7. Click **OK** to proceed.

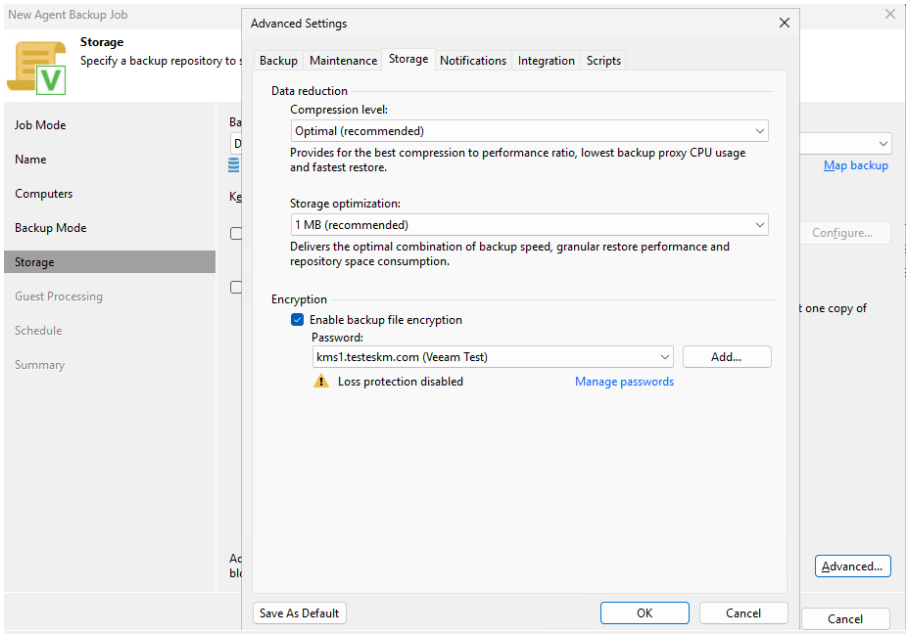

Figure 30 : Storage Configured

8. In the **Guest Processing** section, keep the configuration as the default. Click **Next**.

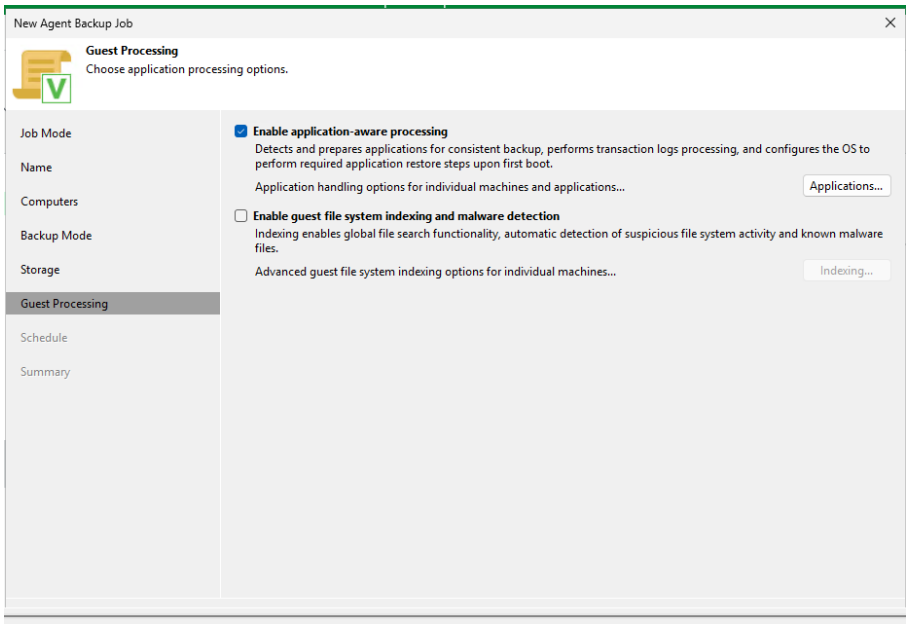

Figure 31 : Configure Guest Processing

9. In the **Schedule** section, select the required option as per your requirements. Click **Apply** to proceed.

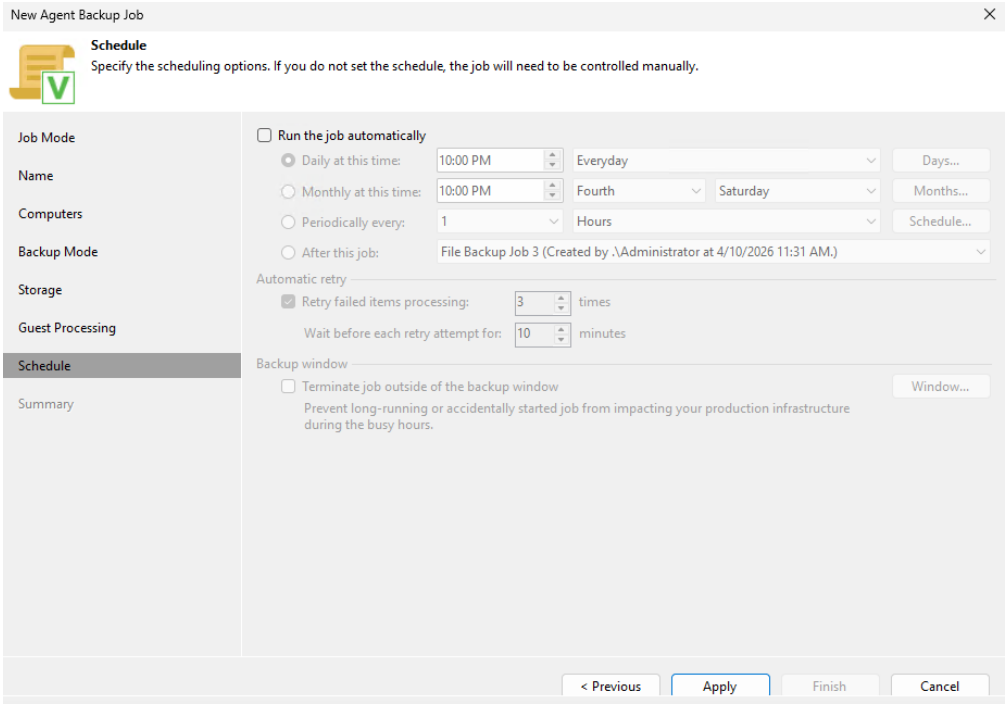

Figure 32 : Schedule Section

10. In the **Summary** section, review the configured settings to verify they align with your requirements, then proceed to confirm the creation of the backup job.

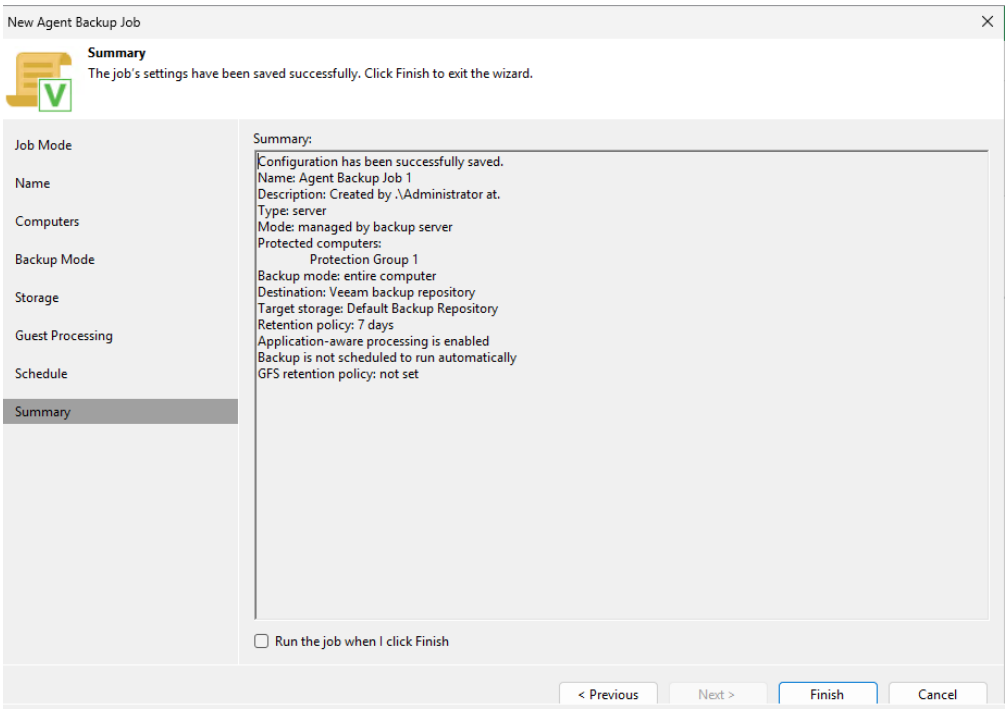

Figure 33 : Summary

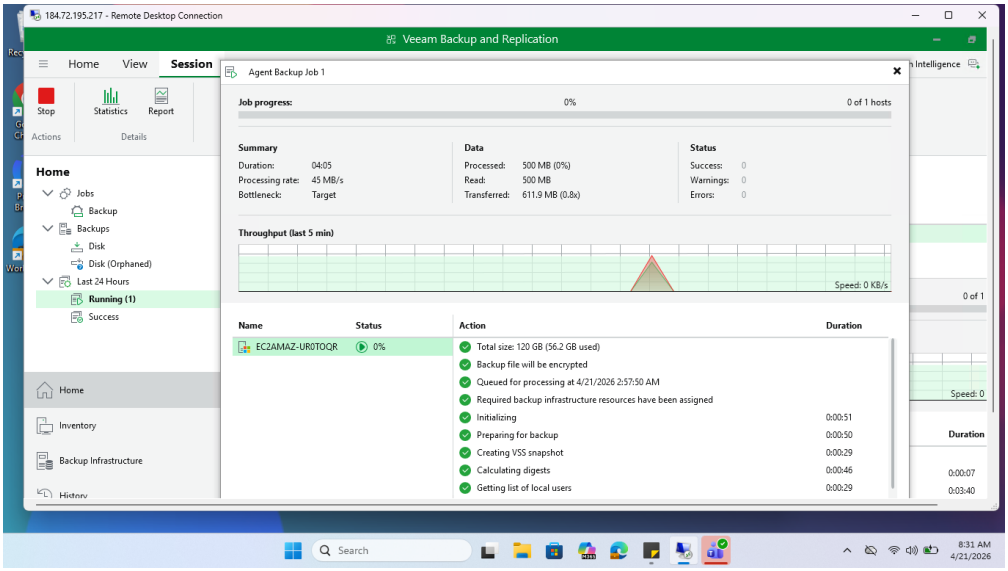

Figure 34 : Graphical Representation of Veeam Backup Job

6.1.2 Unstructured Data Backup to Tape

With Veeam Backup & Replication, unstructured data from various sources can be backed up to tape and restored. Following types of data can be protected:

- Any Microsoft Windows or Linux files.
- Volumes of storage devices with NDMP protocol.
- Data of SMB (CIFS) or NFS file shares.
- Amazon S3, S3 Compatible, Microsoft Azure Blob object storage data.

Add the sources of unstructured data, that has to be protected with the file-to-tape and object-to-tape jobs, to the backup infrastructure.

Now add a Windows- or Linux-managed server as a file server to the inventory of the virtual infrastructure. To do so, follow the steps below.

1. Launch the Veeam Backup & Replication application.
2. In the Veeam Backup & Replication console, select the **Backup Jobs** option from the navigation menu and select the required backup job option, such as **File Share**.

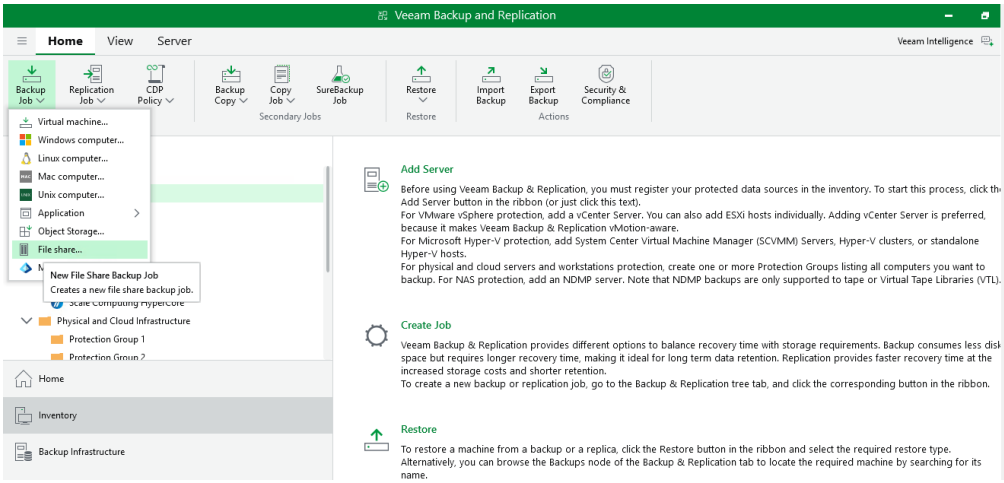

Figure 35 : Click on File Share

3. Select the **File server** as the unstructured data source, and on the next page, enter the **Name** for the backup job.

You can choose **File server**, **File share**, or **NAS filer** as the unstructured data source. The setup steps for all options are similar.

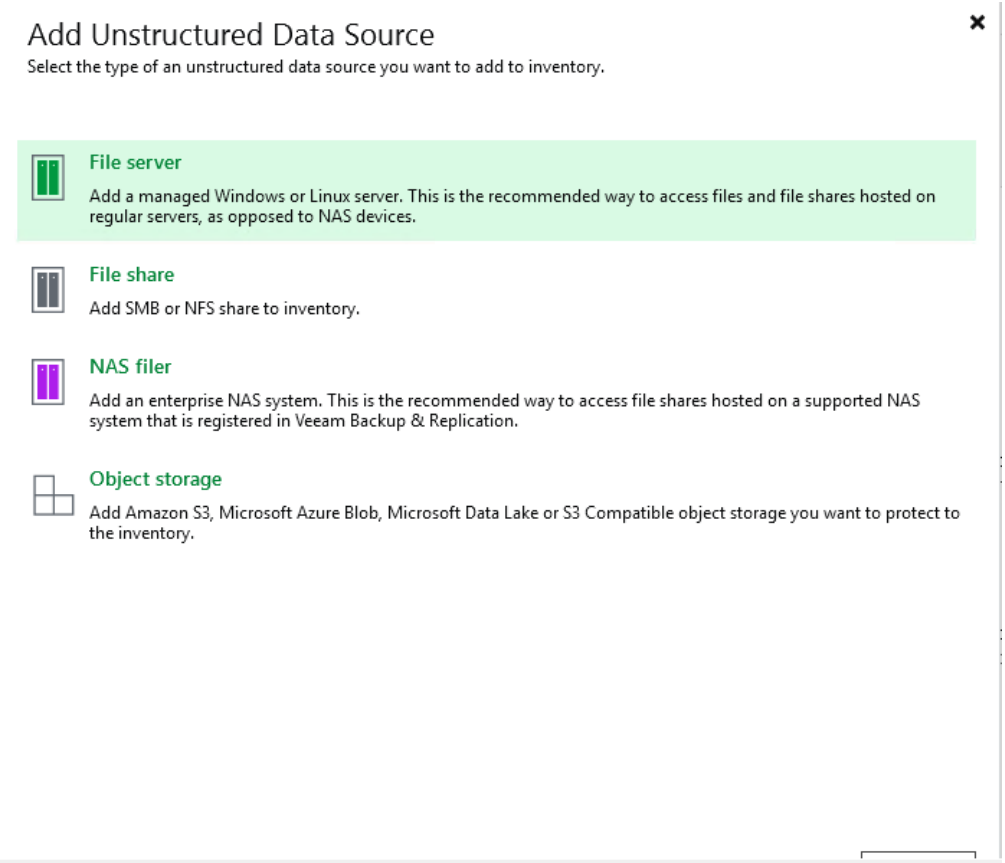

Figure 36 : Unstructured Data Source Added

4. Add a managed server as a **File server** and click **Next**.

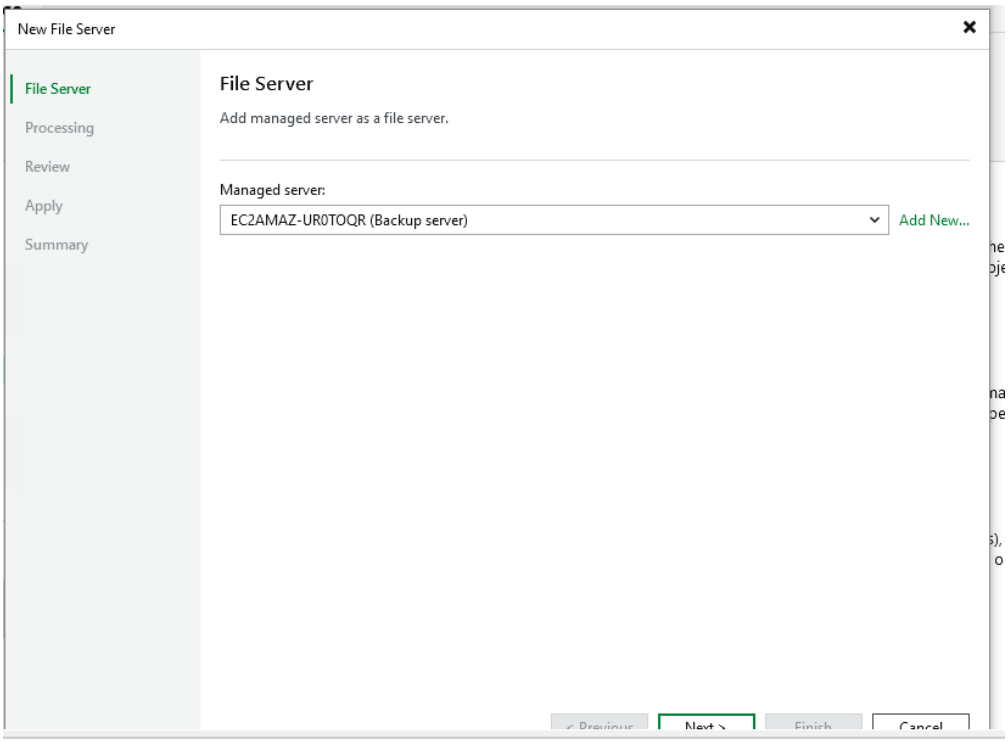

Figure 37 : Add a Managed Server as a File Server

5. Define a cache repository to store the metadata for faster backup performance, and click **Apply**.

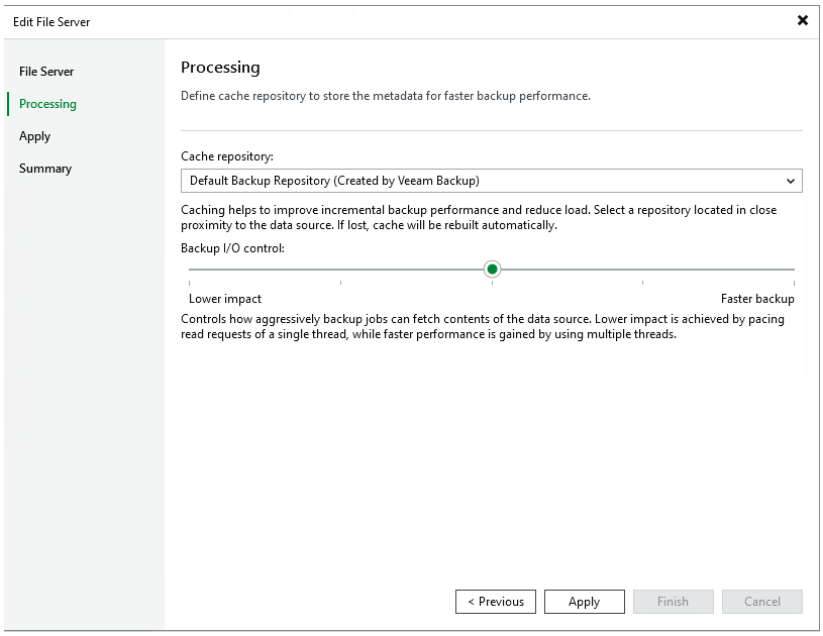

Figure 38 : Cache Repository

6. Review the settings and click **Apply**.

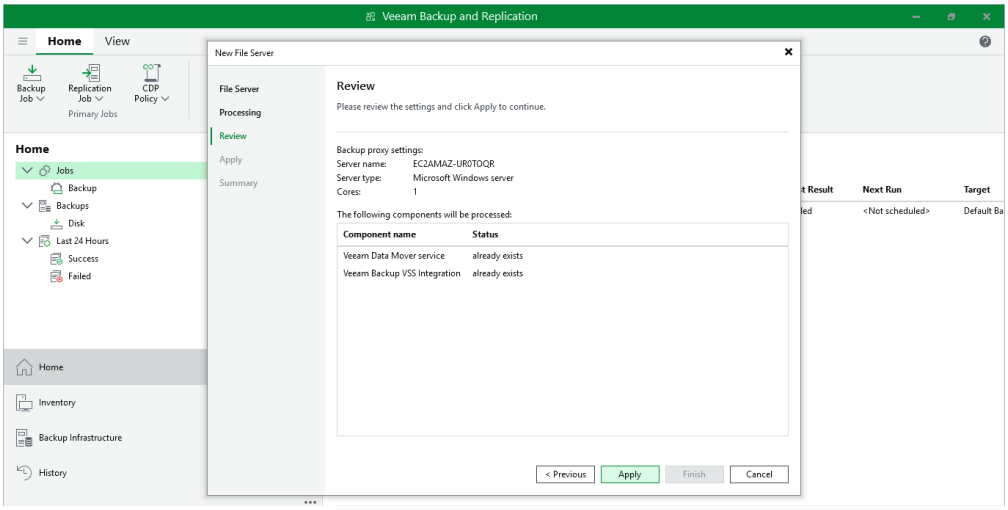

Figure 39 : Review Page

7. The file server was added successfully. Click **Finish**.

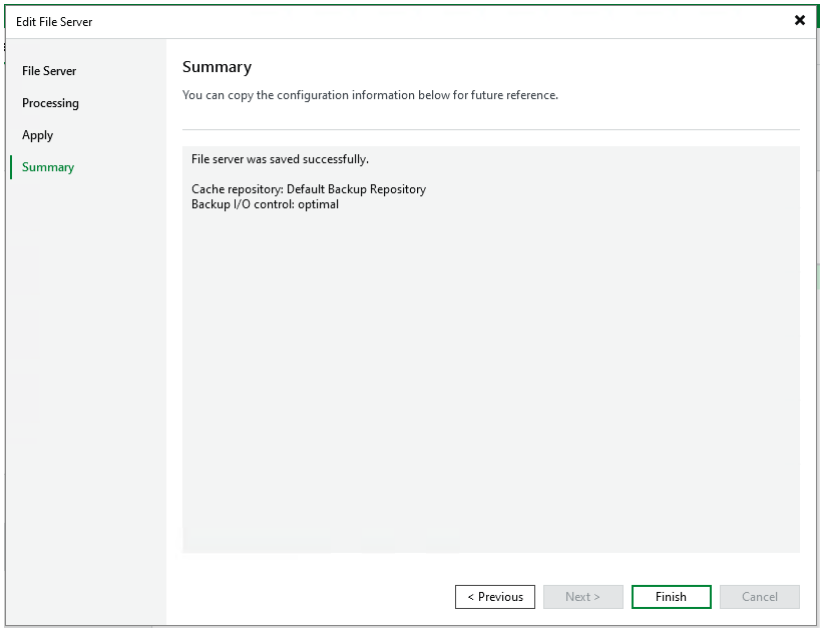

Figure 40 : Summary Window

8. Enter the **Name** and **Description** of the backup job and click **Next**.

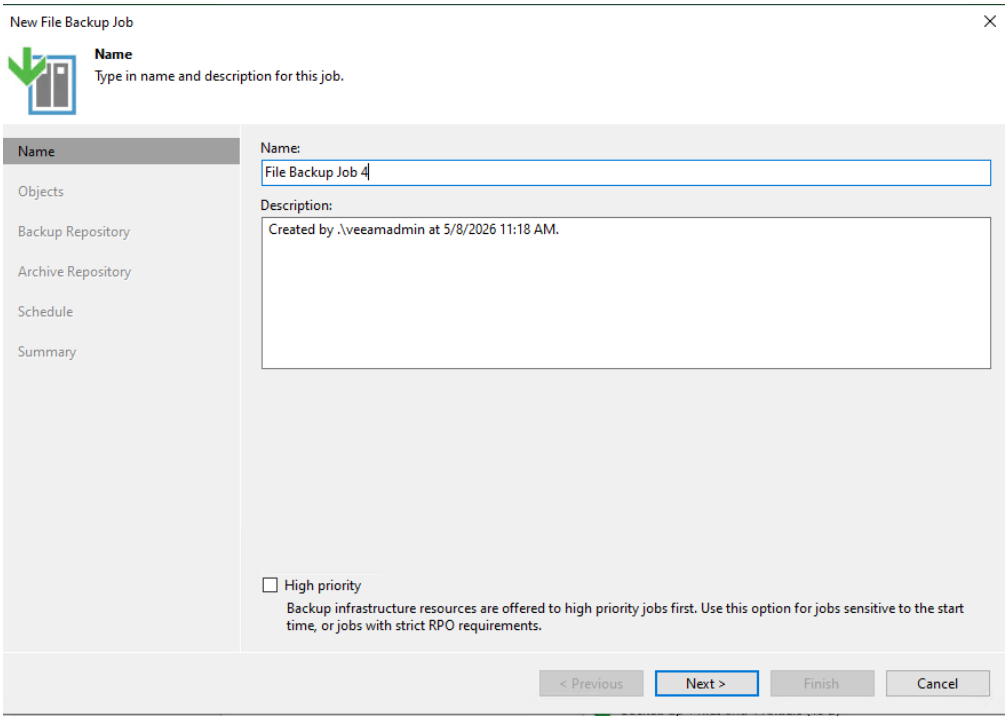

Figure 41 : Enter the Name for the Backup Job

9. Specify objects, files, and folders to be backed up and click **Next**.

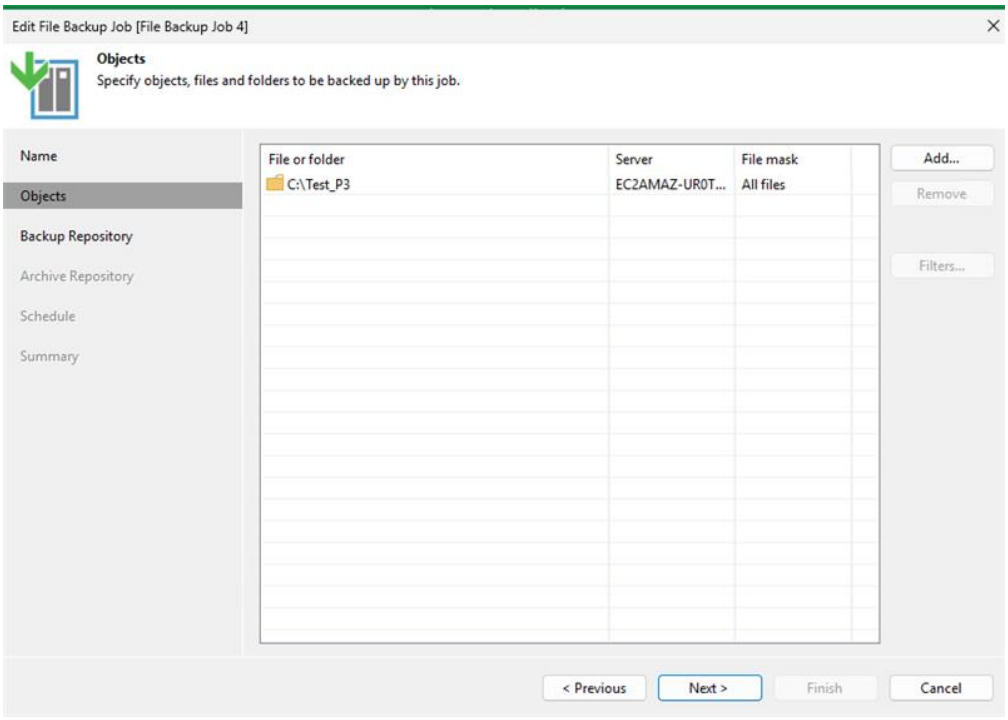

Figure 42 : Add Object

10. In the **Backup repository** section, click on **Advanced**. Under the **Storage** tab, select the **Enable backup file encryption** checkbox. Then, select the registered ESKM Endpoint from the drop-down menu for encrypting the backup files. Click **OK** to proceed.

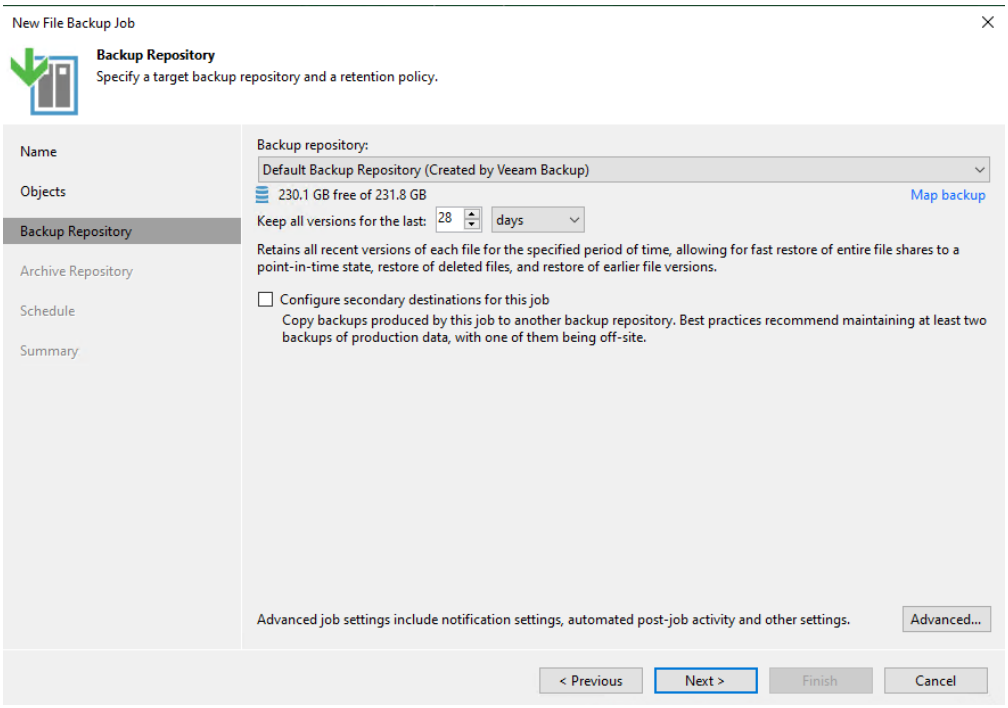

Figure 43 : Backup Repository

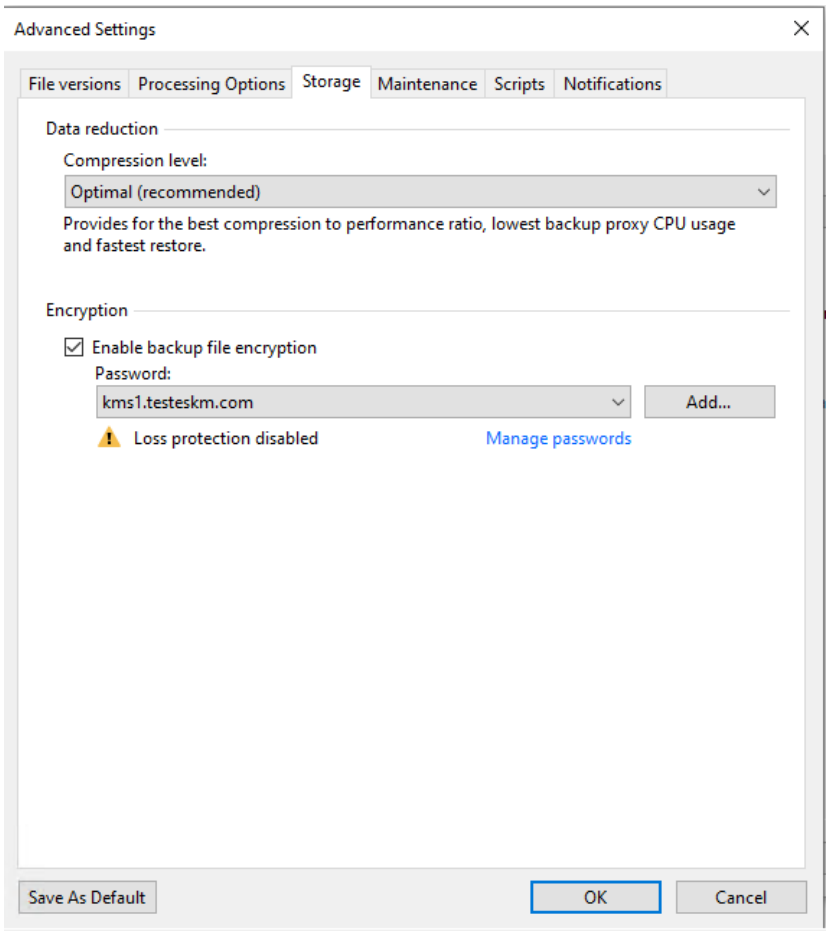

Figure 44 : Storage Tab

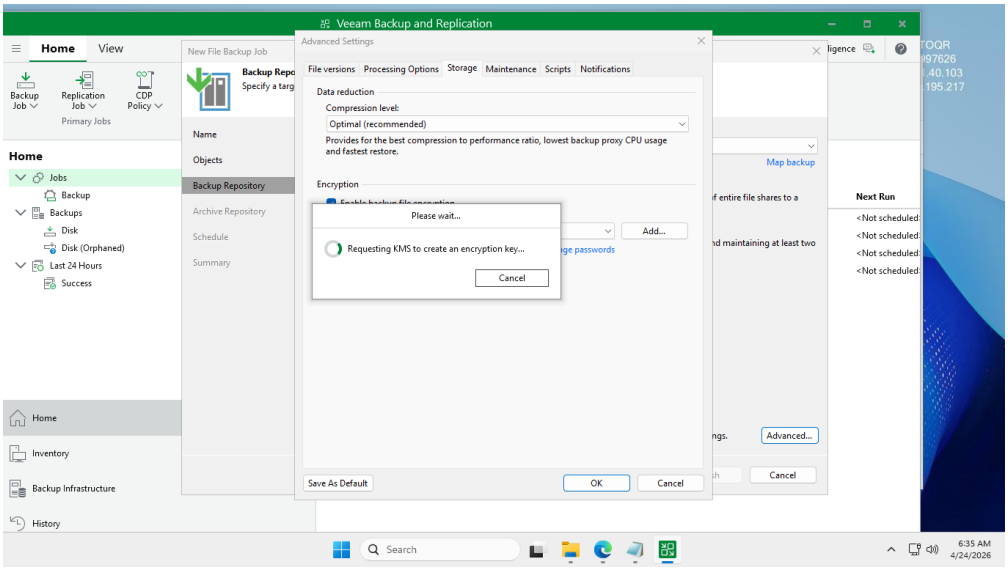

Figure 45 : Requesting KMS to Create an Encryption Key

11. After applying the encryption settings, the **Backup Repository** page is displayed. Click **Next** to continue.
12. Keep the default configuration in the **Archive Repository**. Click **Next**.

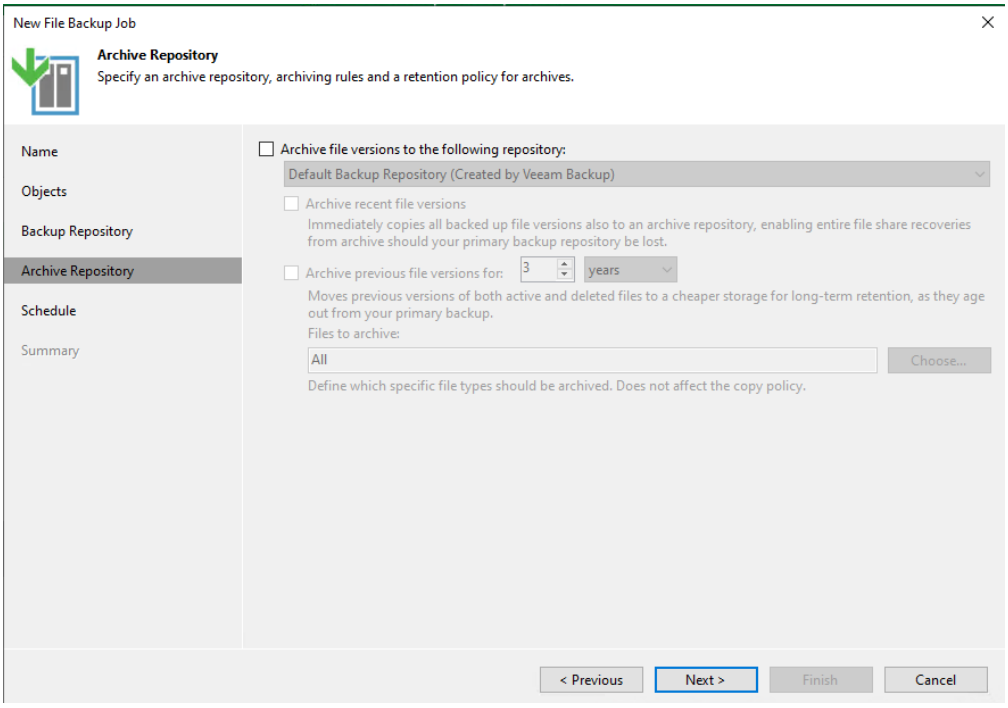

Figure 46 : Archive Repository

13. In the **Schedule** section, select the option that fits your requirements. Click **Apply**.

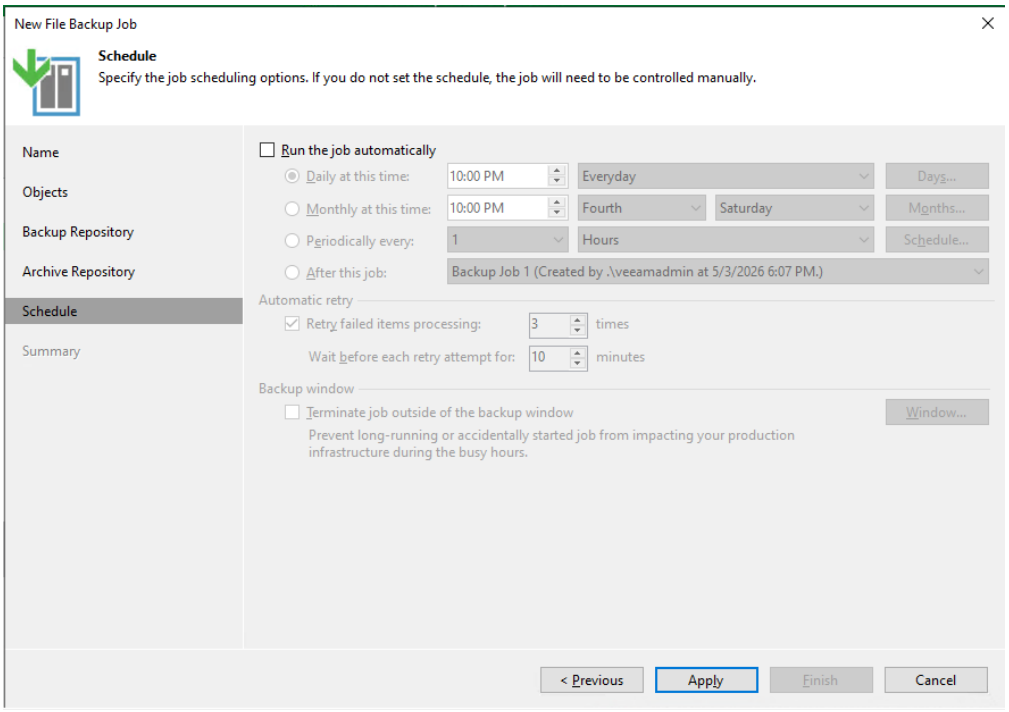

Figure 47 : Schedule Tab

14. In the **Summary** section, review the configured settings to ensure they meet your requirements and confirm the creation of the backup job by clicking **Finish**.

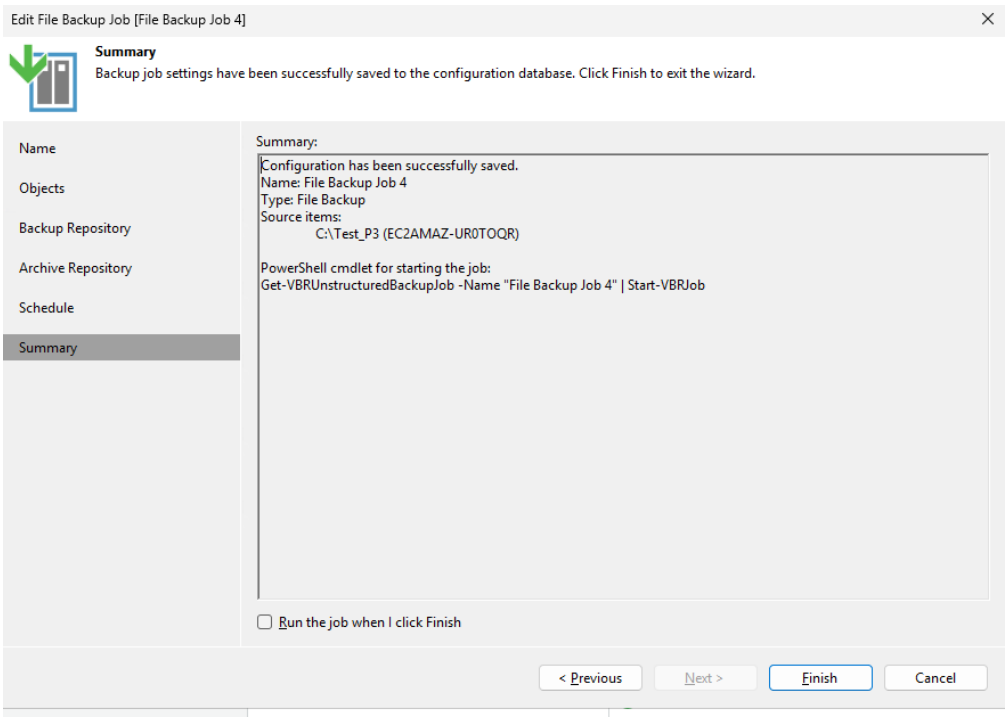

Figure 48 : Summary

6.2 Logs and Validation Steps

6.2.1 Logs and Validation Steps for Creating Backup Jobs

A backup job creates a 4096-bit RSA key on ESKM, which is used to encrypt and decrypt Veeam backup files. We can verify the logs from ESKM by following the steps below.

1. In the ESKM Management console, click **Device** tab.
2. Click **Log Viewer** under **Logs & Statistics**.
3. Click **KMIP** under **Log Viewer**.
4. Review logs related to the encryption and decryption operations performed on Veeam backup jobs.

KMIP Log:

```
2026-04-06 00:37:22 [KMIP Server] [StateChange] Starting KMIP server
2026-04-06 05:28:49 [KMIP Server] [Authentication Success] User:[KMIPClientVeeamBR] From IP: 184.72.195.217
2026-04-06 05:28:49 [KMIP Server] [ClientOperation] User:[KMIPClientVeeamBR] UUID:[] Operation:[QUERY] Result:[SUCCESS]
2026-04-06 05:28:49 [KMIP Server] [Authentication Success] User:[KMIPClientVeeamBR] From IP: 184.72.195.217
2026-04-06 05:28:51 [KMIP Server] [ClientOperation] User:[KMIPClientVeeamBR] UUID:[712e2c4d-0111-48a3-bdb4-cc455b83f92f(Private):1ed471fe-1fac-
2026-04-06 05:28:51 [KMIP Server] [Authentication Success] User:[KMIPClientVeeamBR] From IP: 184.72.195.217
2026-04-06 05:28:51 [KMIP Server] [ClientOperation] User:[KMIPClientVeeamBR] UUID:[1ed471fe-1fac-4947-8ef0-52044f02da31] Operation:[ACTIVATE] O
2026-04-06 05:28:51 [KMIP Server] [Authentication Success] User:[KMIPClientVeeamBR] From IP: 184.72.195.217
2026-04-06 05:28:51 [KMIP Server] [ClientOperation] User:[KMIPClientVeeamBR] UUID:[712e2c4d-0111-48a3-bdb4-cc455b83f92f] Operation:[ACTIVATE] O
2026-04-06 05:28:51 [KMIP Server] [Authentication Success] User:[KMIPClientVeeamBR] From IP: 184.72.195.217
2026-04-06 05:28:51 [KMIP Server] [ClientOperation] User:[KMIPClientVeeamBR] UUID:[1ed471fe-1fac-4947-8ef0-52044f02da31] Operation:[ENCRYPT] Ob
2026-04-06 05:28:51 [KMIP Server] [Authentication Success] User:[KMIPClientVeeamBR] From IP: 184.72.195.217
2026-04-06 05:28:51 [KMIP Server] [ClientOperation] User:[KMIPClientVeeamBR] UUID:[712e2c4d-0111-48a3-bdb4-cc455b83f92f] Operation:[DECRYPT] Ob
2026-04-08 20:32:41 [KMIP Server] [Authentication Success] User:[KMIPClientVeeamBR] From IP: 184.72.195.217
2026-04-08 20:32:41 [KMIP Server] [ClientOperation] User:[KMIPClientVeeamBR] UUID:[] Operation:[QUERY] Result:[SUCCESS]
2026-04-08 20:32:41 [KMIP Server] [Authentication Success] User:[KMIPClientVeeamBR] From IP: 184.72.195.217
2026-04-08 20:32:43 [KMIP Server] [ClientOperation] User:[KMIPClientVeeamBR] UUID:[6b79a3fb-0bed-4103-b315-d960eeff5a86(Private):f1bc14f4-825f-
2026-04-08 20:32:43 [KMIP Server] [Authentication Success] User:[KMIPClientVeeamBR] From IP: 184.72.195.217
2026-04-08 20:32:43 [KMIP Server] [ClientOperation] User:[KMIPClientVeeamBR] UUID:[f1bc14f4-825f-446e-b130-910a51376155] Operation:[ACTIVATE] O
2026-04-08 20:32:43 [KMIP Server] [Authentication Success] User:[KMIPClientVeeamBR] From IP: 184.72.195.217
2026-04-08 20:32:43 [KMIP Server] [ClientOperation] User:[KMIPClientVeeamBR] UUID:[6b79a3fb-0bed-4103-b315-d960eeff5a86] Operation:[ACTIVATE] O
2026-04-08 20:32:43 [KMIP Server] [Authentication Success] User:[KMIPClientVeeamBR] From IP: 184.72.195.217
2026-04-08 20:32:43 [KMIP Server] [ClientOperation] User:[KMIPClientVeeamBR] UUID:[f1bc14f4-825f-446e-b130-910a51376155] Operation:[ENCRYPT] Ob
2026-04-08 20:32:43 [KMIP Server] [Authentication Success] User:[KMIPClientVeeamBR] From IP: 184.72.195.217
2026-04-08 20:32:43 [KMIP Server] [ClientOperation] User:[KMIPClientVeeamBR] UUID:[6b79a3fb-0bed-4103-b315-d960eeff5a86] Operation:[DECRYPT] Ob
```

Figure 49 : ESKM Log Details

5. To view the keys, go to the **Security** tab.
6. Select **KMIP Objects** under the **Keys & KMIP Objects** section. The generated keys will appear here.

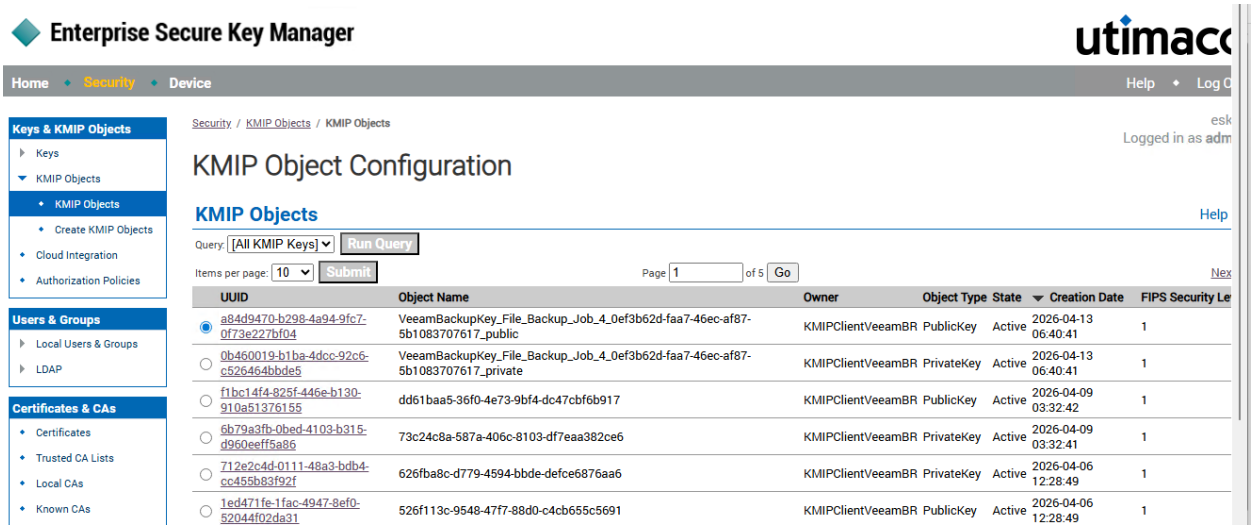

Figure 50 : KMIP Objects

7 Troubleshooting

7.1 Common Issues

If the KMIP server certificate configured in ESKM does not meet the requirements mentioned in the prerequisites, the following error will be encountered while configuring the Key Management Server in Veeam.

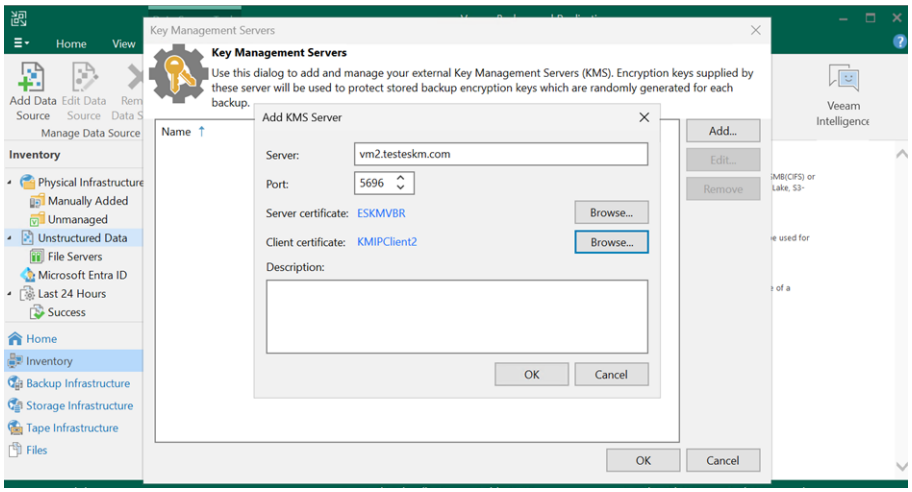

Figure 51 : Add KMS Server Page

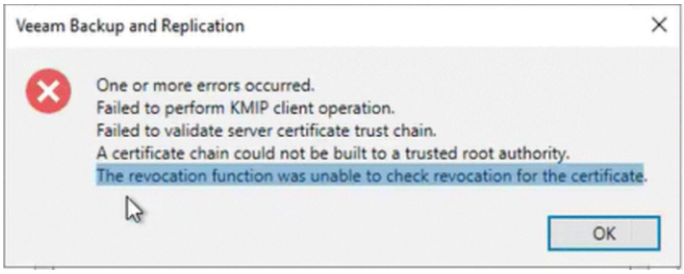

Figure 52 : Error Pop-up

7.2 Log Locations and Interpretation

For detailed steps on log verification, refer to *Logs and Validation Steps for Creating Backup Jobs*.

8 Contact and Support Information

You can reach us from Monday to Friday, 09.00 a.m. to 05.00 p.m., Central European Time (CET).

Utimaco IS GmbH
Krefelder Str. 220
52070 Aachen
Germany

RMA Query

If you need to send the device back to Utimaco IS GmbH, please open a new RMA case (Return Merchandise Authorization). We request that you use the following web address. RMA cases cannot be opened by email or phone.

https://support.hsm.utimaco.com/support/rma/new

Other Support Queries

- Mail (preferred contact method)
  support@utimaco.com
  Attach the diagnostic information to your email.
- Web portal
  https://support.hsm.utimaco.com/support/cases/new/
  The diagnostic information will be requested in our response if necessary.
- By phone
  AMERICAS +1-844-UTIMACO (+1 844-884-6226)
  EMEA +49 800-627-3081
  APAC +81 800-919-1301
  The diagnostic information will be requested in our response if necessary.

You can reach us from Monday to Friday, 09.00 a.m. to 05.00 p.m., Central European Time (CET).

Utimaco IS GmbH
Krefelder Str. 220
52070 Aachen
Germany

RMA Query

If you need to send the device back to Utimaco IS GmbH, please open a new RMA case (Return Merchandise Authorization). We request that you use the following web address. RMA cases cannot be opened by email or phone.

https://support.hsm.utimaco.com/support/rma/new

Other Support Queries

- Mail (preferred contact method)
  support@utimaco.com
  Attach the diagnostic information to your email.
- Web portal
  https://support.hsm.utimaco.com/support/cases/new/
  The diagnostic information will be requested in our response if necessary.
- By phone
  AMERICAS +1-844-UTIMACO (+1 844-884-6226)
  EMEA +49 800-627-3081
  APAC +81 800-919-1301
  The diagnostic information will be requested in our response if necessary.

9 Appendices

9.1 References

This document serves as a comprehensive guide for integrating ESKM module with Veeam Backup & Replication.

Title	Description	Document/Link
ESKM Installation Guide	Step-by-step guide for installing and configuring ESKM	*2021-0047 Installation and Replacement Guide*
Veeam Backup & Replication Installation Guide	User Guide for Deploying and Installing Veeam Backup & Replication on Windows	https://helpcenter.veeam.com/archive/backup/120/hyperv/install_vbr.html
Installing Veeam Infrastructure Appliance with ISO	User guide for deploying Veeam Backup & Replication using the Linux-based infrastructure appliance ISO.	*Installing Veeam Infrastructure Appliance with ISO - Veeam Backup & Replication User Guide*
Protection Group Creation	User guide for creating and configuring protection groups in Veeam Backup & Replication	https://helpcenter.veeam.com/docs/backup/agents/protection_group_add.html?ver=120

Table 5: References

For more information on other Utimaco products and offerings, please visit the official Utimaco website: *Utimaco Portal*.