Veeam

Backup & Replication

12.3.1.1139

Integration Guide

ESKM

8.54.0

utimaco®

Imprint

Copyright 2025	Utimaco IS GmbH
	Germanusstr. 4
	D-52080 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	1.0.0
Date	2025-07-18
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 Utimaco ESKM with Veeam Backup & Replication to enable secure and encrypted backup functionality. Together, Veeam Backup & Replication and Utimaco ESKM deliver a comprehensive solution for secure, compliant, and resilient data protection. The guide walks through 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 Utimaco ESKM administrators.

1.3 Purpose of the Integration

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

The primary objective of this integration is to:

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

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	Press **OK**
`Monospaced`	Code that is given for explanation or as an example, file paths	`chsm-create`
Italic	References and important terms	See *Sample Chapter* in the *CryptoServer - Sample Manual*

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 Utimaco 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 Key Management Interoperability Protocol (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 Utimaco 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 Utimaco ESKM with Veeam Backup & Replication.

Operating System	Veeam Backup & Replication Version	Utimaco ESKM Version
Windows Server 2025 Datacenter Edition	12.3.1.1139	8.54.0

Table 3: List of Tested Versions

3.2 Supported Platforms

- Utimaco ESKM hardware appliance
- Utimaco ESKM virtual/cloud appliance

3.3 Software Requirements

Software	Software Requirements
Utimaco ESKM	8.54.0
Veeam Backup & Replication Version	12.3.1.1139

Table 4: List of Software Requirements

3.4 Prerequisites

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

- **Veeam Backup & Replication Version**: 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.
- 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.

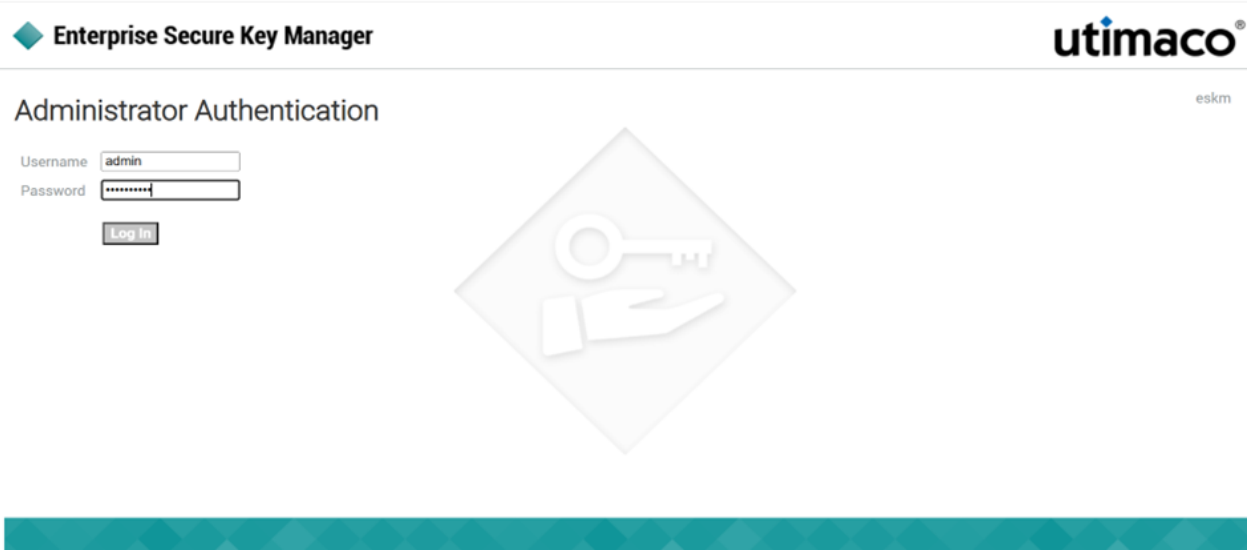

Figure 1 : ESKM Login

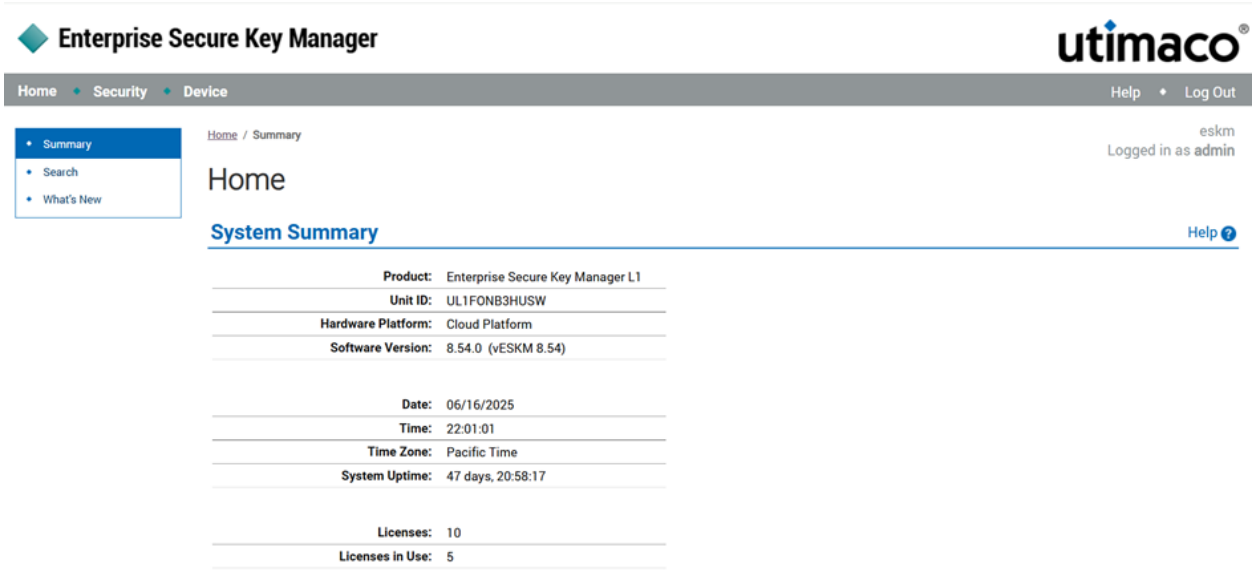

Figure 2 : ESKM Home Page

4.2 Setting up Veeam Backup & Replication

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.

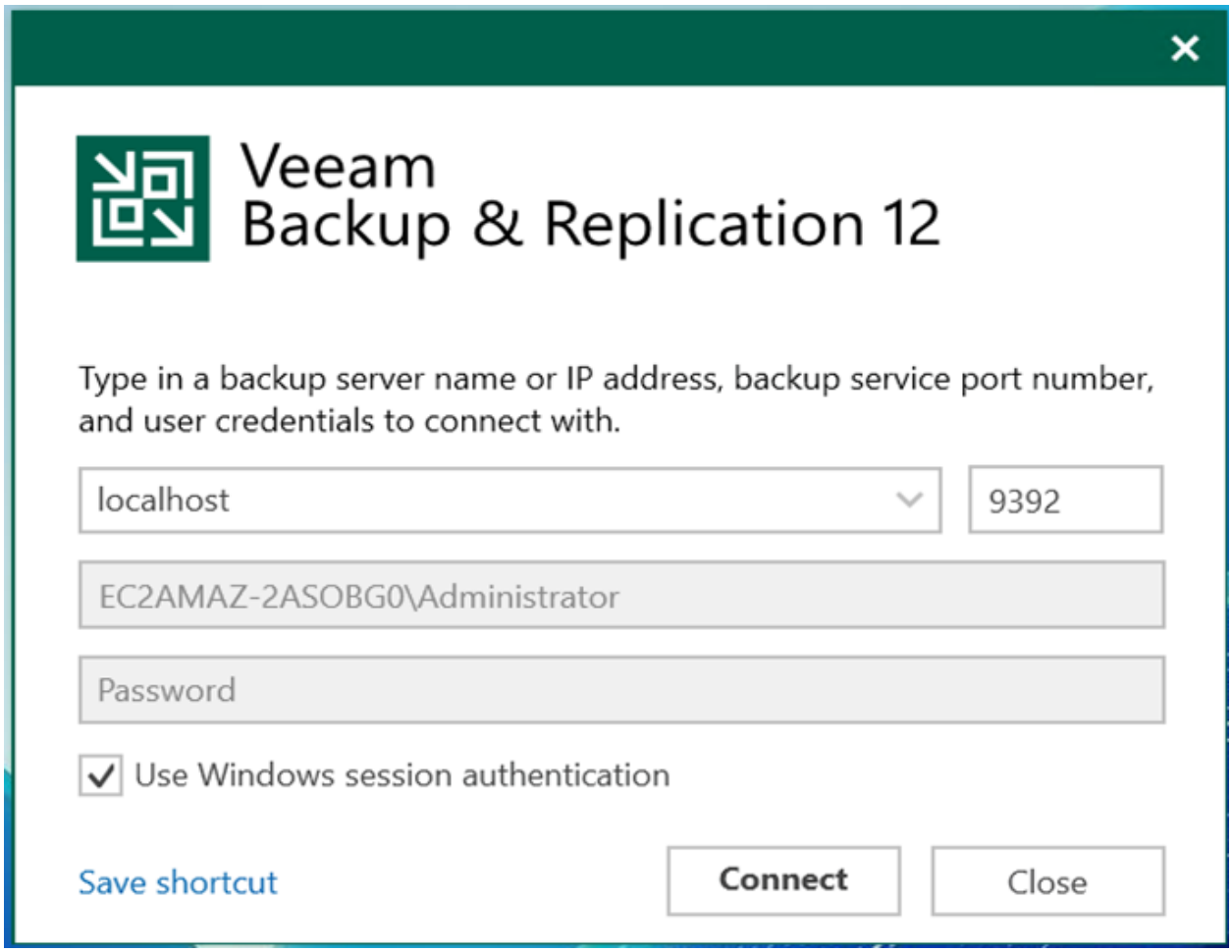

Figure 3 : Veeam Backup & Replication Login Page

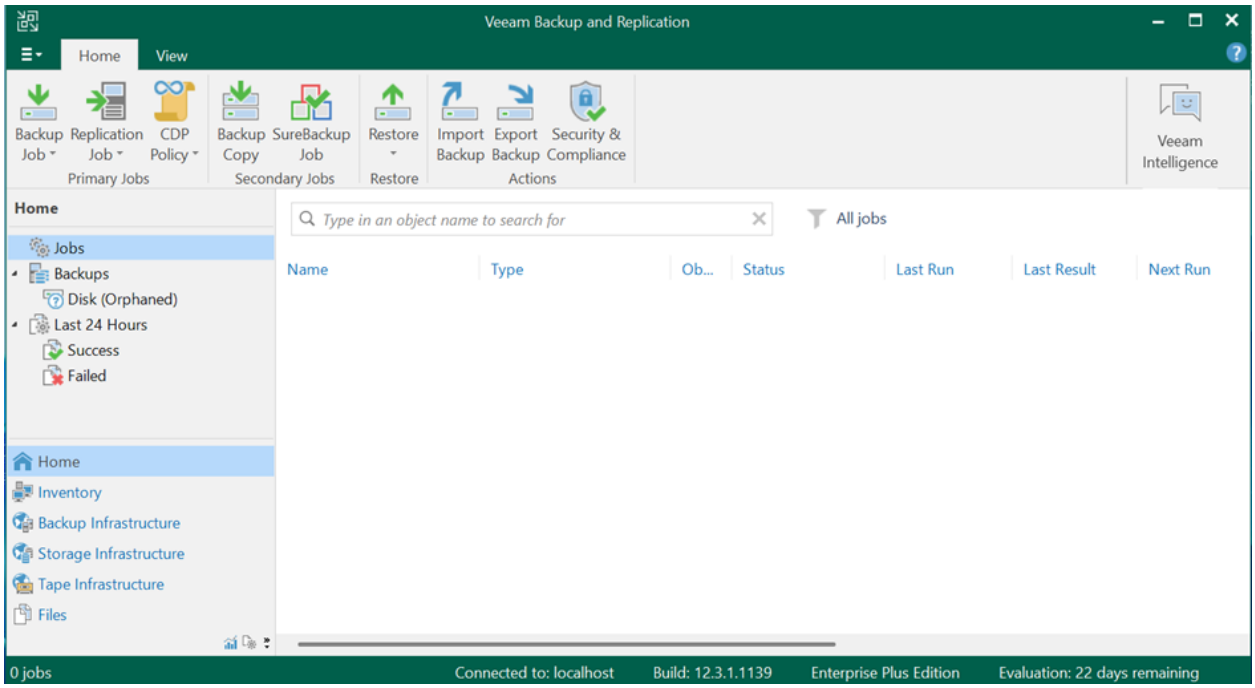

Figure 4 : Veeam Backup & Replication Main Page

5 Integration Steps

To support a robust and secure backup infrastructure, integrating a Key Management Service (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 Utimaco ESKM as a Key Management Service (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 Utimaco ESKM

It is essential to configure Utimaco 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 **Create Certificate** section.
4. Enter a **Certificate Authority Name** and **Common Name**. These may have the same value, for example, ESKM Local CA.
5. Enter your **Organizational information.**
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.**

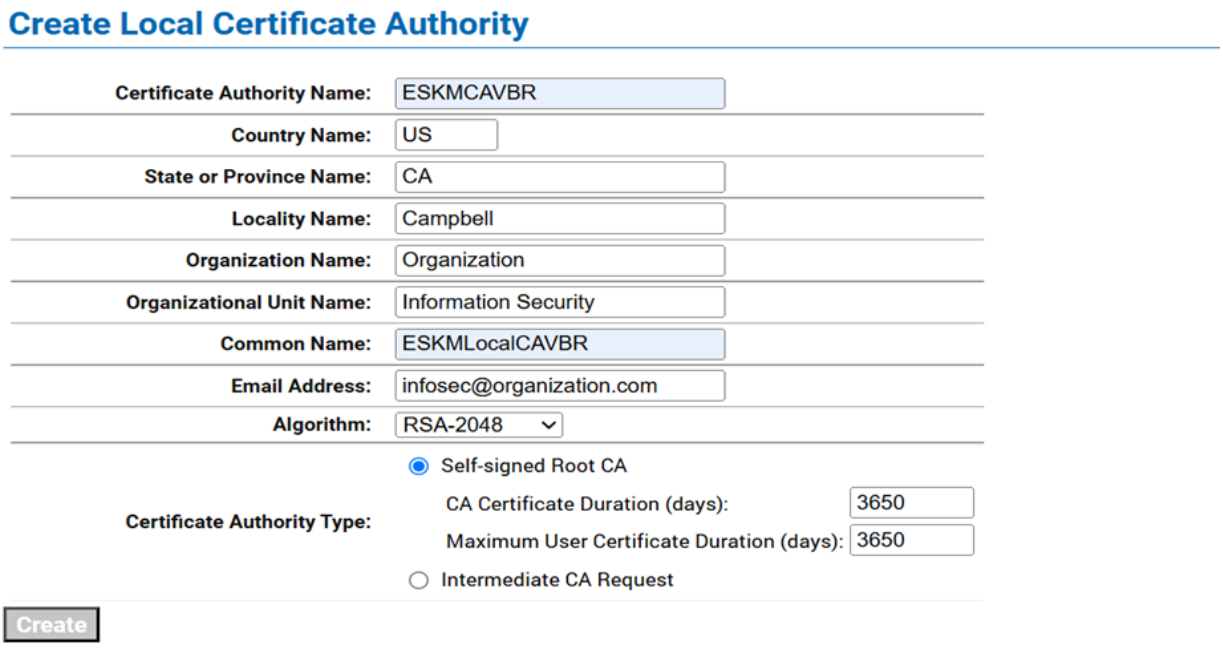

Figure 5 : Local CA Creation Page

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

Figure 6 : 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.**

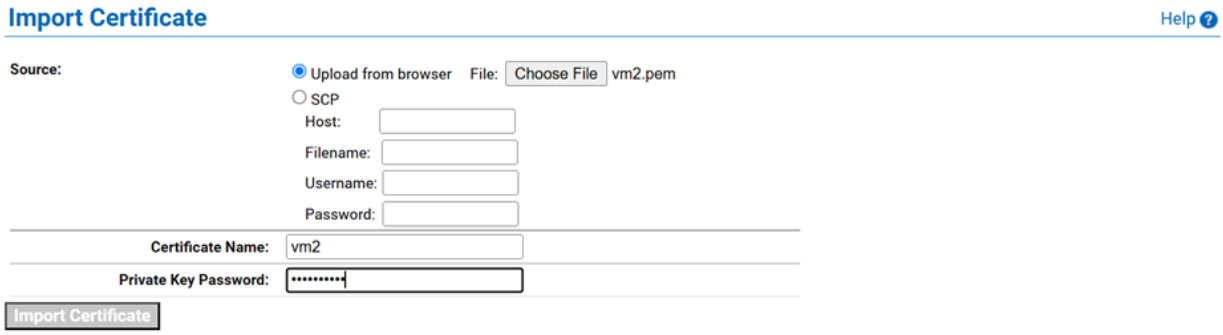

Figure 7 : Import Certificate

5. Click **Import Certificate.**

Figure 8 : 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 client certificate:

1. Go to the **Security** tab.
2. Go to the **Security** tab and in the **Certificates & CA**, click **Certificates.**
3. Scroll down to the **Create Certificate** section.

4. Enter a **Certificate Name** and **Common Name** (for example KMIPClient2).
5. Enter your **Organizational information**.
6. Enter or Type the **Subject Alternative Name, Algorithm.**
7. Choose the **Creation Type** as **Certificate Signed by Local CA** (Select the CA name you created in Setting up local CA, for example, ESKMCAVBR).
8. Select the **Certificate Purpose** as **Client.**
9. Click **Create.**

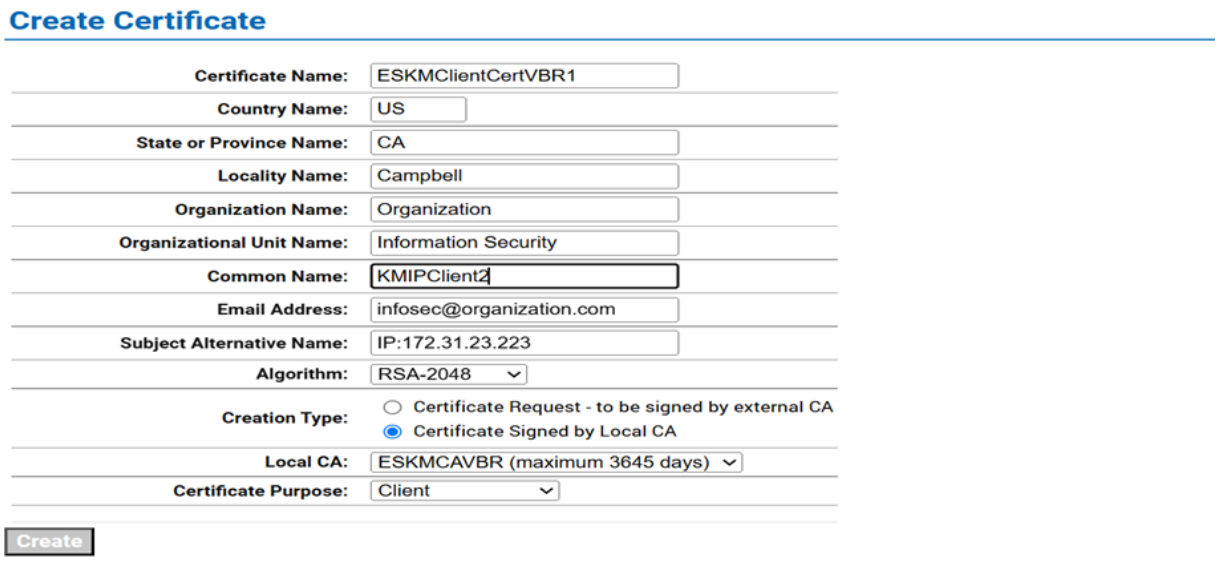

Figure 9 : Client Certificate Creation

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

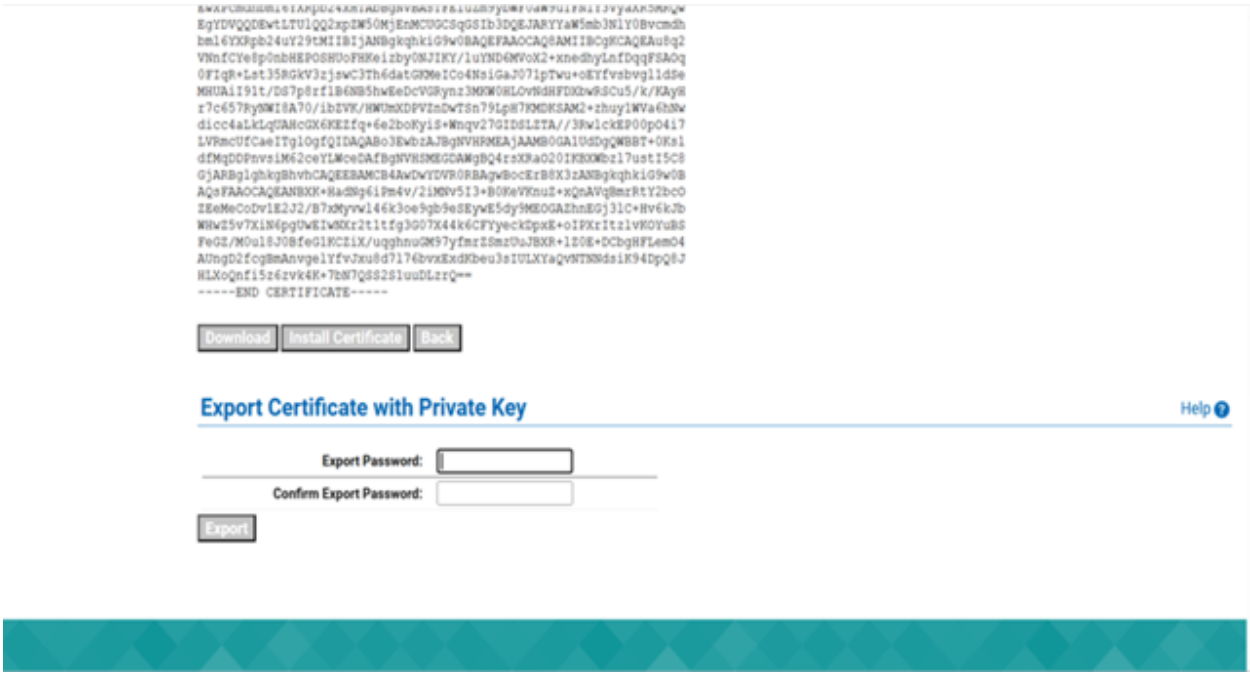

Figure 10 : Exporting Client Certificate

11. The certificate will be downloaded in p12 format.
12. Click the **Download** button to save the certificate content for local user creation.

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. In the **Users & Groups > Local Users and Groups**, select **Local Users**.
3. Scroll down and click **Add.**
4. Enter the **Username,** which is the same as the **Common Name (KMIPClient2)** provided during client certificate creation.
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**.

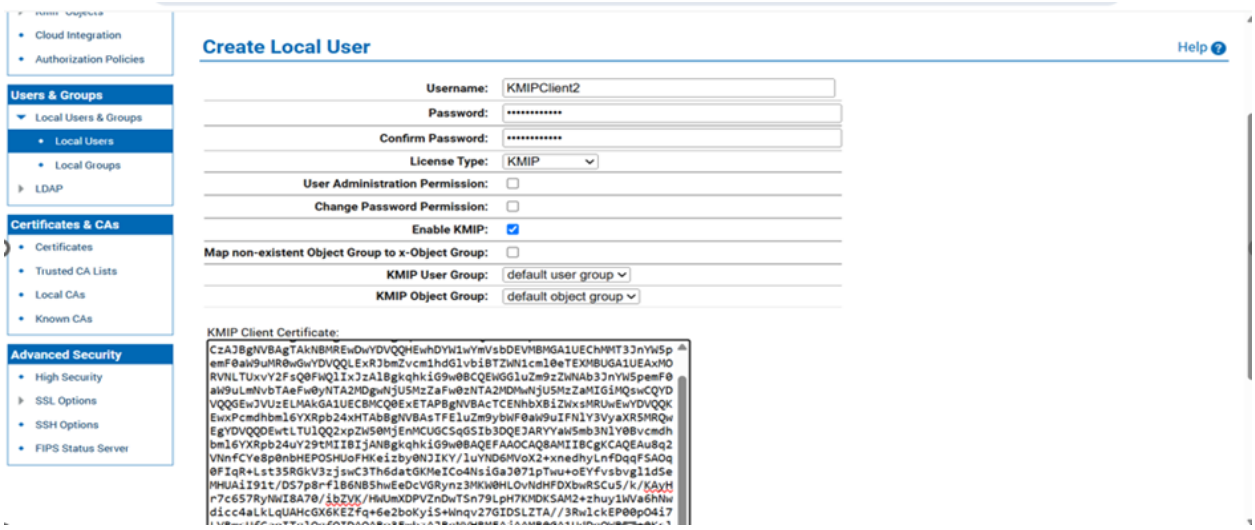

Figure 11 : Local User Creation

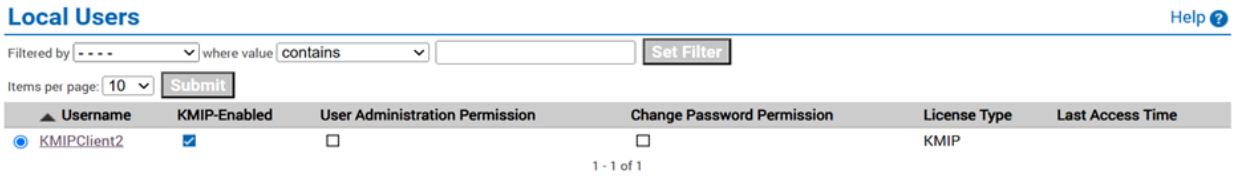

Figure 12 : Created Local User

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.

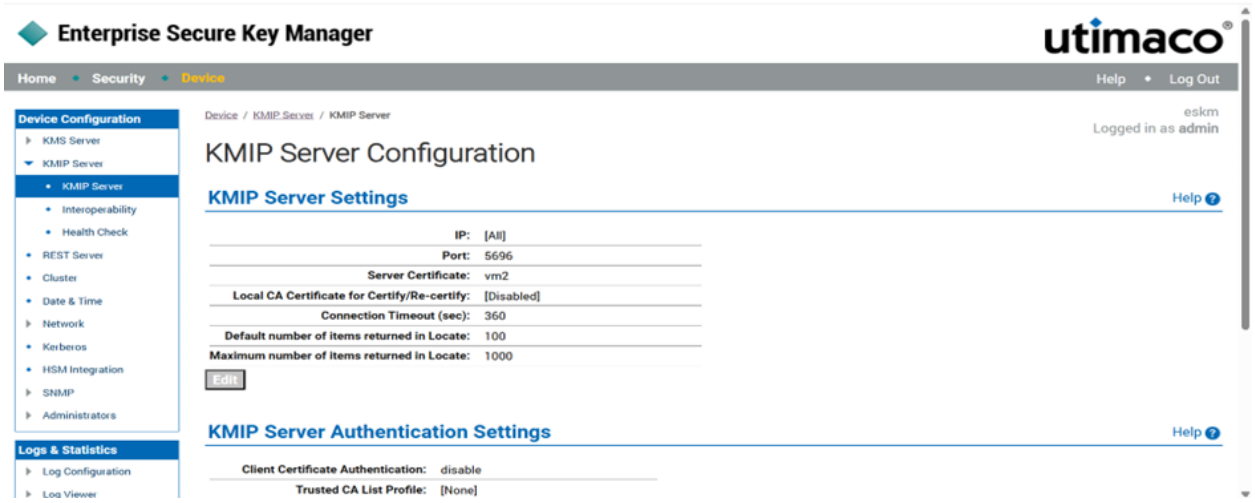

Figure 13 : KMIP Server Configuration

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 Utimaco ESKM as a Key Management Service (KMS)

To enable this integration, follow the steps outlined below within the Veeam User Interface (UI):

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

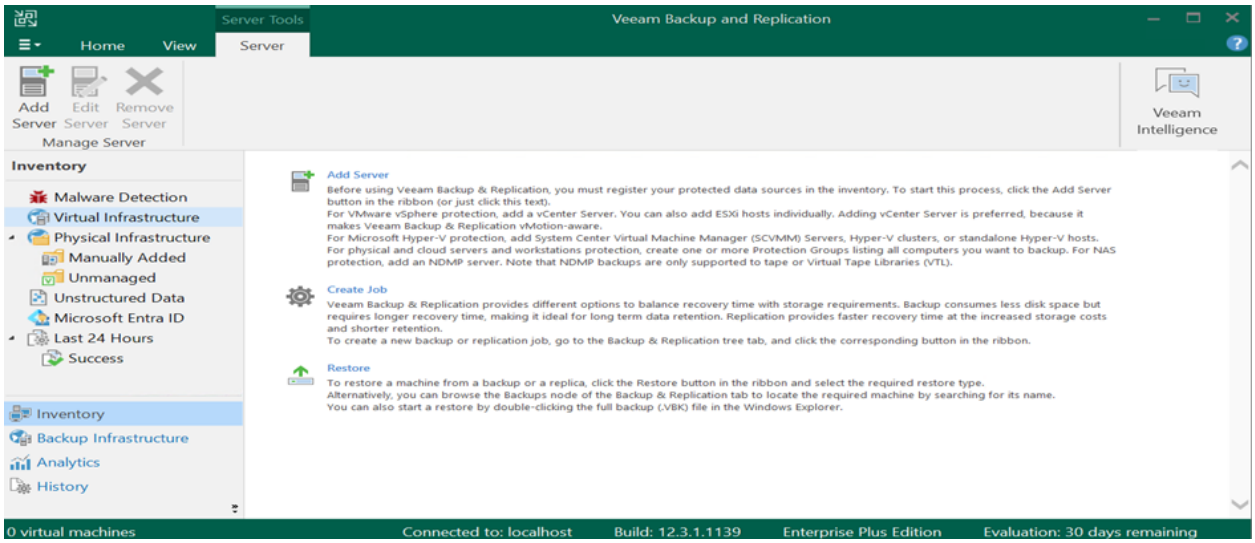

Figure 14 : Veeam Backup & Replication Home Page

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

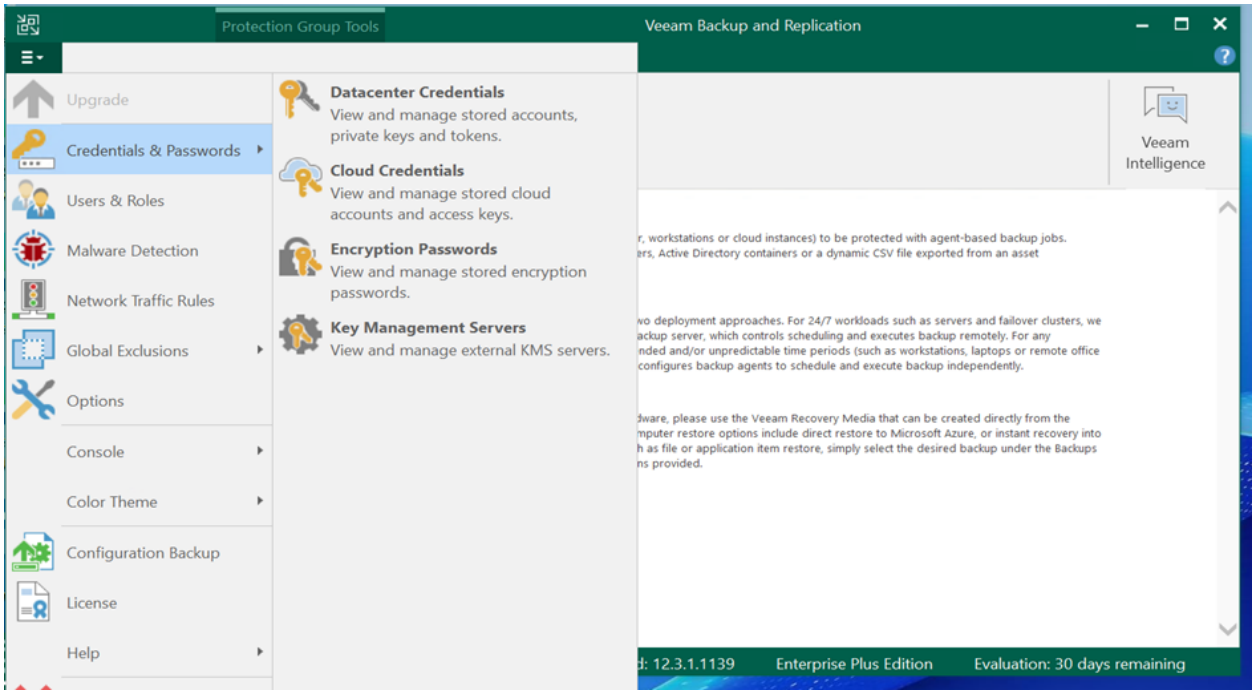

Figure 15 : Credentials and Passwords Page

3. Click **Add,** and it will prompt for the server URL, server certificate, and client certificate.

Ensure that the default port number is set to 5696, taken care of during the installation phase.

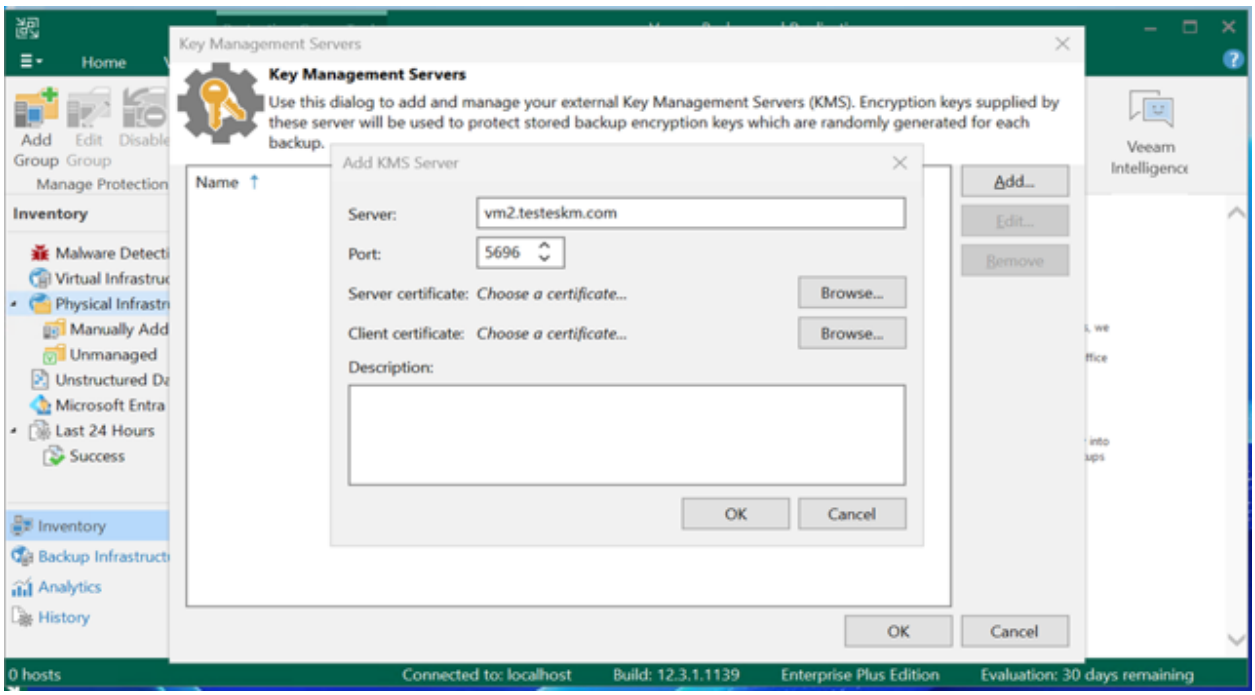

Figure 16 : Server Name Added

4. Upload the client and server certificates generated in Sections 4.3 and 4.4.

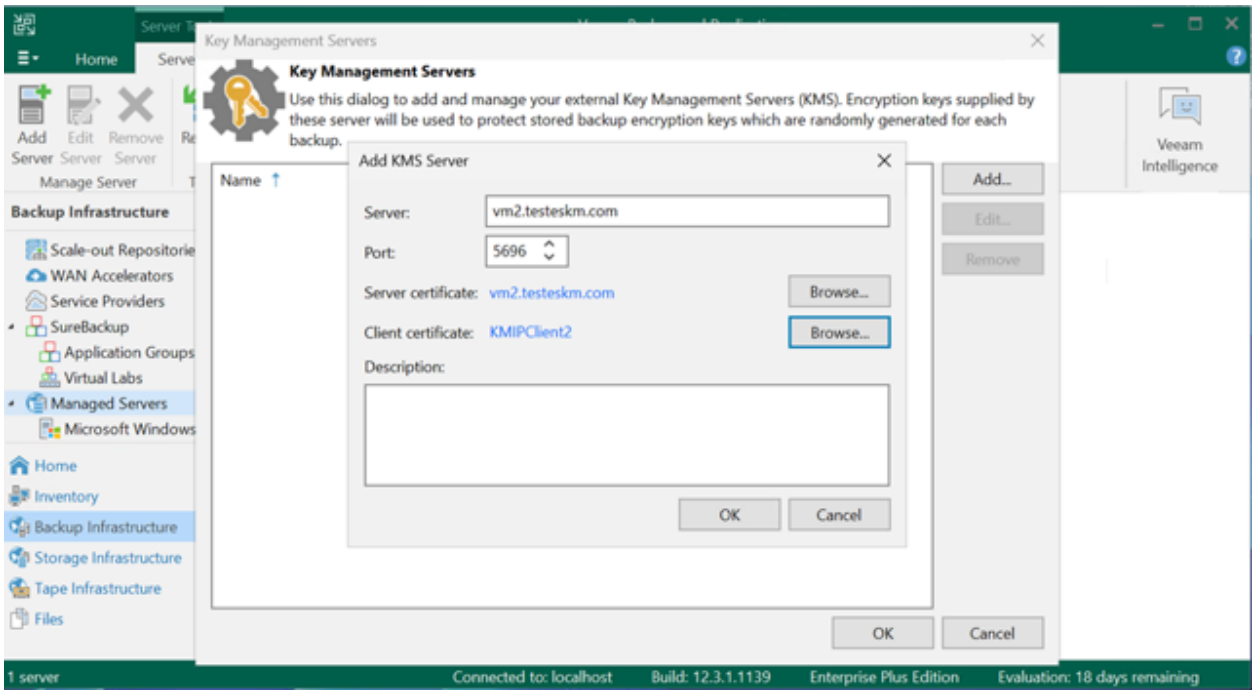

Figure 17 : Server and Client Certificates Added

5. After you have provided the required information, click **OK**.

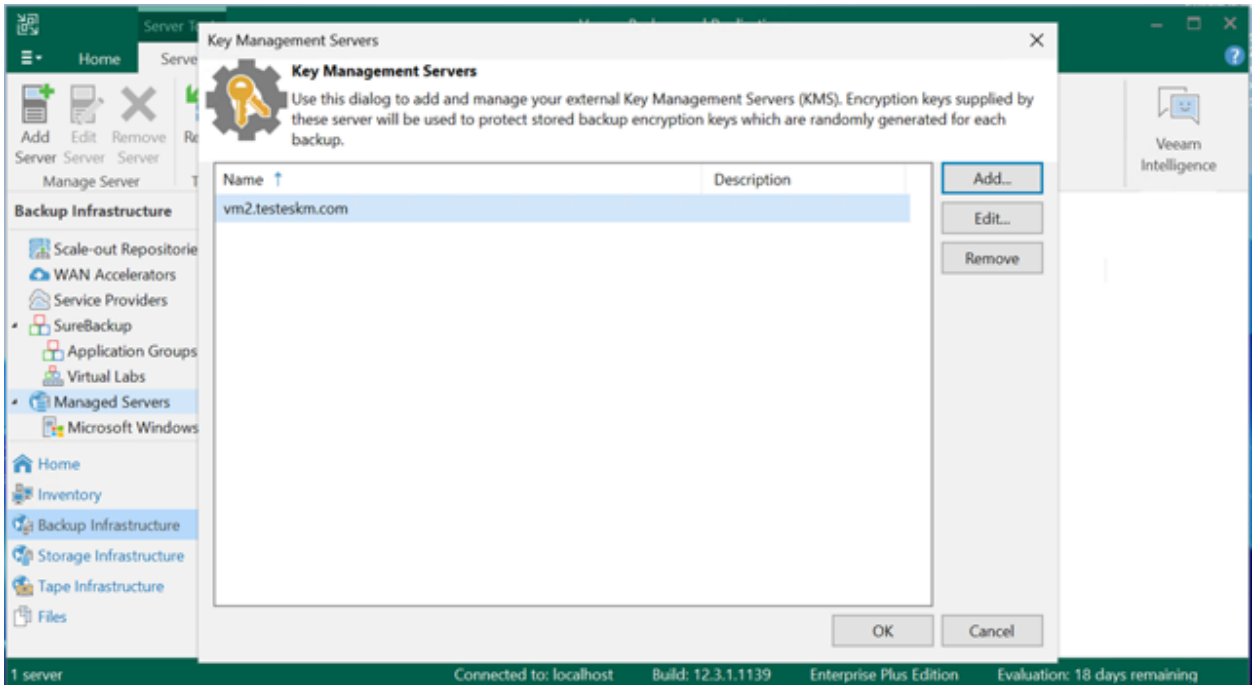

Figure 18 : Summary

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.

To learn the steps on how to create a protection group, refer to the *Create Protection Group* documentation.

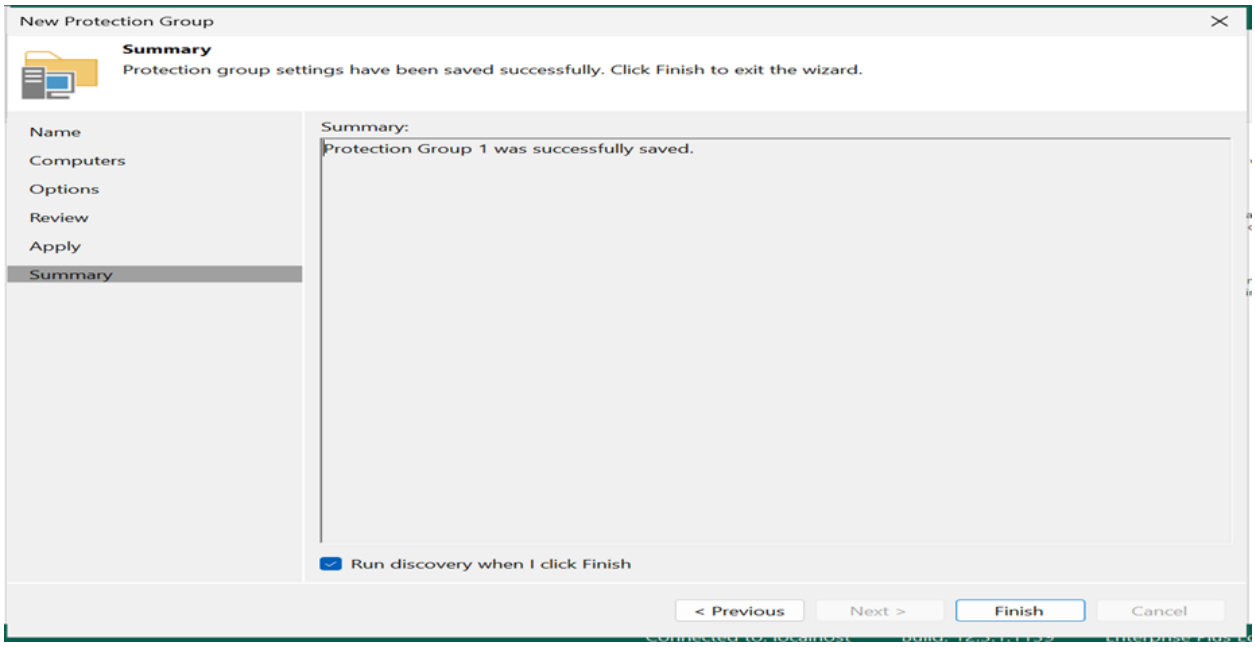

Figure 19 : Created Protection Group

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 you to group 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 Utimaco 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 virtual machines (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**.

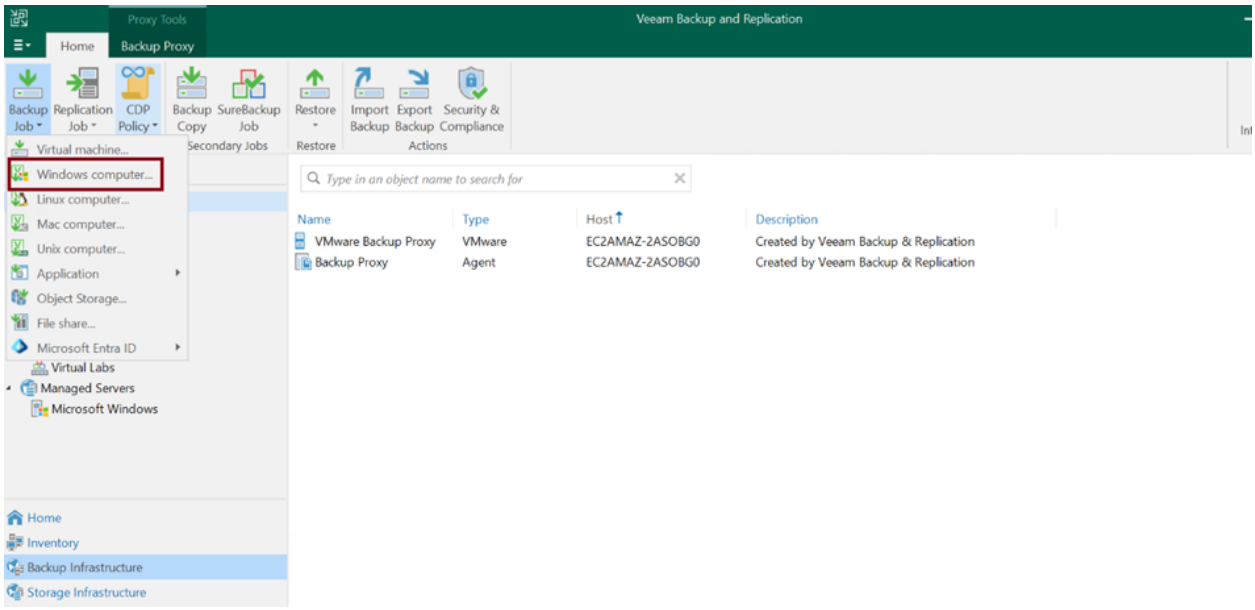

Figure 20 : Backup Job Option is Windows Computer

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**.

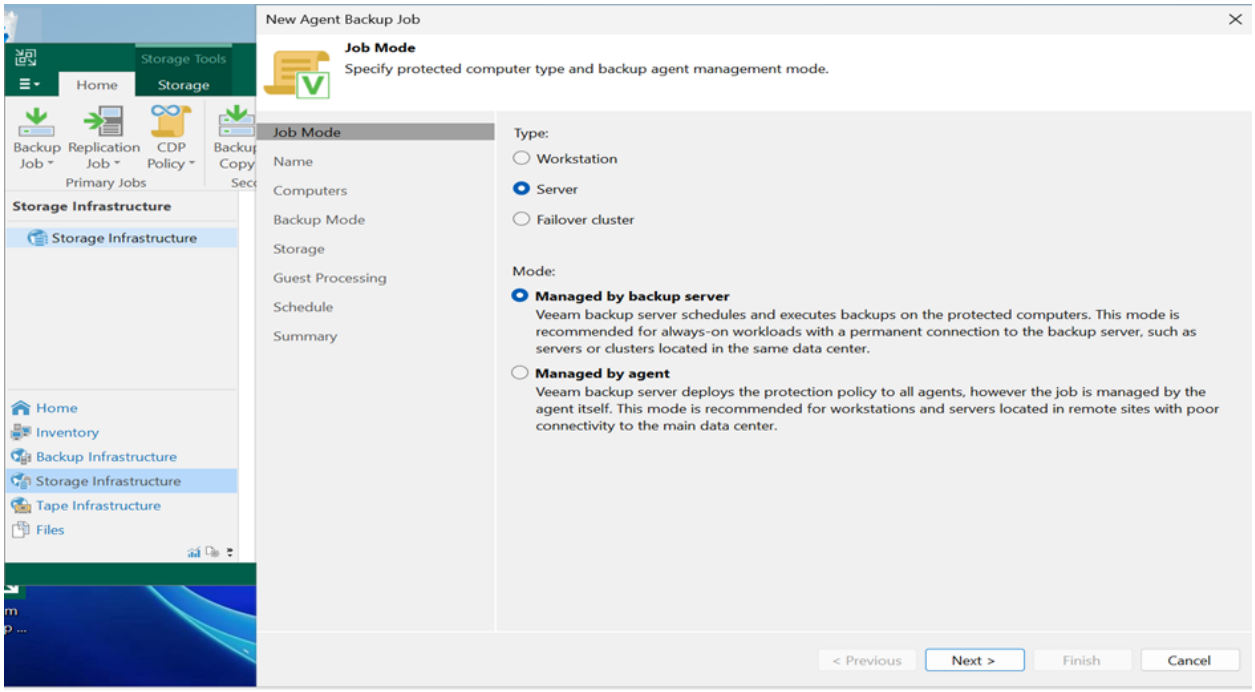

Figure 21 : Choose the Type and Mode

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

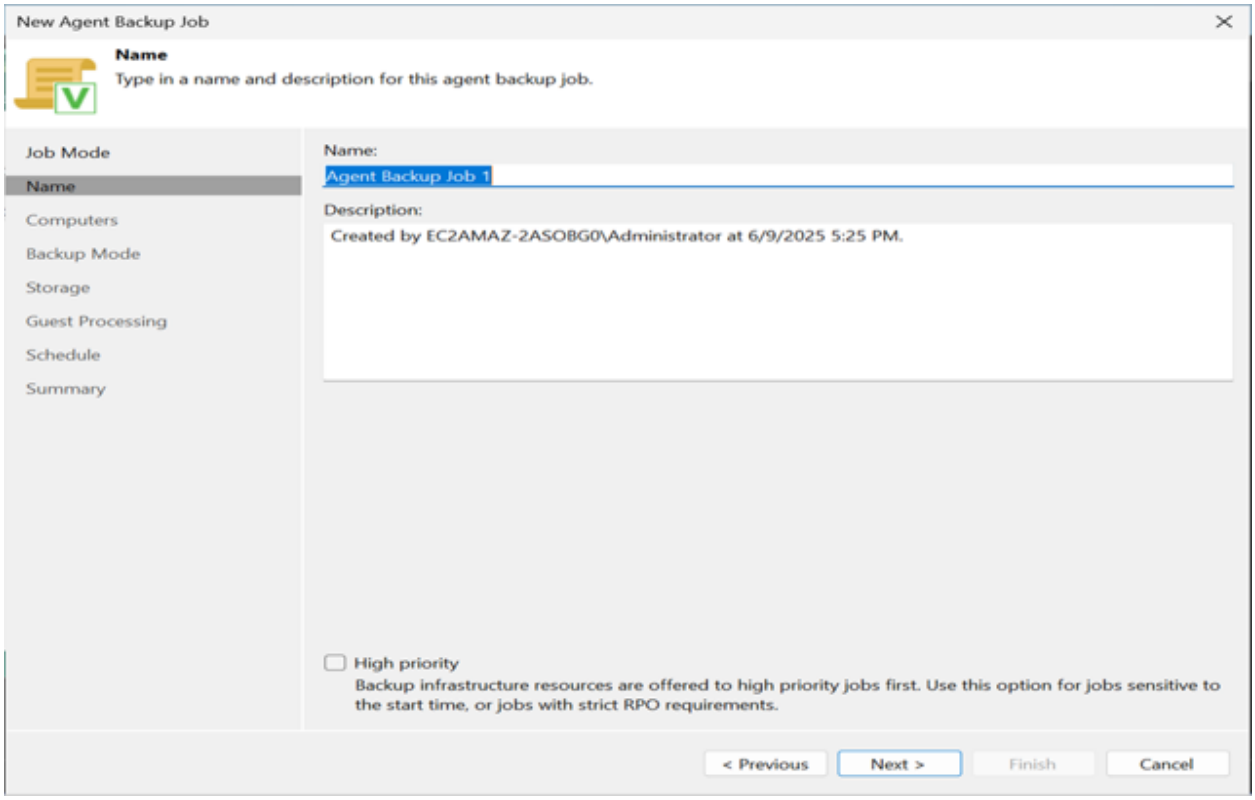

Figure 22 : Add Details

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**.

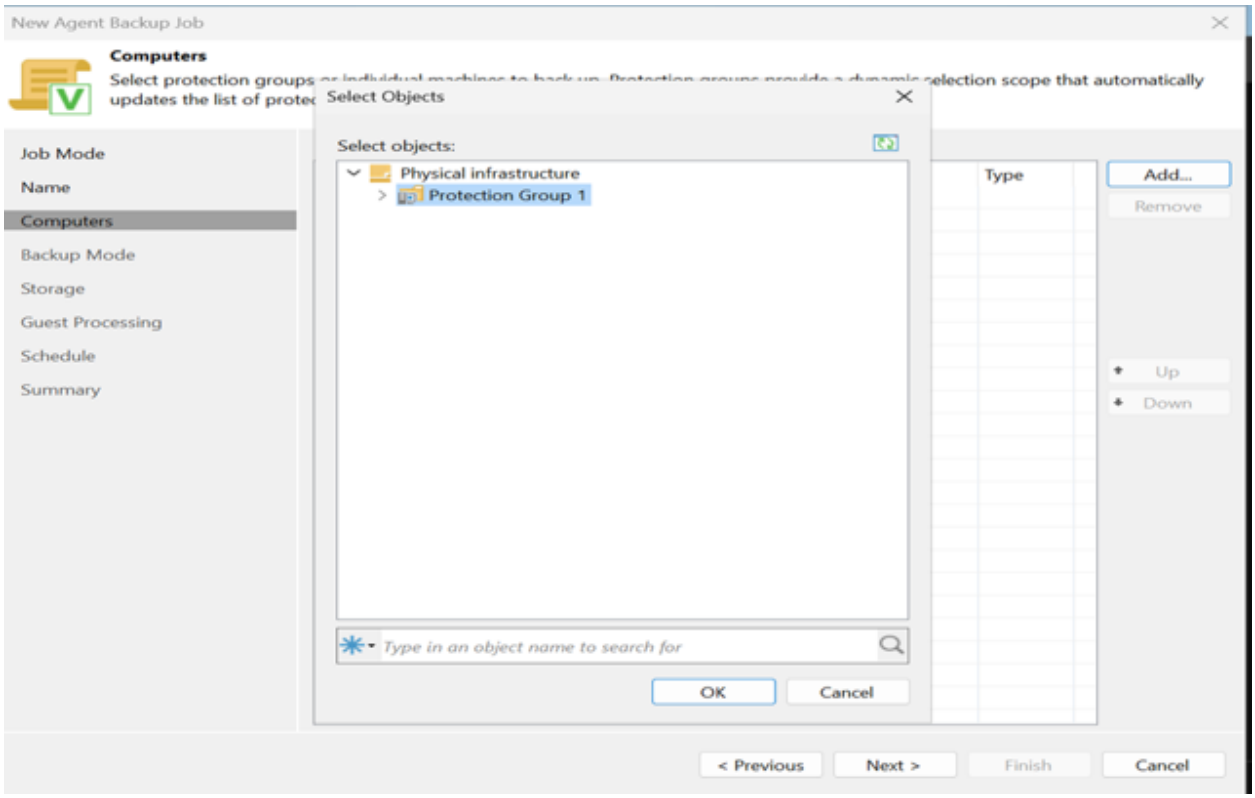

Figure 23 : Choose the Protection Group

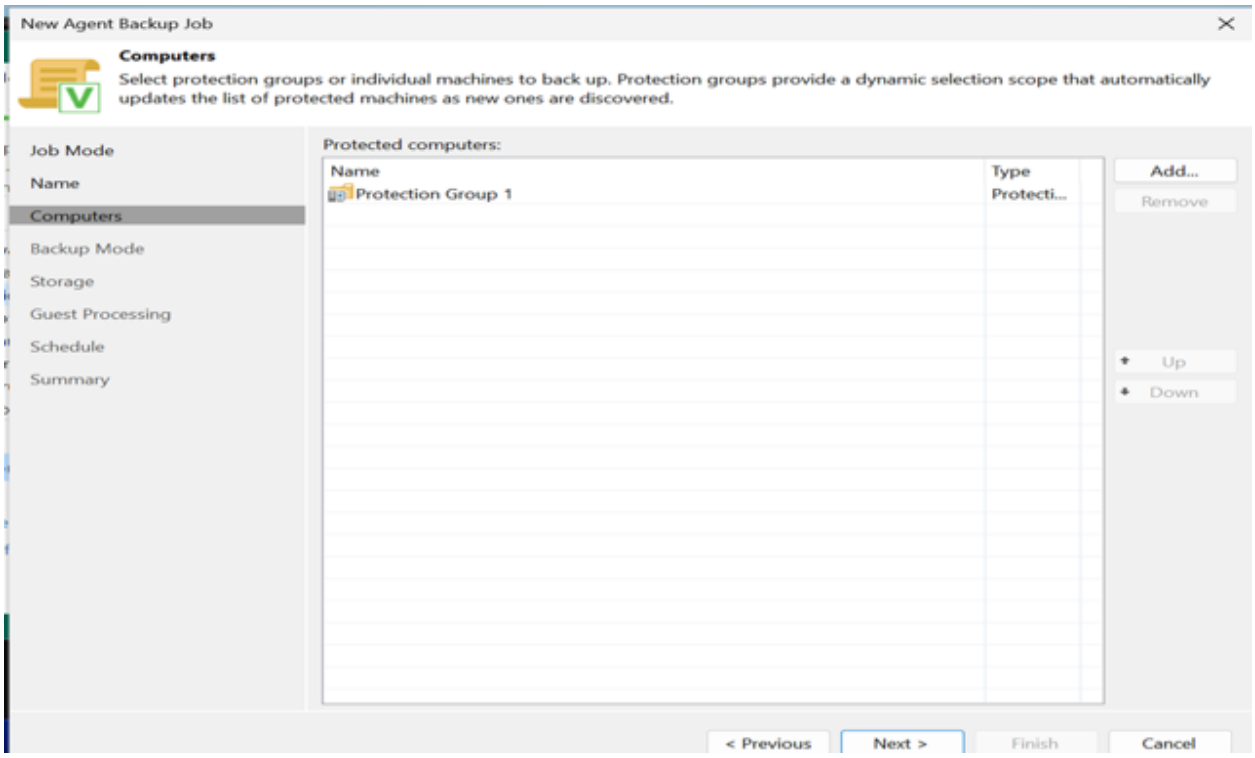

Figure 24 : Protection Group Added

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

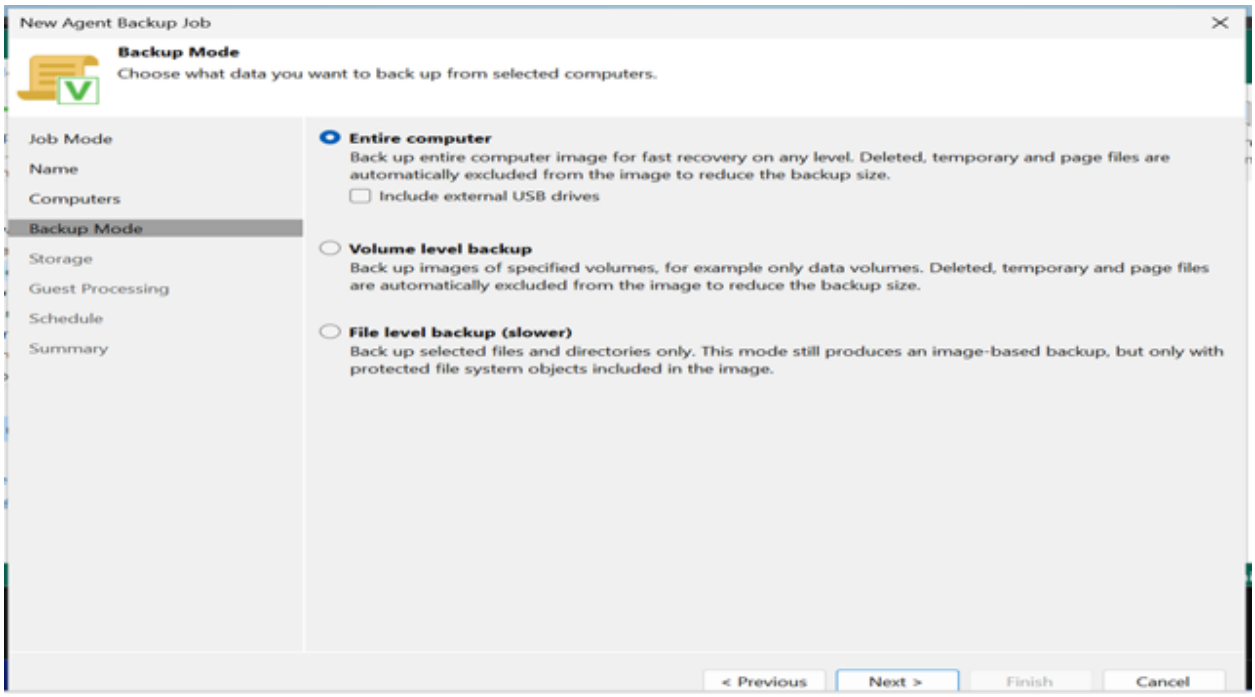

Figure 25 : Select Backup Mode

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

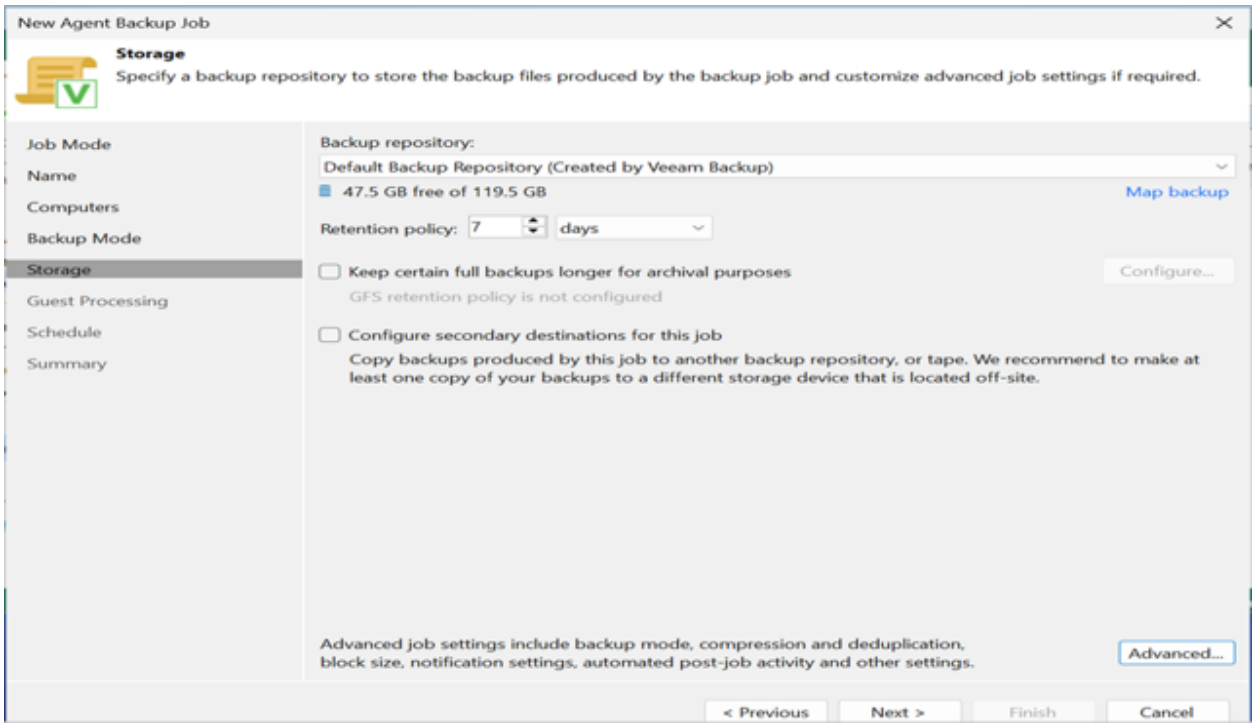

Figure 26 : Configure Storage

7. Click **OK** to proceed.

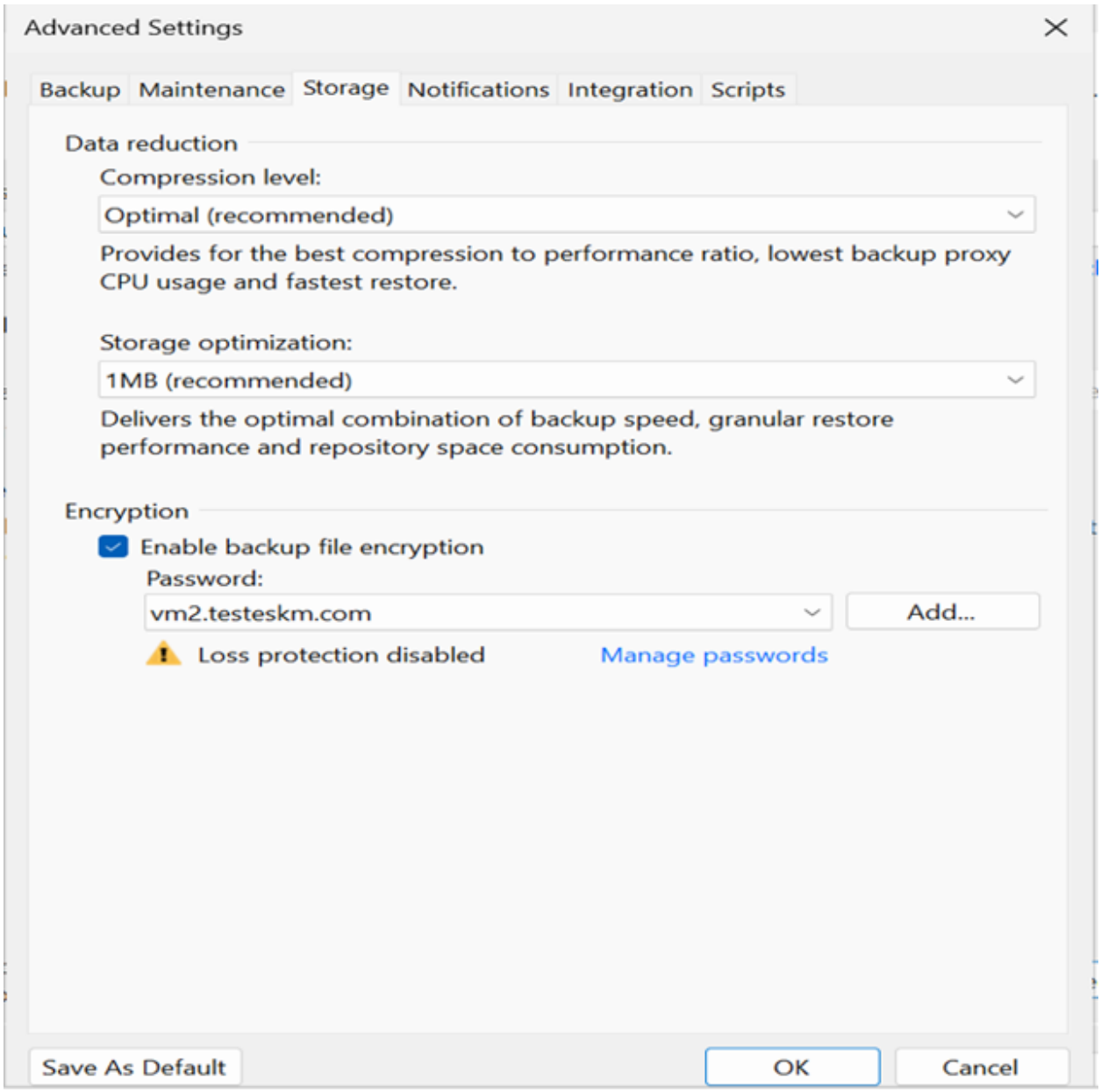

Figure 27 : Storage Configured

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

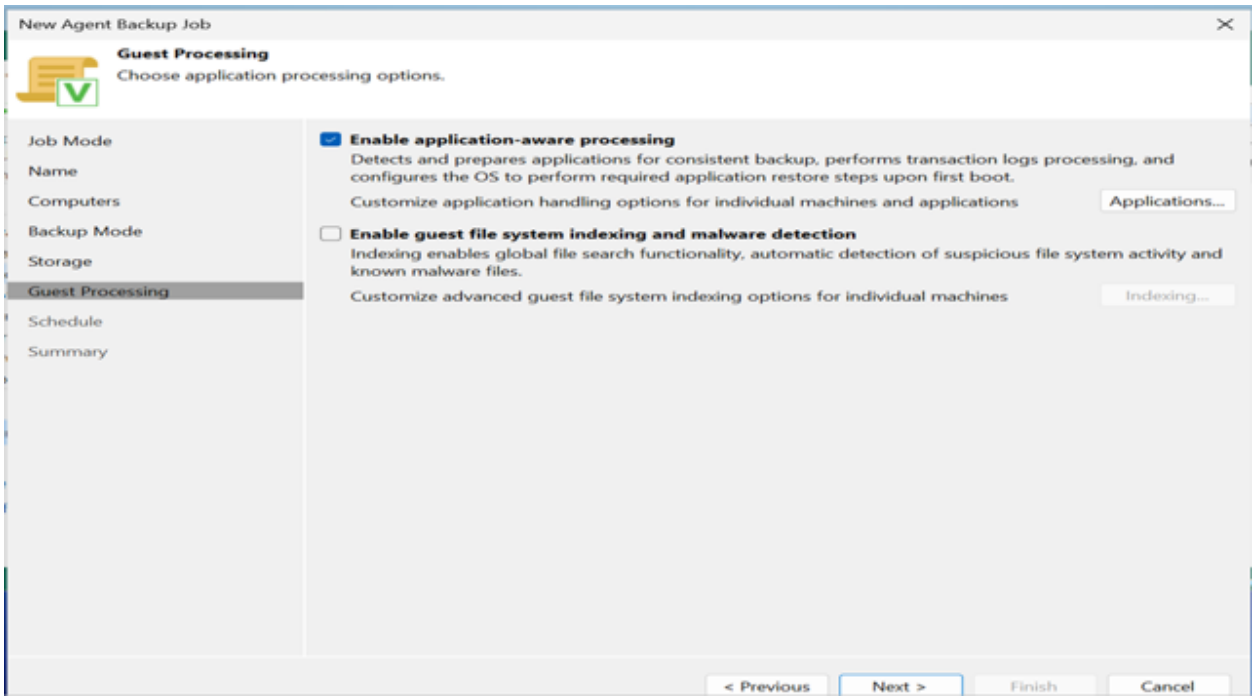

Figure 28 : Configure Guest Processing

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

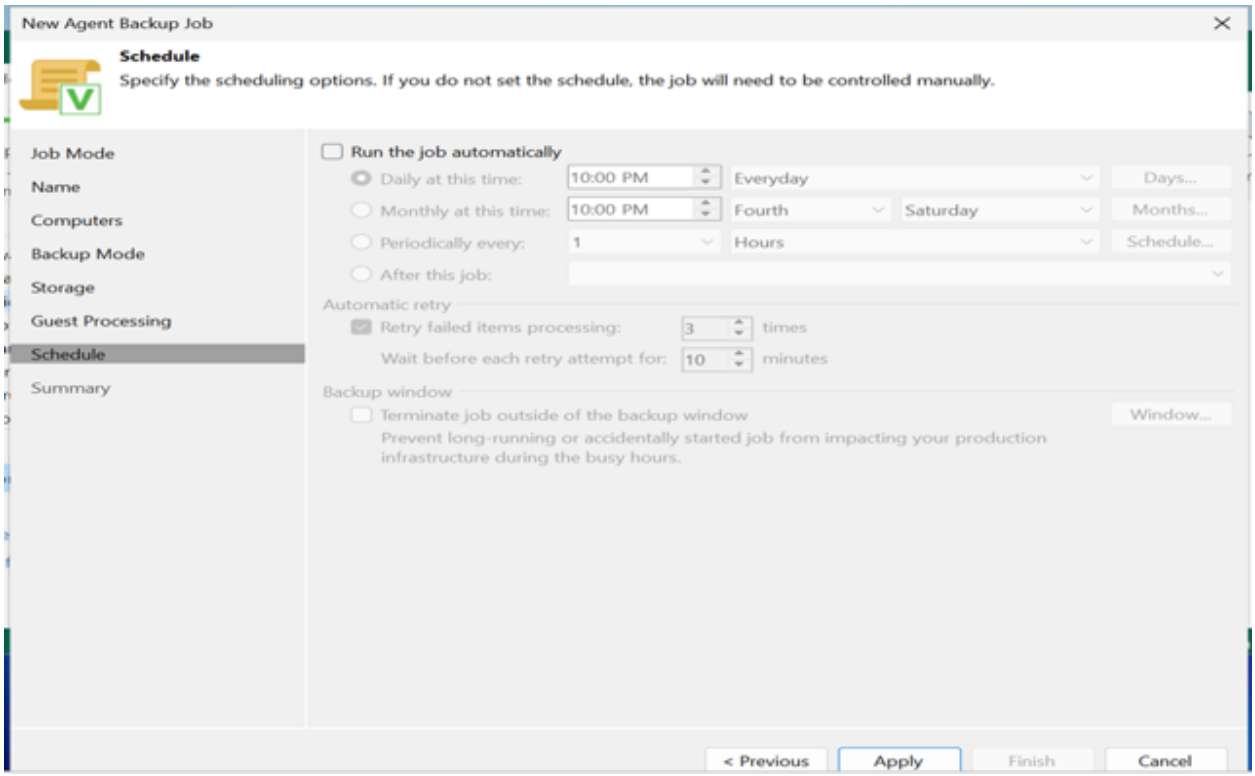

Figure 29 : Schedule

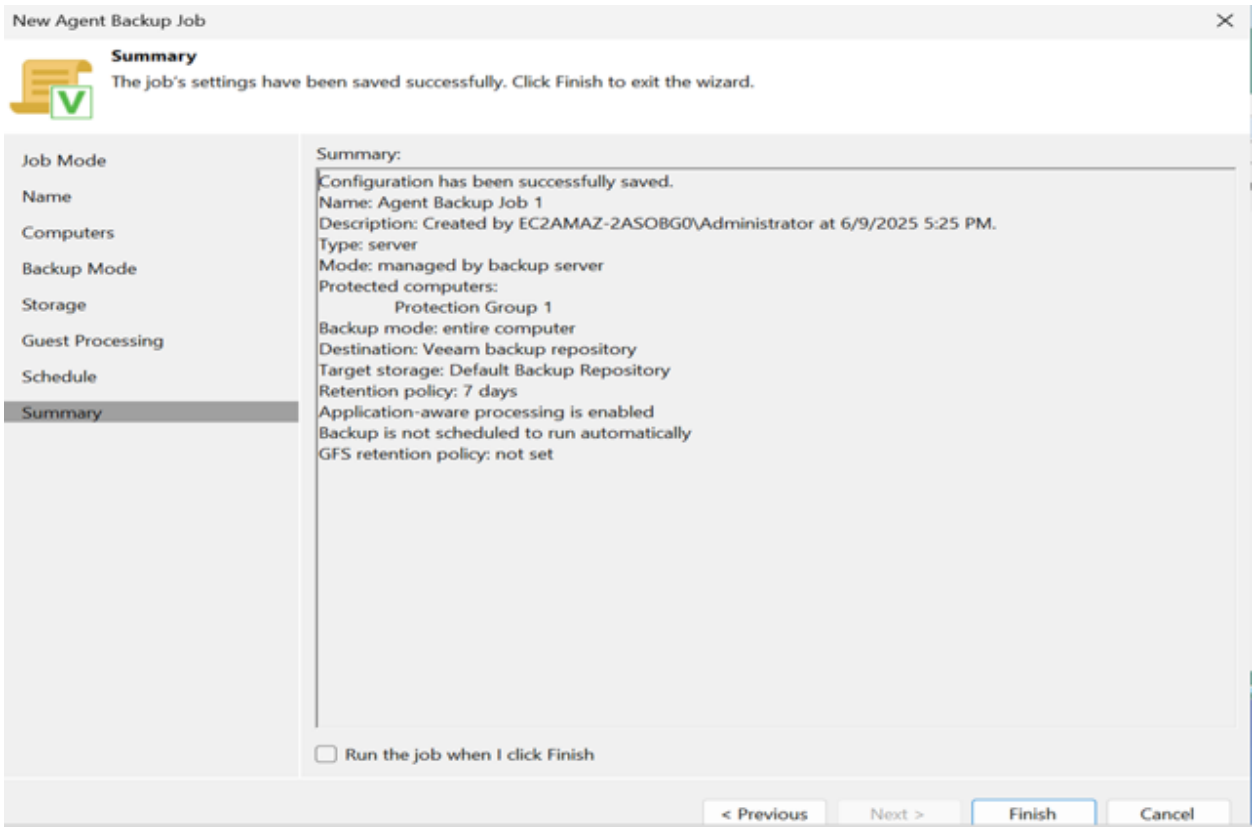

Figure 30 : Summary

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.

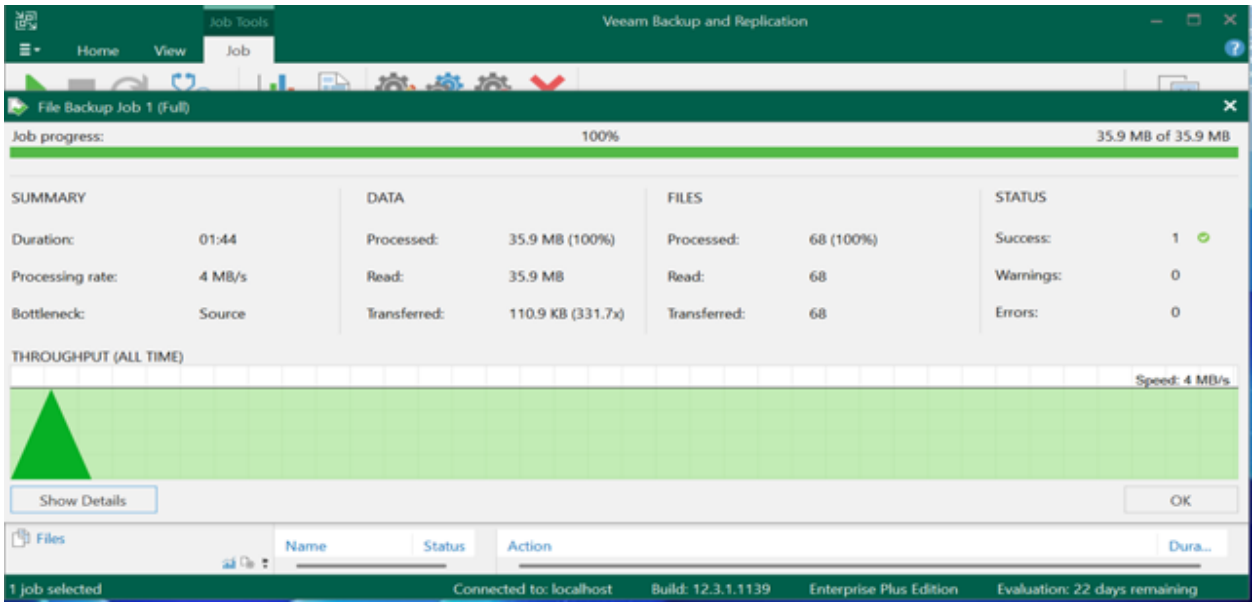

Figure 31 : Graphical Representation of Veeam Backup Job

6.1.2 Unstructured Data Backup to Tape

With Veeam Backup & Replication, we can easily back up to tape and restore unstructured data from various sources. You can protect the following types of data:

- 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.

The user must add to the backup infrastructure the sources of unstructured data that you plan to protect with the file-to-tape and object-to-tape jobs.

Here, we are adding 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**.

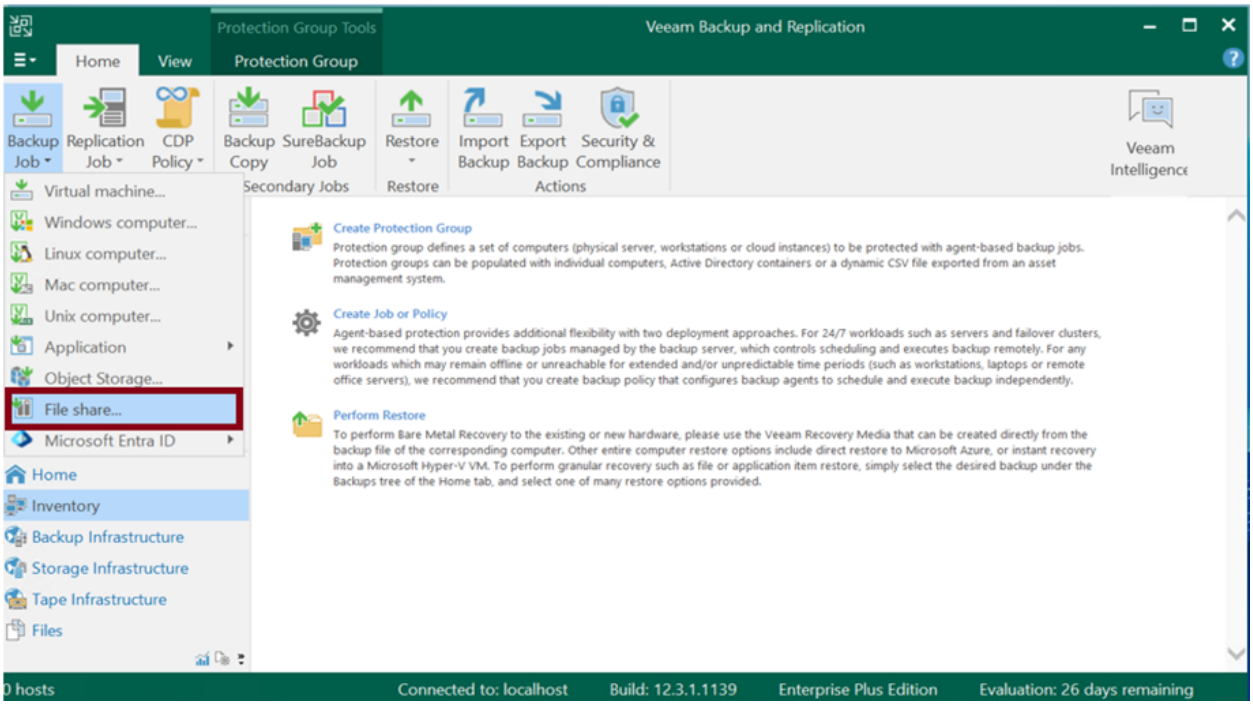

Figure 32 : Click on File Share

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

We can choose File Server, File Share, or NAS Filer as the unstructured data source. The remaining steps are similar.

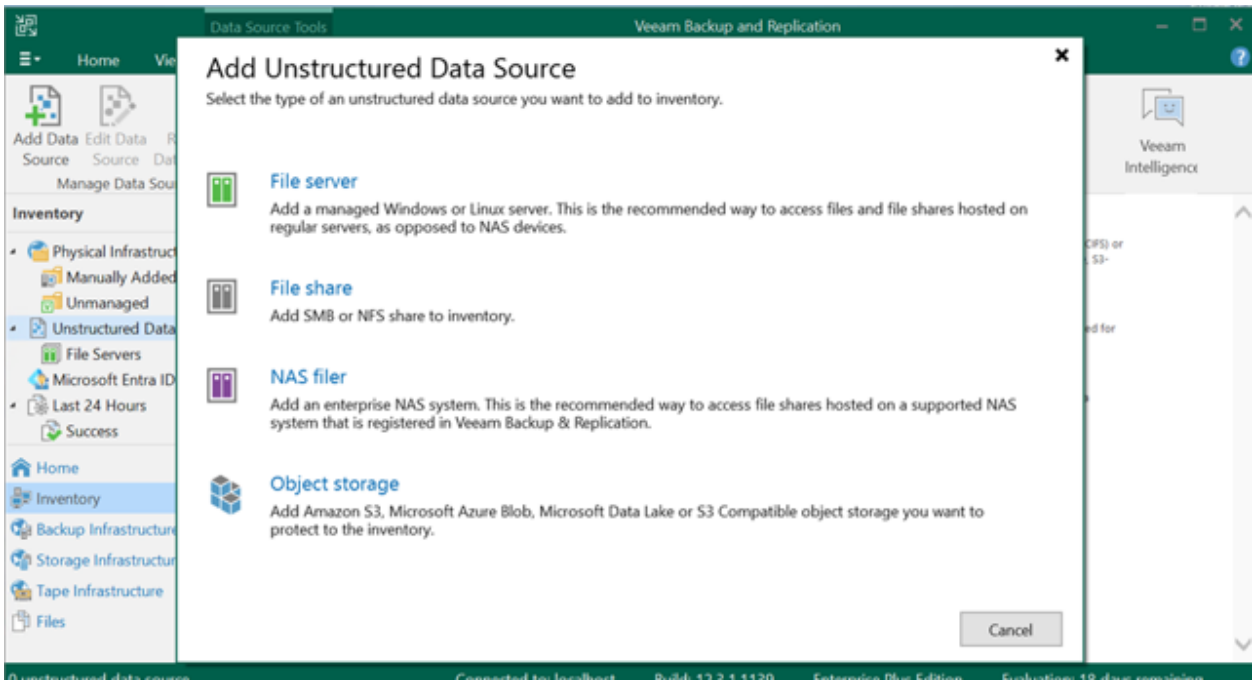

Figure 33 : Unstructured Data Source Added

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

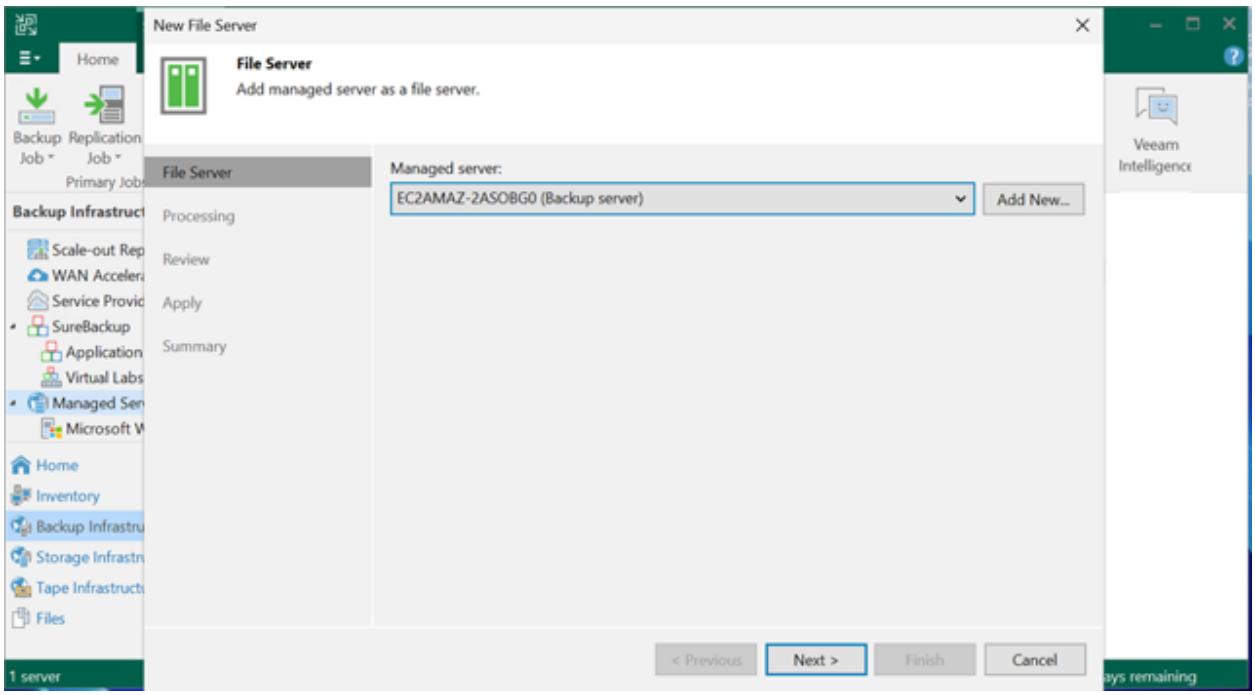

Figure 34 : Add a Managed Server as a File Server

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

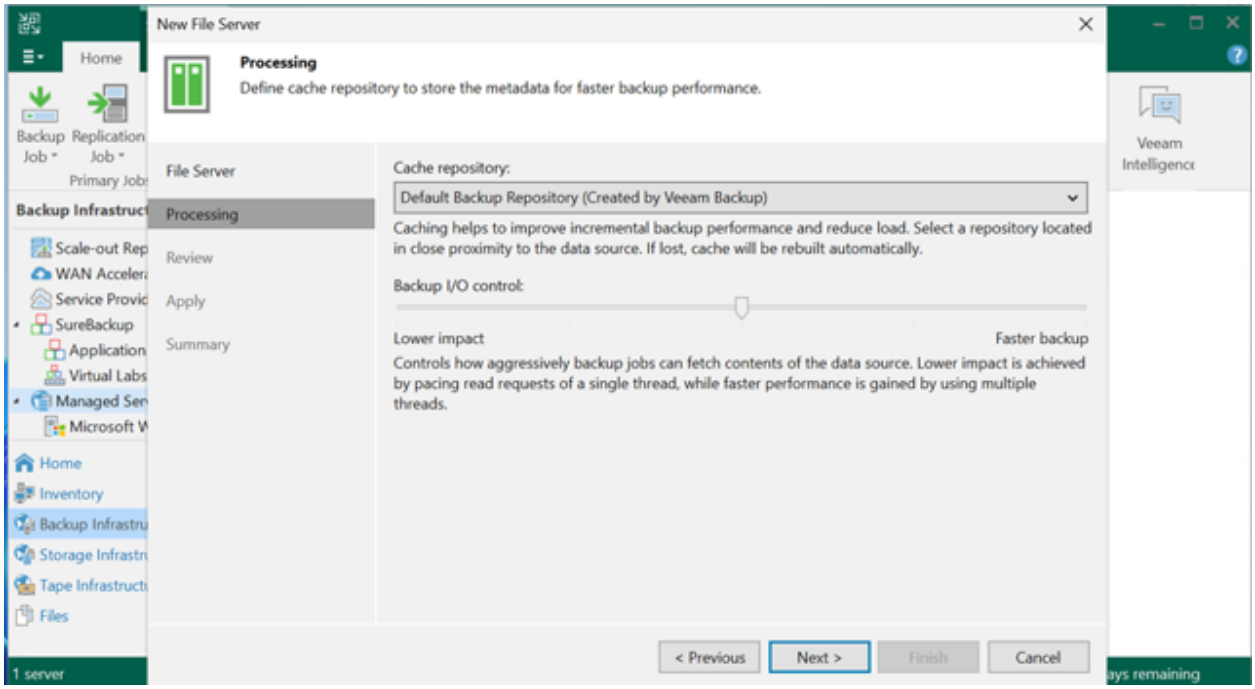

Figure 35 : Cache Repository

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

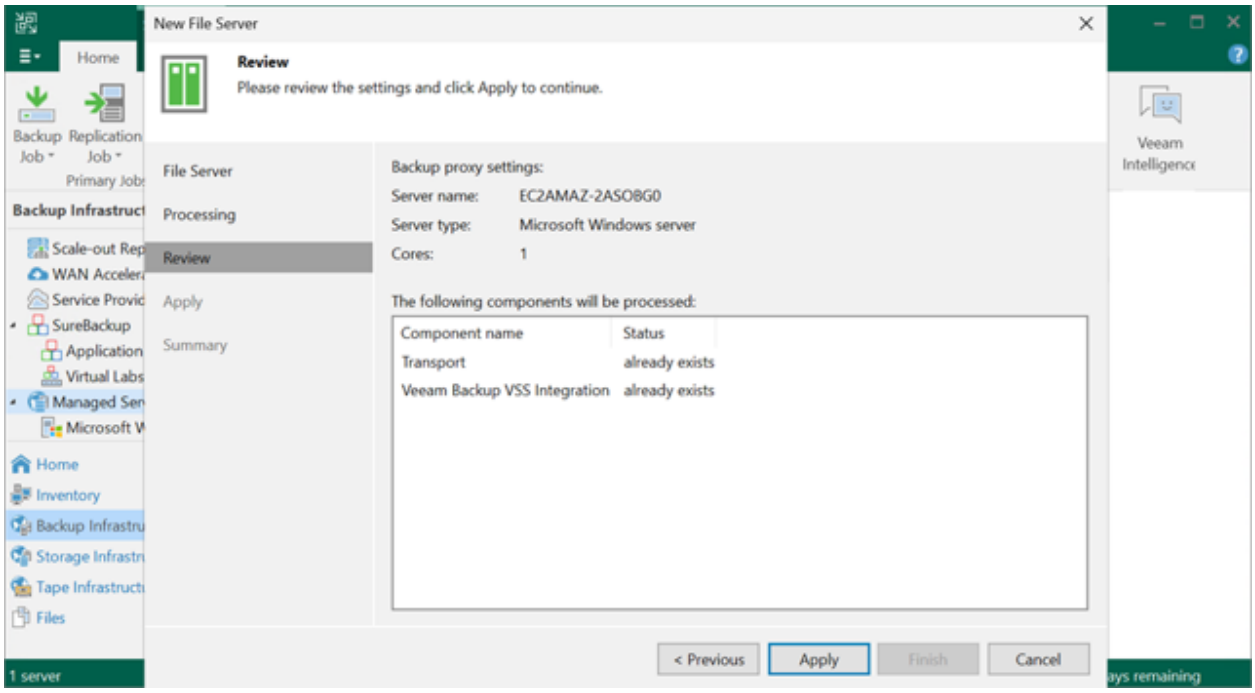

Figure 36 : Review Page

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

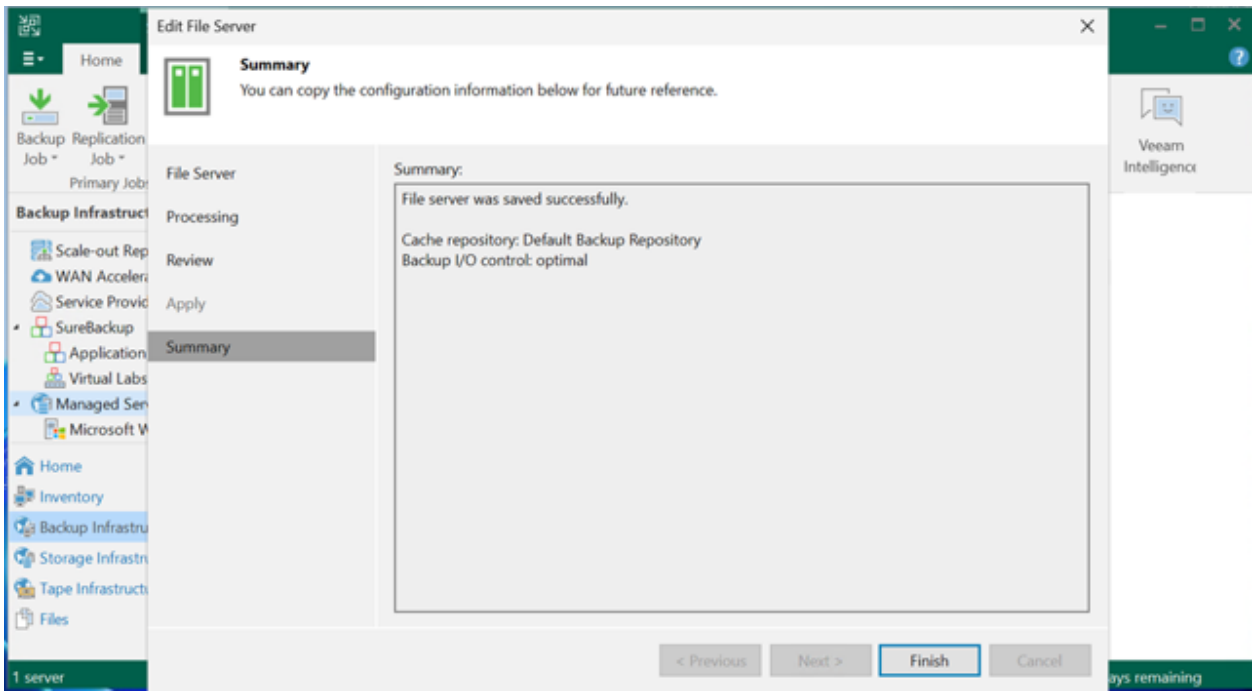

Figure 37 : Summary

8. Enter the name and description of the backup job and click **Next.**

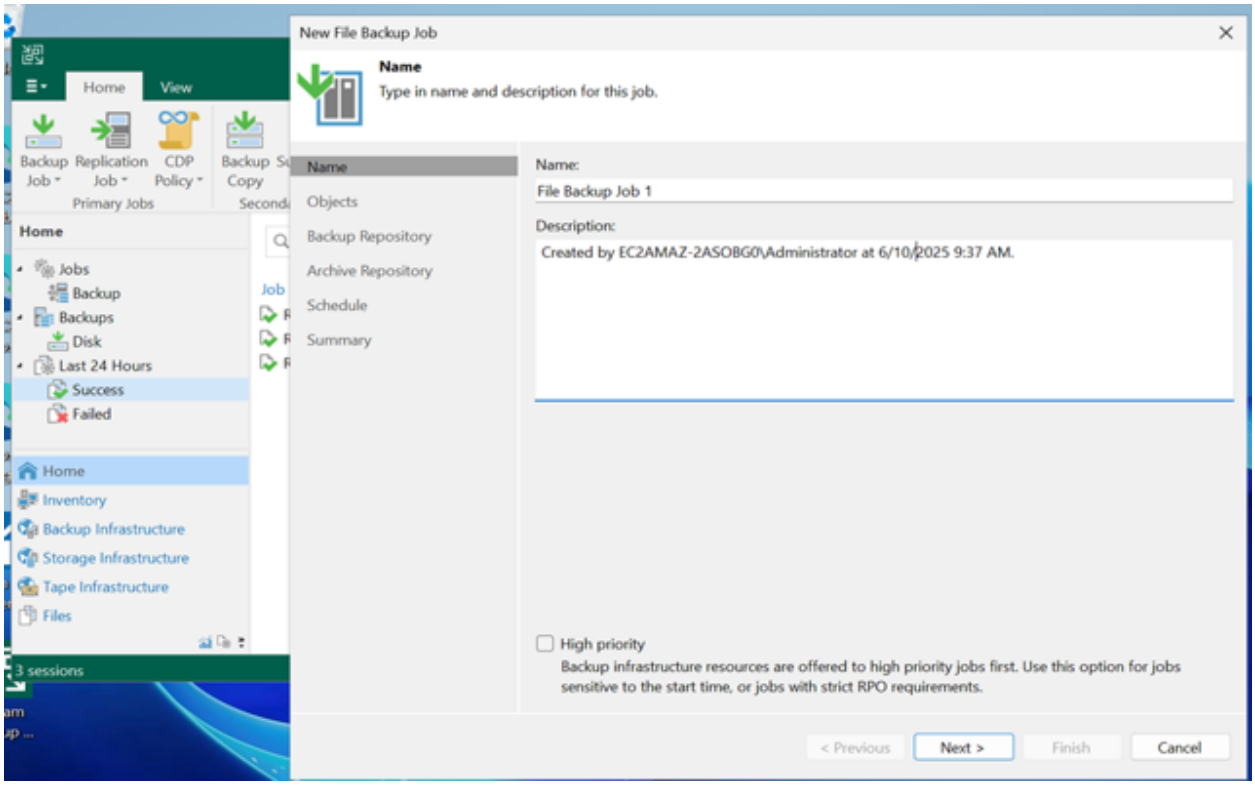

Figure 38 : Enter the Name for the Backup Job

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

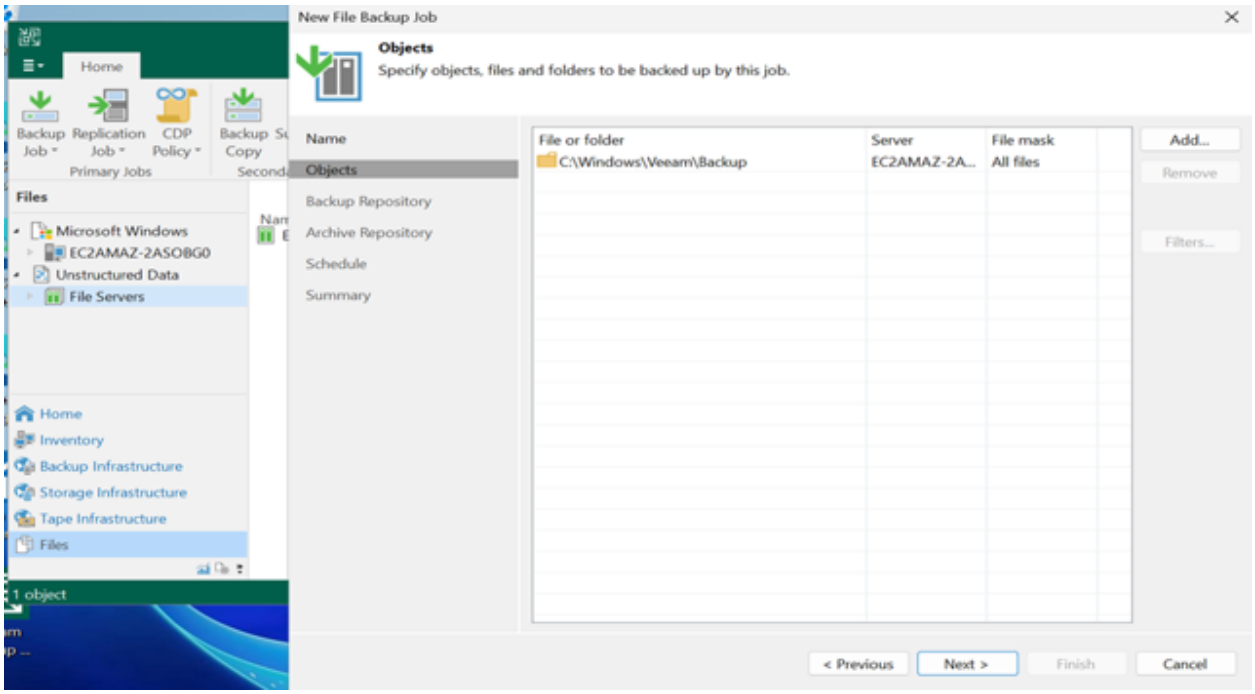

Figure 39 : Add Object

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

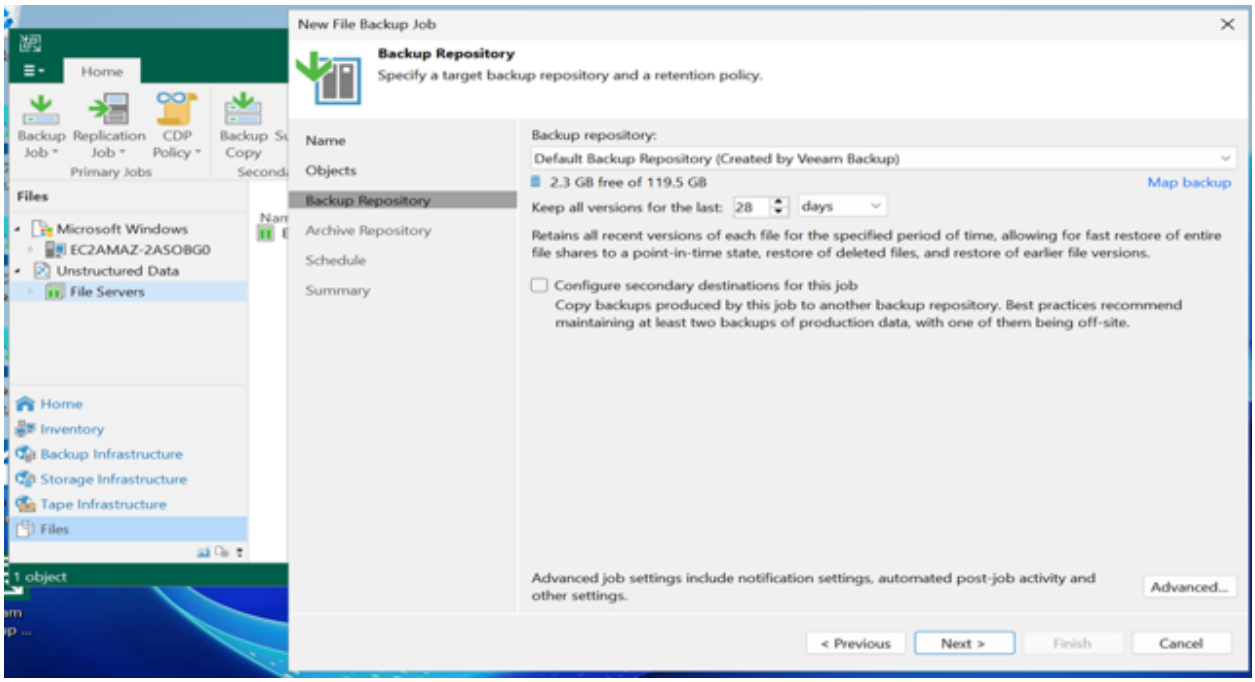

Figure 40 : Backup Repository

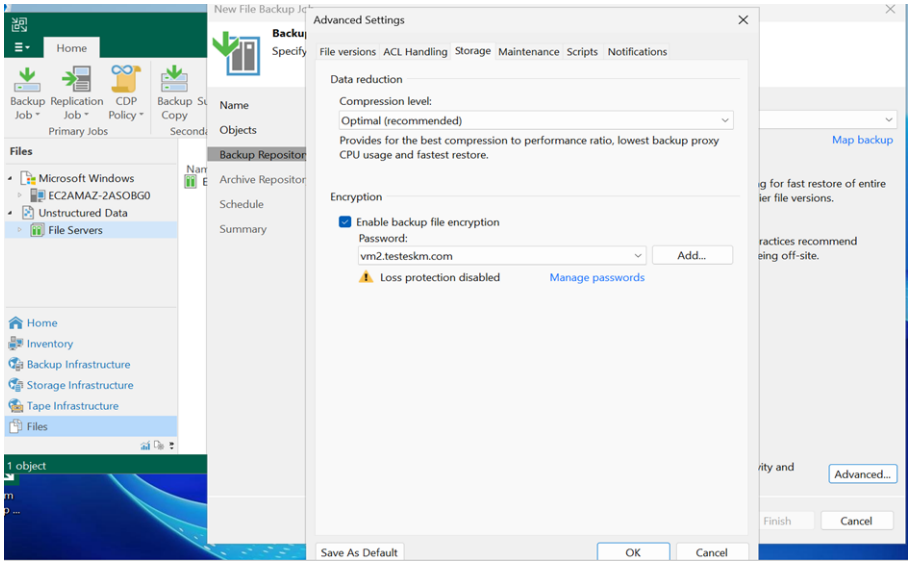

Figure 41 : Storage Tab

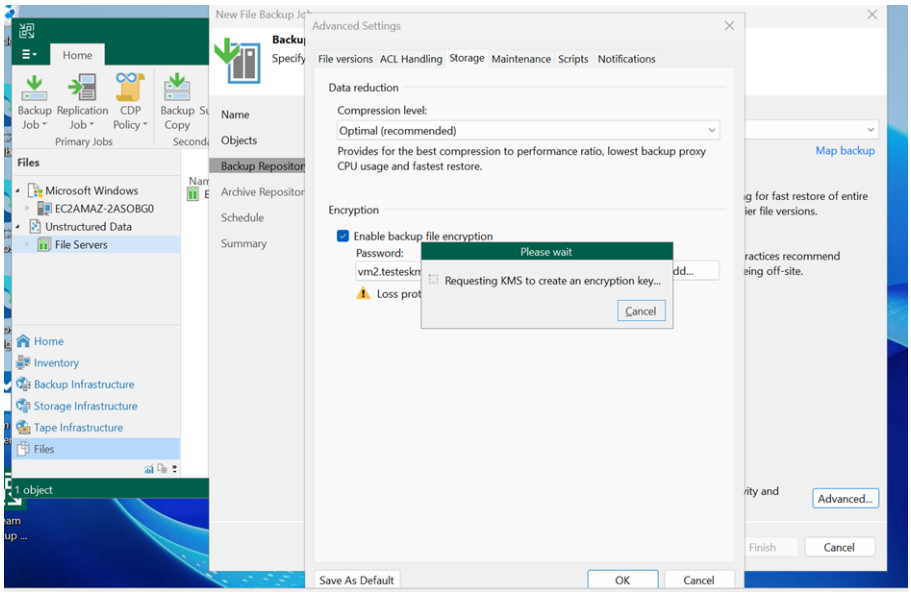

Figure 42 : Requesting KMS to Create an Encryption Key

11. Keep the **Archive Repository** with the same default configuration. Click **Next** to proceed.

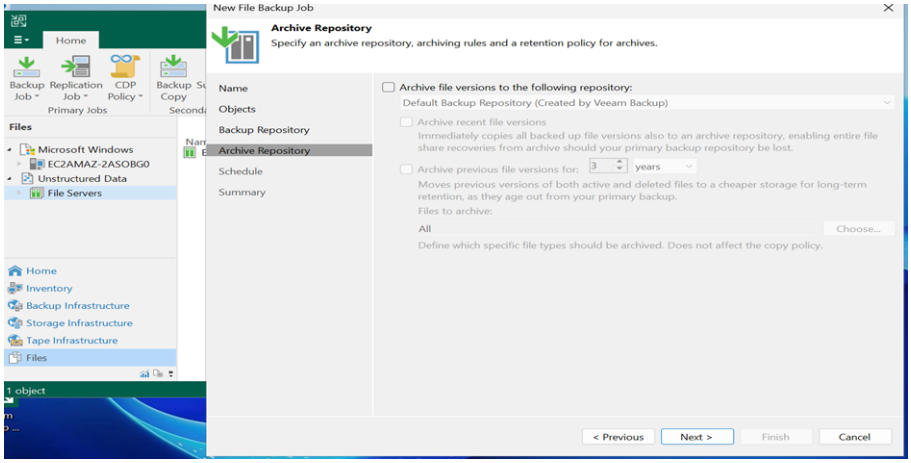

Figure 43 : Archive Repository

12. In the **Schedule** section, select the option that fits your requirements. Click **Apply** to proceed.

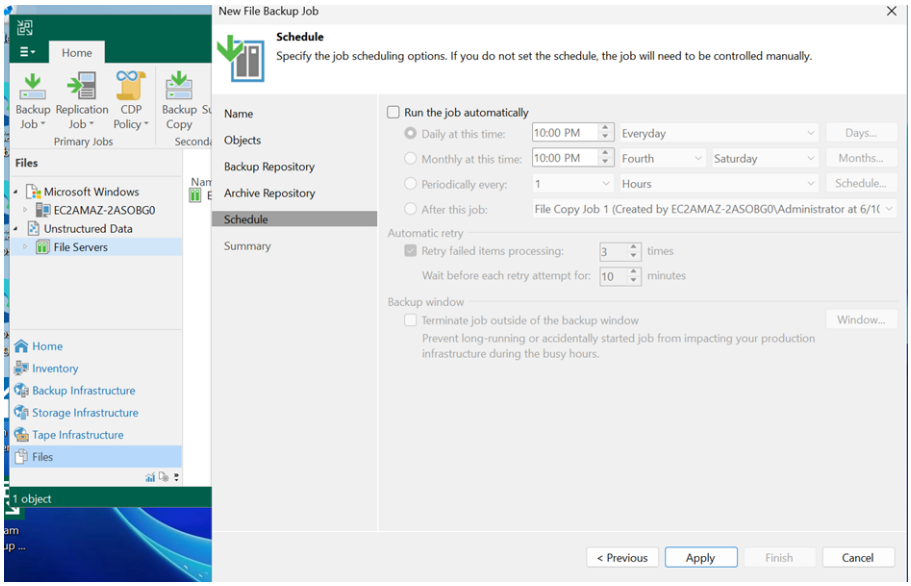

Figure 44 : Schedule Tab

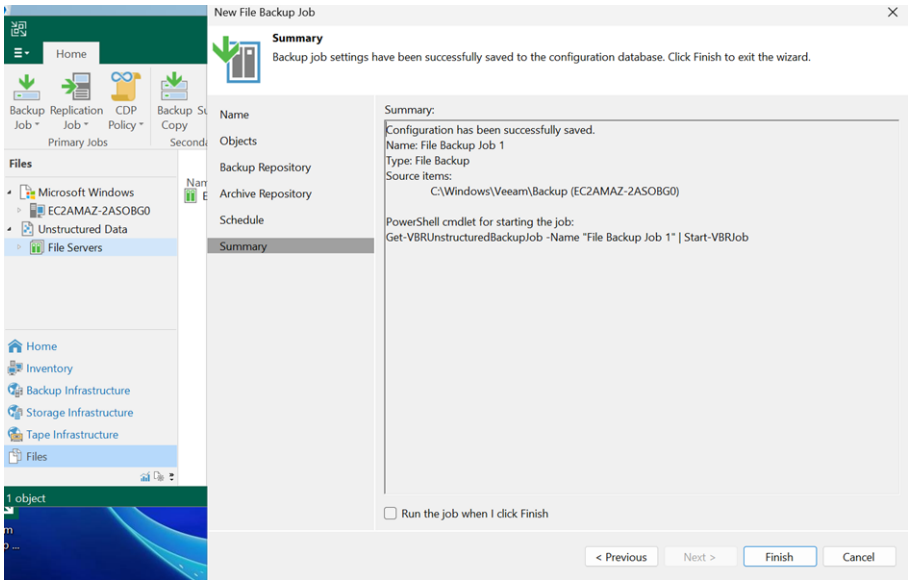

Figure 45 : Summary

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

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 Utimaco ESKM, which is then used to encrypt and decrypt Veeam backup files. We can verify the logs from Utimaco ESKM by following the steps below:

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

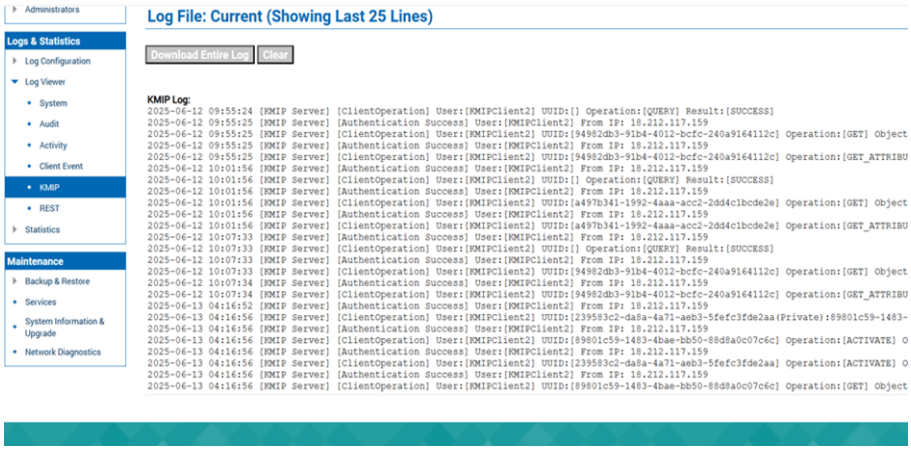

Figure 46 : Log Details

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.

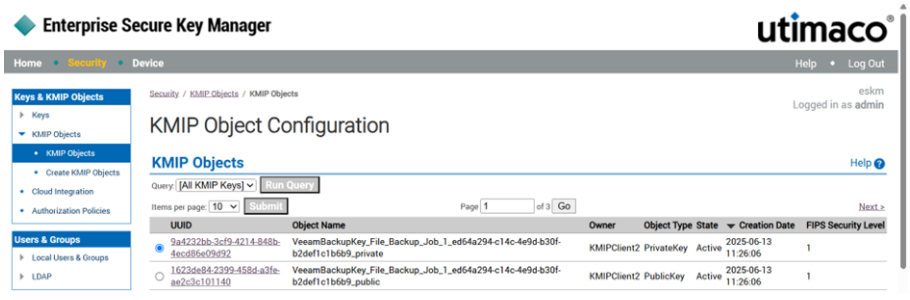

Figure 47 : KMIP Objects

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.

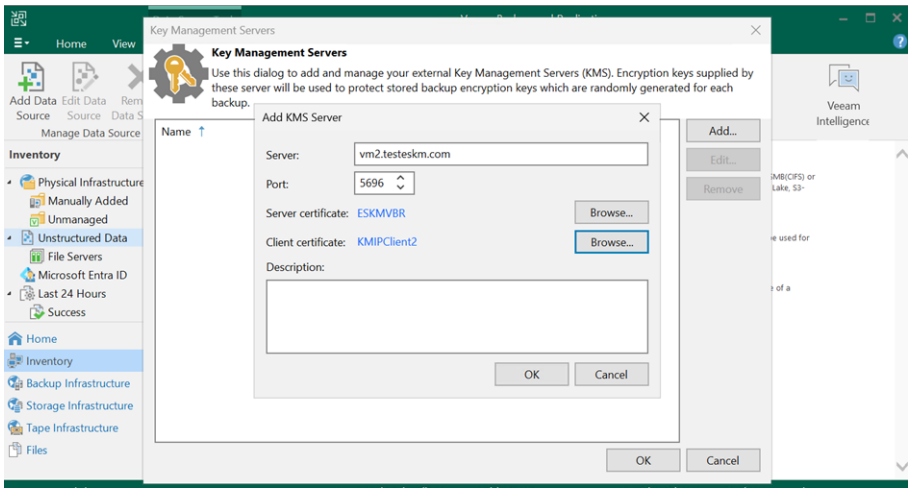

Figure 48 : Add KMS Server Page

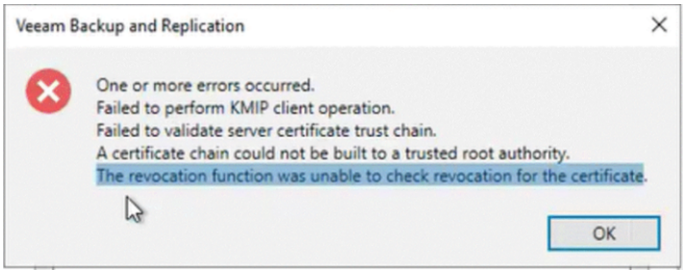

Figure 49 : Error Page

7.2 Log locations and interpretation

We can verify the logs from Utimaco ESKM by following the steps below:

1. In the ESKM Management Console, click the **Device** tab.
2. Click on **Log Viewer** under Logs & Statistics.
3. Click on **KMIP** under Log Viewer.

4. Review logs related to the encryption and decryption operations performed on Veeam backup jobs.

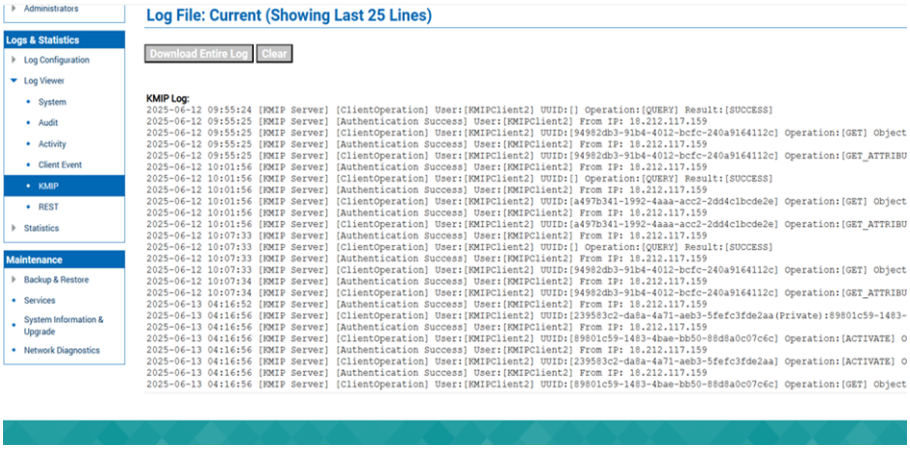

Figure 50 : KMIP Log

7.3 Contact for support

7.3.1 Utimaco Technical Support

For technical questions, contact Utimaco Technical Support:

- E-mail: support-atalla@utimaco.com
- Telephone: 800-500-7858 (U.S.A.) +1-916-414-0216 (International)
- Website: https://support.utimaco.com/

Before contacting Utimaco with your questions, collect the following information:

- Product model names and numbers.
- Technical support registration number or NonStop system number (if applicable).
- Service Agreement ID number (SAID).
- Product serial numbers.
- Error messages.
- Software version number.

7.3.2 24-hour Support

24-hour emergency support is available to those customers who have valid service contracts. Use this service for product and system emergencies that occur after normal working hours or on weekends and U.S. holidays. Questions about product installation and setup are supported during normal working hours.

For 24-hour emergency support call: 800-500-7858 (U.S.A.) +1-916-414-0216 (International).

8 Appendices

8.1 References

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

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