Acronis

acronis.com

Acronis Cyber Frame Cloud

26.03

Early Access Program Evaluation Guide

User Guide

REVISION: MONDAY, MARCH 30, 2026

Table of contents

Acronis Cyber Frame Cloud

Early Access Program Evaluation Guide

Watch the demo video
A companion demo video is available on YouTube and walks through the key parts of the evaluation journey covered in this guide. https://go.acronis.com/cyber-frame-EAP-demo

Prerequisites for Acronis Cyber Frame Cloud

In the initial release, the Acronis-hosted edition of Cyber Frame (Cloud edition) will be available across 34 data centers worldwide. Some data centers will not have Cyber Frame infrastructure deployed locally; in such cases, workloads will be hosted on clusters located in other data centers.

You can find the list of data centers where Cyber Frame Cloud will be available, along with rollout dates, here. Additional cluster locations for each data center are specified in the “Additional available regions” column.

Overview

Acronis Cyber Frame is a service-provider-ready HCI and IaaS solution integrated into Acronis Cyber Protect Cloud. It lets partners provision virtual machines, networking and storage, then apply backup, disaster recovery, security and RMM from the same management plane.

The main goal of this EAP is to validate whether Cyber Frame fits the infrastructure services you want to deliver and provides a credible path to onboard, operate and migrate real customer workloads.

What this guide is designed to validate

- Provisioning: From initial access to first working workload.
- Operational clarity across networking, protection and monitoring.
- External access and hybrid connectivity patterns.
- Restore and migration readiness for real customer scenarios.

Cloud and Local in one sentence each

- Cyber Frame Cloud: Acronis-hosted, fast to activate and the recommended starting point for EAP validation.
- Cyber Frame Local: SP-hosted, intended for partners who need infrastructure ownership, location control or stronger long-term margin leverage.

Evaluation journey at a glance

Run the labs in order. Each one builds on the previous one so the evaluation stays practical and reflects how a service provider would actually onboard and validate the platform.

- Lab 1: Build a basic customer environment and apply cyber protection.
- Lab 2: Set up site-to-site VPN connectivity.
- Lab 3: Evaluate migration workflows.
- Local follow on: Assess when to continue with Cyber Frame Local.

Guided hands-on validation

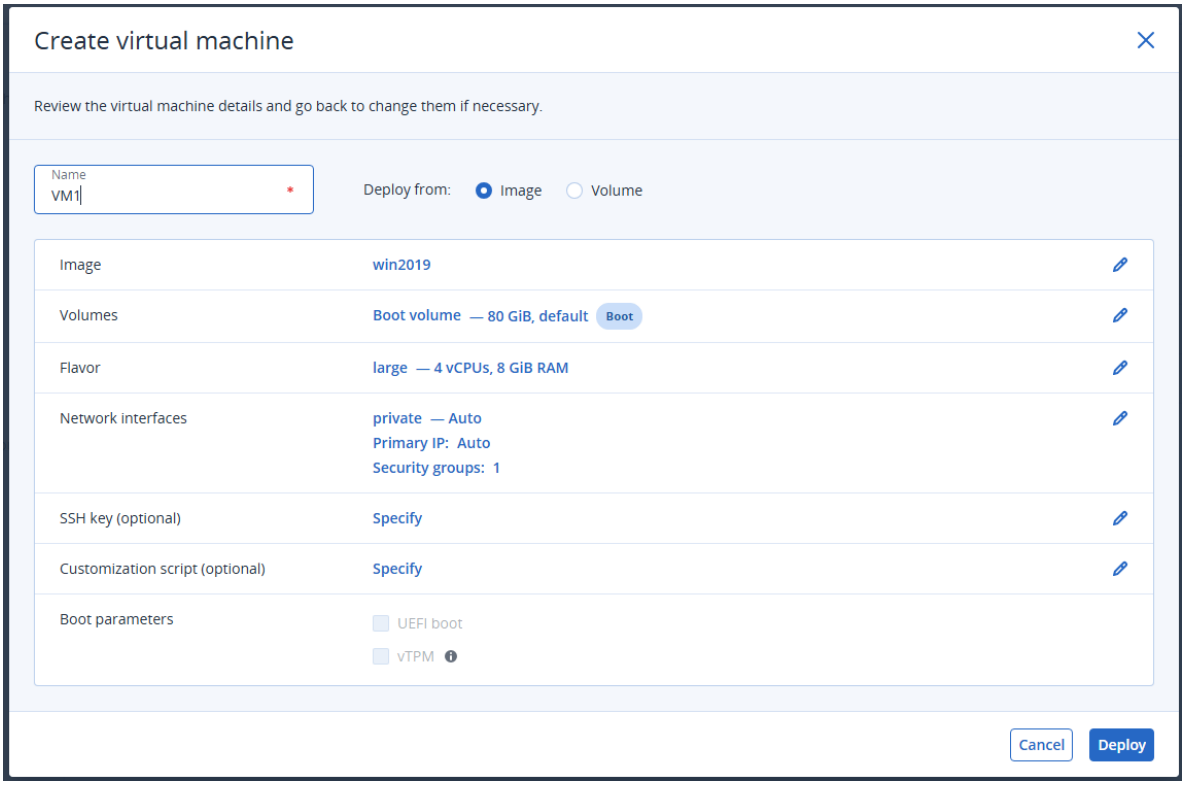
Lab 1. Build a basic customer environment and apply cyber protection.

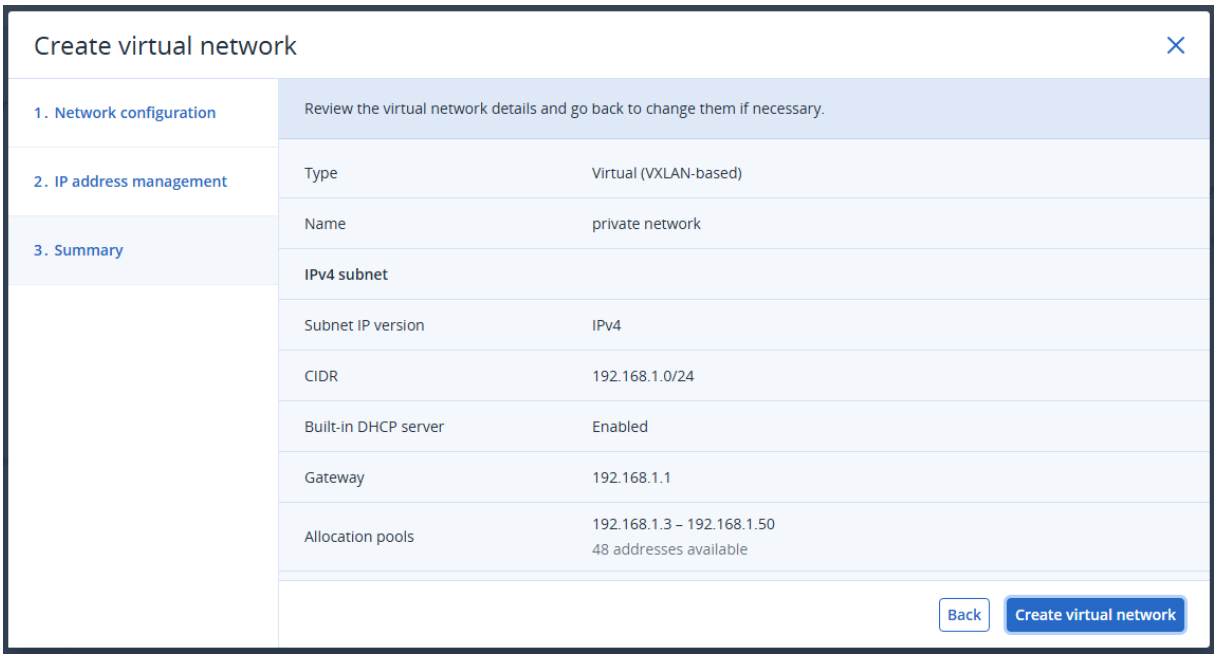
Objective	Deploy a Linux VM on a private virtual network and protect the deployed VM with Acronis Cyber Protect services.
Success criteria	A private network exists, Linux VM is running, protection plan is applied, the first backup completes and one VM can be restored successfully from the new backup.

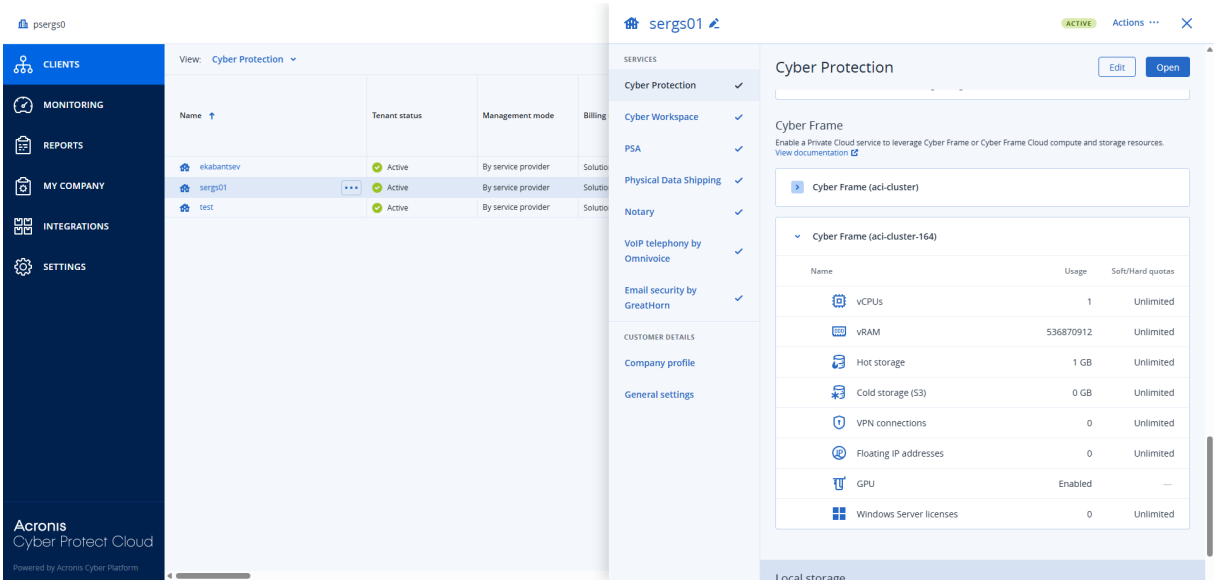
Suggested path

- Log in as a partner tenant and navigate to Settings → Locations to review available Cyber Frame locations. If no locations are available, it means your data center has not been updated yet (check the status here). If you want to add Cyber Frame Local, click Add Location → Cyber Frame and complete the setup.
- Create a new tenant and enable Cyber Frame for it in the Cyber Protection section during tenant creation. Activate the tenant and confirm the email.
- Log in to the customer tenant using the credentials defined in the previous step. This is a limitation of the Early Access Program; when the product is officially released, you will be able to manage the tenant as a partner without relogging.
- Navigate to Infrastructure → Cyber Frame.
- Create a private network: Go to Compute → Networks, click Create virtual network, enter a network name such as private-net, and configure a subnet such as 192.168.10.0/24.
- Create the first VM: Go to Compute → Virtual Machines, click Create virtual machine, choose an available Linux image, keep the default flavor unless a larger VM is needed, and attach the VM to the private network created in the previous step.
- Once the virtual machine is created, navigate to the Workloads tab, open Cyber Frame, locate the newly created workload, open it, go to Protection, create a protection plan and run the first

backup.







Lab 2. Validate site-to-site VPN connectivity

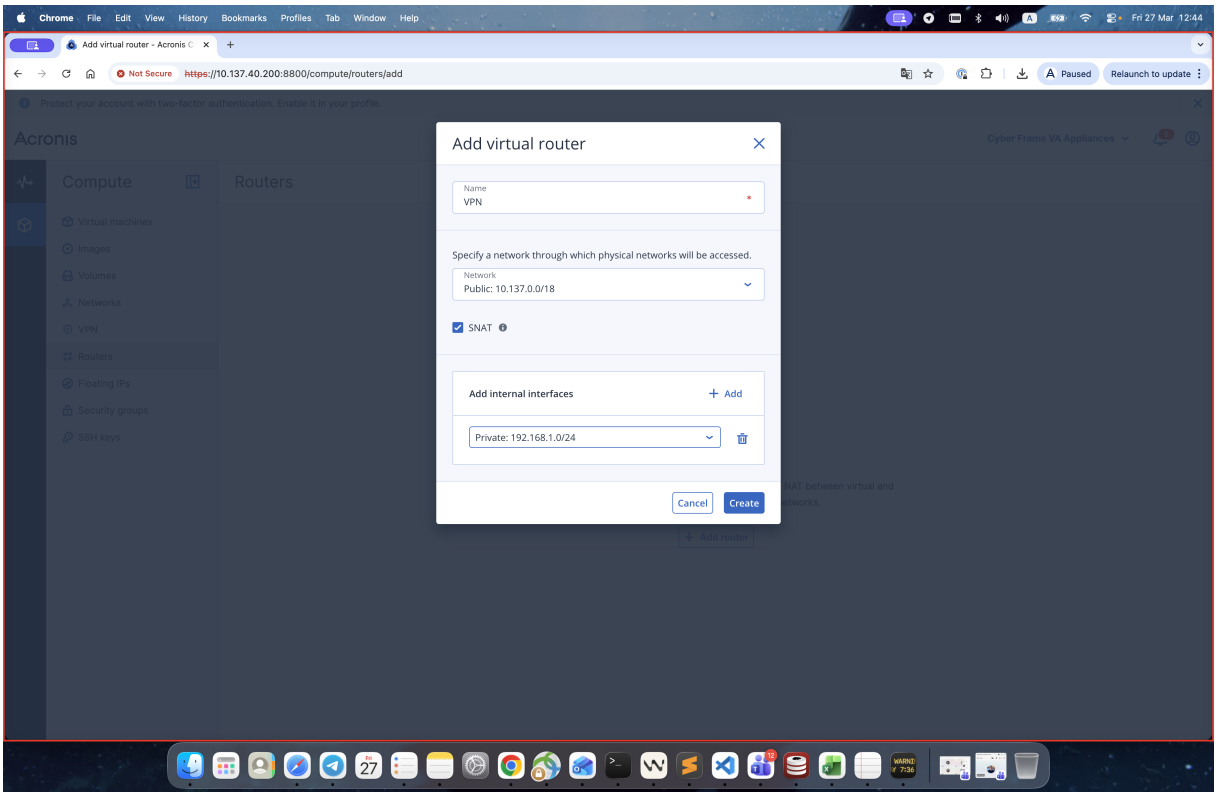
Objective	Create an IPsec VPN between Cyber Frame and an office network, then verify private connectivity in both directions.
Success criteria	The VPN status becomes Active, a VM private IP can be reached from the office network, an office host can be reached from the VM.

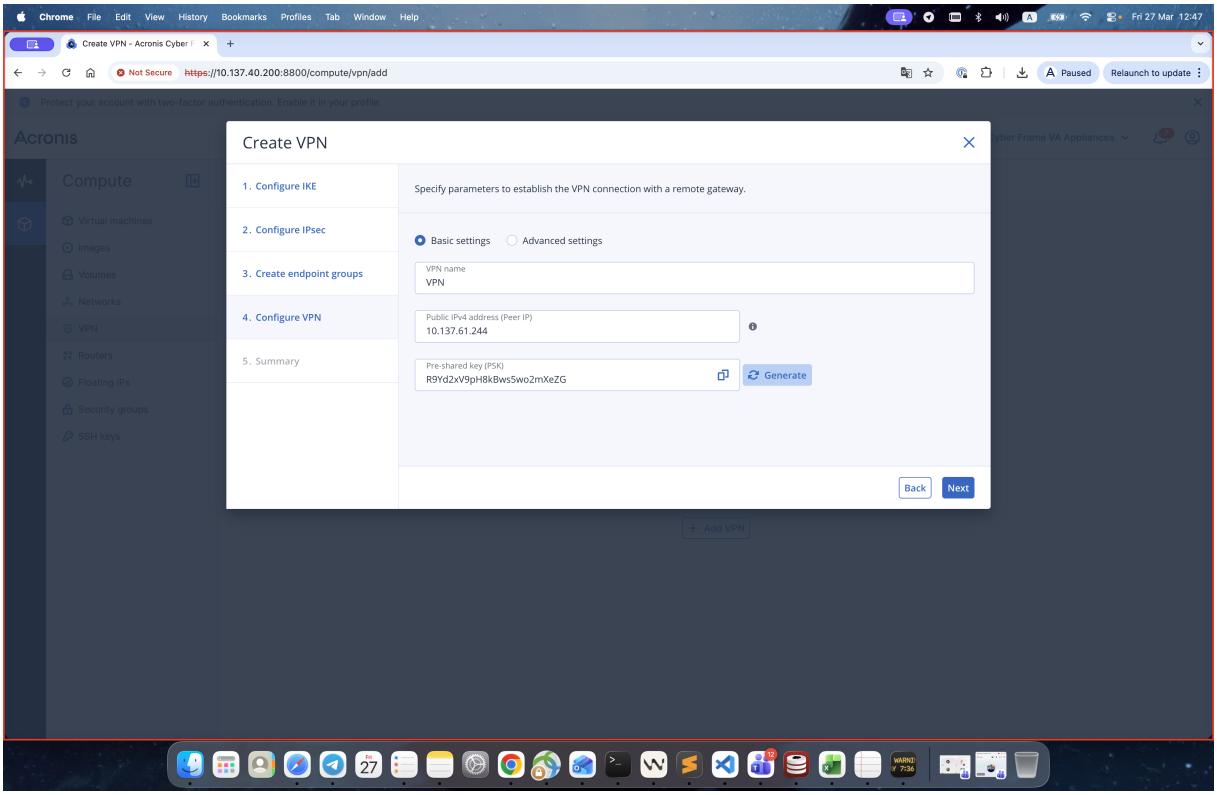
Suggested path

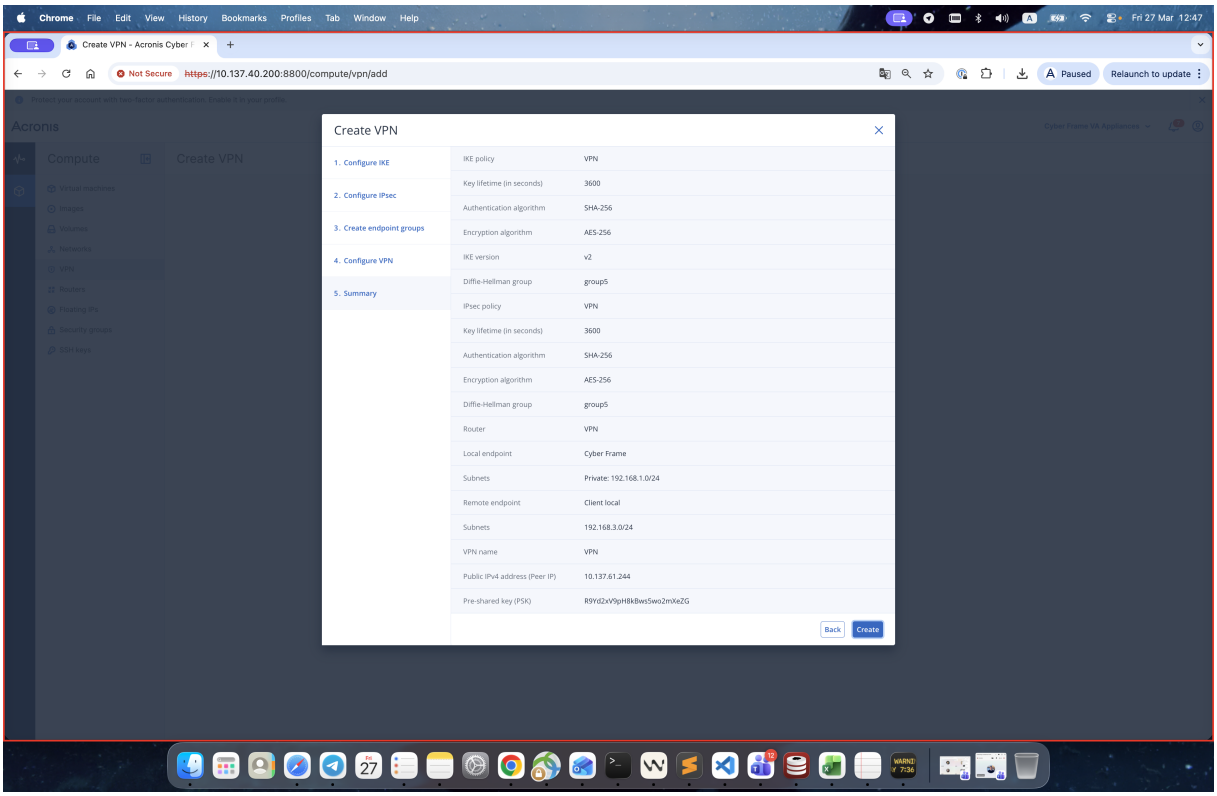
1. Create a private network for the VM: open Cyber Frame → Networks, click Create network, enter the network name, configure the subnet and gateway, then save the network. The network connected to the router must have a gateway specified.
2. Create a virtual router to connect the private network to the external network: open Compute → Routers, click Add router, enter the router name, select the external physical network as the external gateway, add the private network as an internal interface and create the router.
3. Set up VPN configuration: go to VPN, click Add VPN.
4. Configure the IKE policy: Create a new IKE policy and set: Policy name, key lifetime, authentication algorithm, encryption algorithm, IKE version, DH group. Then click Next.
5. Configure the IPsec policy: Create a new IPsec policy and set: Policy name, key lifetime, authentication algorithm, encryption algorithm, DH group. Then click Next.
6. Create endpoint groups: Select the router created earlier, then configure: Local endpoint name, Local subnet (the network created earlier), Remote endpoint name, Remote subnet (the network on your local site). Click Next.
7. Configure the VPN connection: VPN connection name, Peer IP / Remote gateway IP (office firewall public IP), generate the preshared key.
8. Create the VPN: Review the settings and click Create. Right after creation the status can change from Pending creation to Down. This is expected until the remote side is configured with

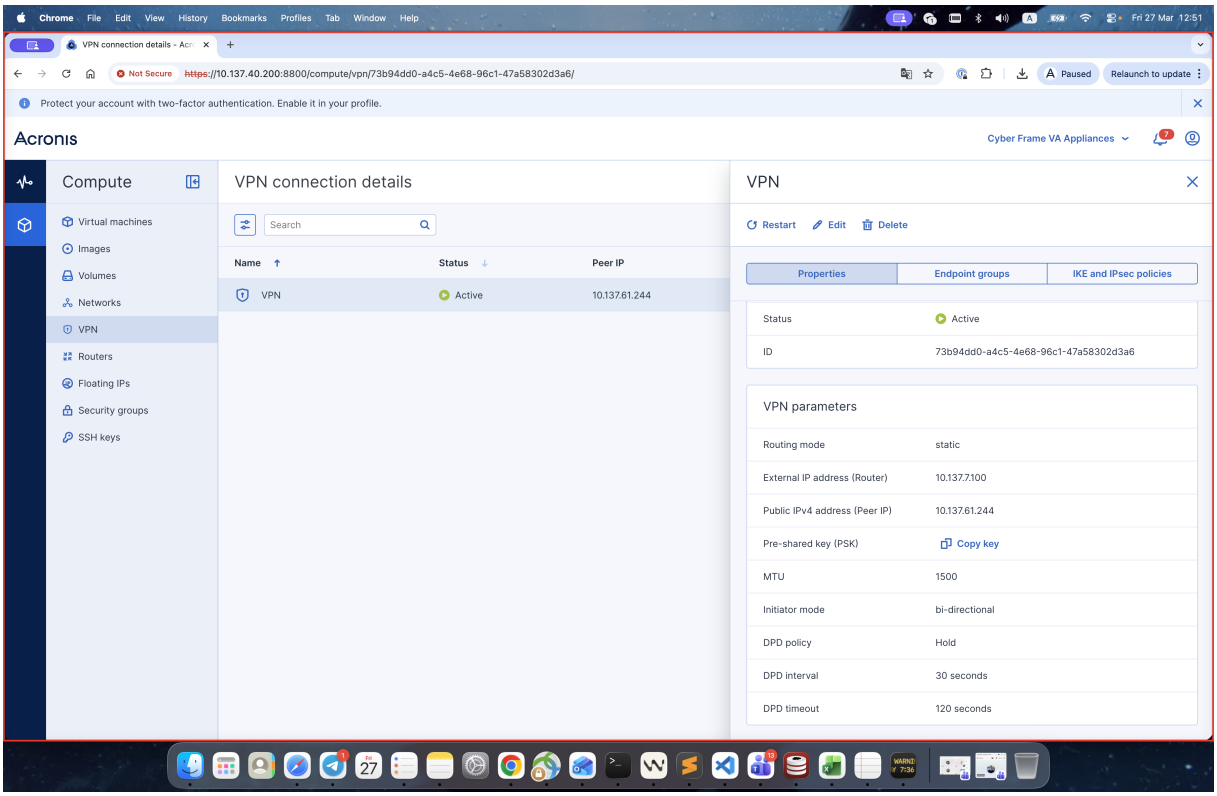
matching parameters.

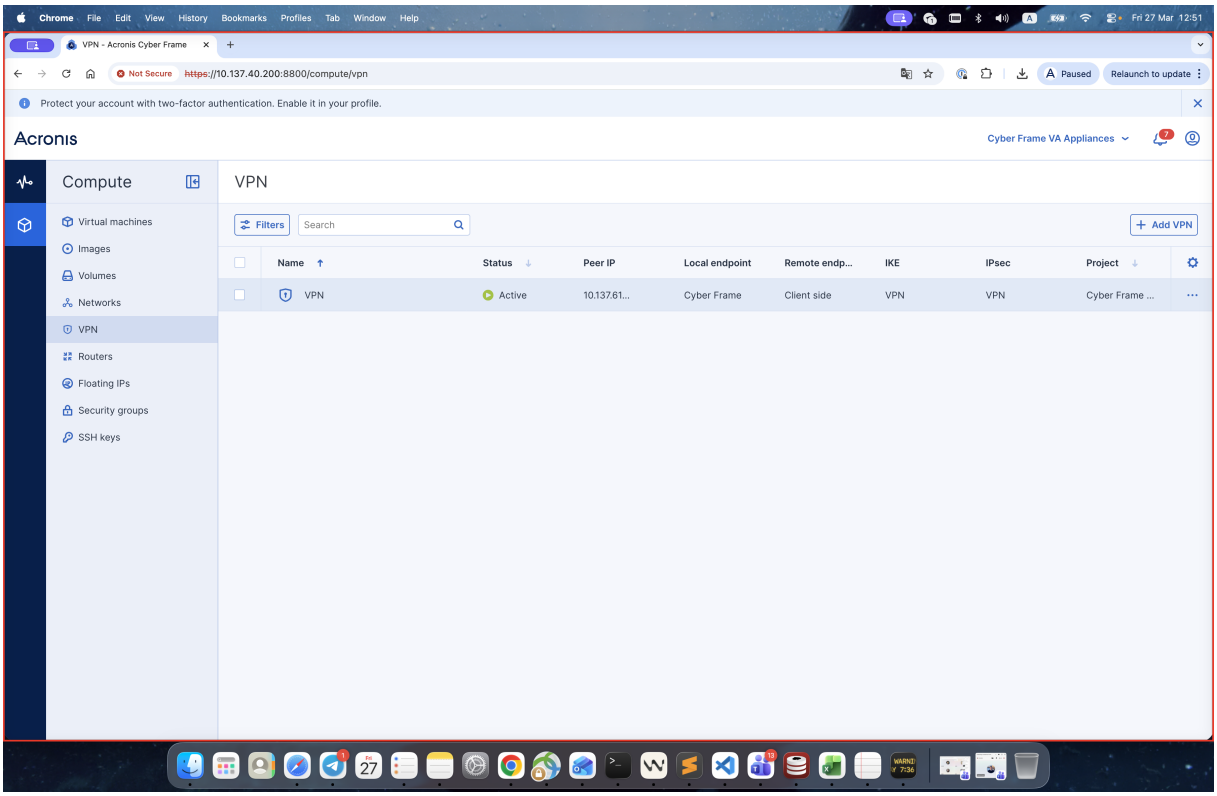
9. Use the VPN connection parameters to complete the configuration on your local firewall. Once the remote-side settings are applied, the VPN connection should be established. If needed, select the VPN connection and click Restart.
10. Then add VMs to the private network connected to the router used for the VPN connection.











Migration evaluation

Migration is a core part of the Cyber Frame value proposition, but not every evaluator needs to execute every migration path during the Early Access Program (EAP). Choose the method that best

aligns with your source environment and risk tolerance.

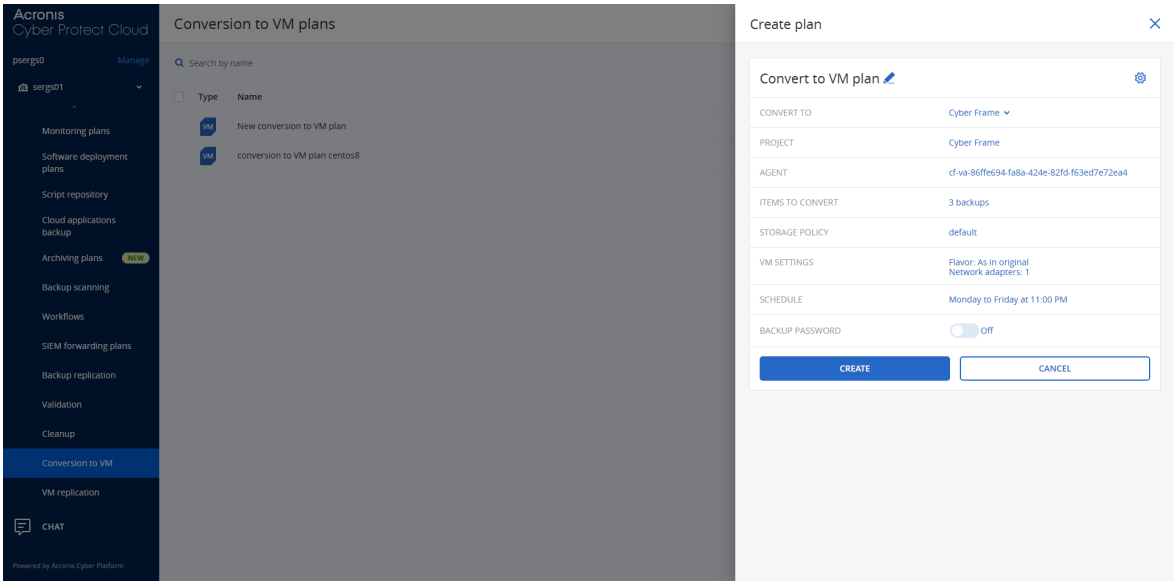
As part of the EAP, two migration methods are available: Convert-to-VM plan and restore-based migration. With general availability, a natively integrated migration tool for VMware-hosted VMs will also be introduced.

Method A. Convert to VM

Use this path when there is no direct source-to-target connectivity, when you want staged migration with test-before-cutover or when you want to keep source systems running until the final synchronization.

1. Make sure Cyber Frame resources are already provisioned for the customer in Acronis Cyber Protect Cloud and sign in to the Cyber Protection Console.
2. Install the Acronis Agent on the source machines or on the source virtualization host, depending on the source platform.
3. Create a Protection Plan for the source workloads and run the initial full backup of the source VMs or physical machines.
4. Store the backups in Acronis Cloud or another supported public cloud storage target that is available for the migration workflow.
5. Create a Convert to VM plan with the workload backups as the source and Cyber Frame as the target.
6. Run the Convert to VM plan once to create the initial VM copies in Cyber Frame.
7. Use those initial VMs to validate boot behavior, hardware sizing and network settings before the final cutover.
8. At the planned cutover time, stop the source workloads.
9. Run backup again so a final incremental backup is created.
10. Run the Convert to VM plan a second time to synchronize the latest changes and complete the migration.
11. Validate the final VM state in Cyber Frame, then proceed with source decommissioning only after

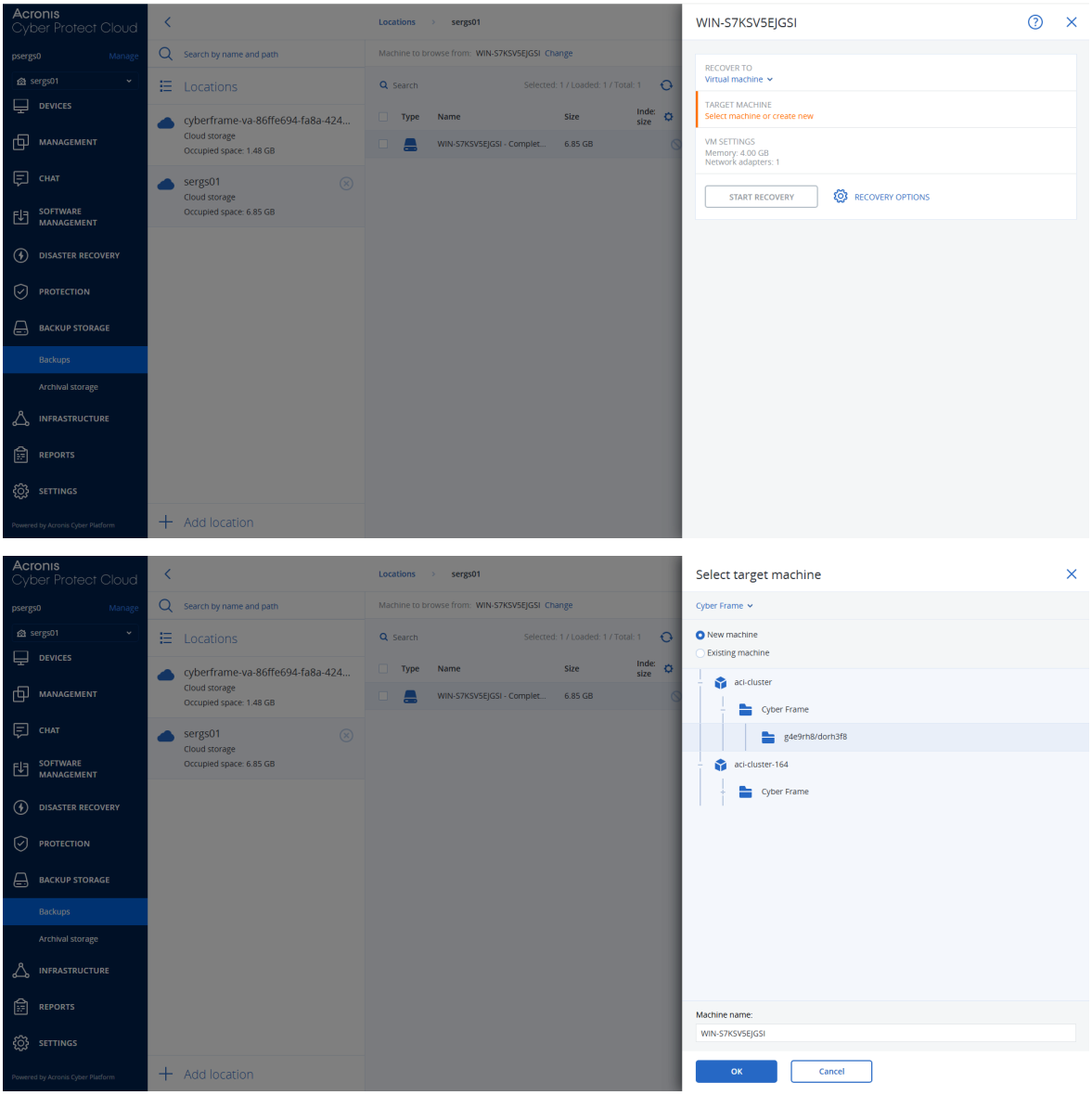
the migrated workload is accepted.



Method B. Restore to VM

Use this path for selective migrations, small environments, test pilots and cases where one-by-one restore is simpler than staged orchestration.

1. Provision the destination resources in Cyber Frame before you begin the restore.
2. Install Acronis Agent for VMware or Azure and connect it to the source environment if the source workload is not already protected.
3. Create and run a Protection Plan so the source VM has a current backup.
4. In the Cyber Protection Console, select the VM backup you want to migrate.
5. Choose Restore to → Cyber Frame VM.
6. Configure the target compute, storage and network settings for the restored VM.
7. Run the restore operation to create the VM in Cyber Frame.
8. Validate guest startup, private network reachability and any application checks you need for acceptance.
9. Decommission the original VM only after the restored workload is confirmed as healthy.



6. Local edition: What to validate next

This guide is intentionally cloud-first. Once cloud validation is complete, move to Cyber Frame Local only if infrastructure ownership, jurisdiction or long-term unit economics are central to your business model. If you are interested in a Local deployment in your data center or colocation facility, please reach out to your partner success manager, who will schedule an onboarding call with a solutions engineer to discuss the details.

Refer to documentation for installation guide: link

- POC baseline: Three nodes for evaluation or staging.
- Production guidance: Five or more nodes recommended.
- Key planning items: server compatibility, storage media, VLANs, 25G networking, firewall, static IPs, DNS and time sync.

- Primary Local question: Would operating your own cluster improve margin, sovereignty positioning or service differentiation enough to justify the added operational footprint?

EAP exit checklist

- [ ] We deployed test workloads in Cyber Frame Cloud and validated private networking.
- [ ] We applied protection and completed at least one restore test.
- [ ] We validated secure external access or site-to-site VPN, ideally both.
- [ ] We tested at least one migration method or documented why migration testing was deferred.
- [ ] We recorded blockers, unclear UI steps and follow-up questions.
- [ ] We reviewed the Cyber Frame price list (please reach out to your partner success manager for the price list) and recorded any pricing or packaging follow-up questions.

Glossary

B

Backup set

A group of backups to which an individual retention rule can be applied. For the Custom backup scheme, the backup sets correspond to the backup methods (Full, Differential, and Incremental). In all other cases, the backup sets are Monthly, Daily, Weekly, and Hourly. A monthly backup is the first backup created after a month starts. A weekly backup is the first backup created on the day of the week selected in the Weekly backup option (click the gear icon, then Backup options > Weekly backup). If a weekly backup is the first backup created after a month starts, this backup is considered monthly. In this case, a weekly backup will be created on the selected day of the next week. A daily backup is the first backup created after a day starts, unless this backup falls within the definition of a monthly or weekly backup. An hourly backup is the first backup created after an hour starts, unless this backup falls within the definition of a monthly, weekly, or daily backup.

C

Cloud server

[Disaster Recovery] General reference to a recovery or a primary server.

Cloud site (or DR site)

[Disaster Recovery] Remote site hosted in the cloud and used for running recovery infrastructure, in case of a disaster.

D

Data loss prevention (formerly, data leak prevention)

A system of integrated technologies and organizational measures aimed at detecting and preventing accidental or intentional disclosure / access to confidential, protected, or sensitive data by unauthorized entities outside or inside the organization, or the transfer of such data to untrusted environments.

Data loss prevention agent

A data loss prevention system's client component that protects its host computer from unauthorized use, transmission, and storage of confidential, protected, or sensitive data by applying a combination of context and content analysis techniques and enforcing centrally managed data loss prevention policies. Cyber Protection provides a fully featured data loss prevention agent. However, the functionality of the agent on a protected computer is limited to the set of data loss

prevention features available for licensing in Cyber Protection, and depends upon the protection plan applied to that computer.

Device control module

As part of a protection plan, the device control module leverages a functional subset of the data loss prevention agent on each protected computer to detect and prevent unauthorized access and transmission of data over local computer channels. These include user access to peripheral devices and ports, document printing, clipboard copy/paste operations, media format and eject operations, as well as synchronizations with locally connected mobile devices. The device control module provides granular, contextual control over the types of devices and ports that users are allowed to access on the protected computer and the actions that users can take on those devices.

Differential backup

A differential backup stores changes to the data against the latest full backup. You need access to the corresponding full backup to recover the data from a differential backup.

F

Failback

Switching a workload from a spare server (such as a virtual machine replica or a recovery server running in the cloud) back to the production server.

Failover

Switching a workload from a production server to a spare server (such as a virtual machine replica or a recovery server running in the cloud).

Finalization

The operation that makes a temporary virtual machine that is running from a backup into a permanent virtual machine. Physically, this means recovering all of the virtual machine disks, along with the changes that occurred while the machine was running, to the datastore that stores these changes.

Full backup

A self-sufficient backup containing all data chosen for backup. You do not need access to any other backup to recover the data from a full backup.

I

Incremental backup

A backup that stores changes to the data against the latest backup. You need access to other backups to recover data from an incremental backup.

L

Local site

[Disaster Recovery] The local infrastructure deployed on your company's premises.

M

Module

Module is a part of protection plan providing a particular data protection functionality, for example, the backup module, the Antivirus & Antimalware protection module, and so on.

P

Physical machine

A machine that is backed up by an agent installed in the operating system.

Point-to-site (P2S) connection

[Disaster Recovery] A secure VPN connection from outside to the cloud and local sites by using your endpoint devices (such as a computer or laptop).

Primary server

[Disaster Recovery] A virtual machine that does not have a linked machine on the local site (such as a recovery server). Primary servers are used for protecting an application or running various auxiliary services (such as a web server).

Production network

[Disaster Recovery] The internal network extended by means of a VPN tunneling and covering both local and cloud sites. Local servers and cloud servers can communicate with each other in the production network.

Protection agent

Protection agent is the agent to be installed on machines for data protection.

Protection plan

Protection plan is a plan that combines the data protection modules including Backup, Antivirus & Antimalware protection, URL filtering, Windows Defender Antivirus, Microsoft Security Essentials, Vulnerability assessment, Patch management, Data protection map, Device control.

Public IP address

[Disaster Recovery] An IP address that is needed to make cloud servers available from the Internet.

R

Recovery point objective (RPO)

[Disaster Recovery] Amount of data lost from outage, measured as the amount of time from a planned outage or disaster event. RPO threshold defines the maximum time interval allowed between the last suitable recovery point for a failover and the current time.

Recovery server

[Disaster Recovery] A VM replica of the original machine, based on the protected server backups stored in the cloud. Recovery servers are used for switching workloads from the original servers, in case of a disaster.

Runbook

[Disaster Recovery] Planned scenario consisting of configurable steps that automate disaster recovery actions.

S

Single-file backup format

A backup format, in which the initial full and subsequent incremental backups are saved to a single .tibx file. This format leverages the speed of the incremental backup method, while avoiding its main disadvantage– difficult deletion of outdated backups. The software marks the blocks used by outdated backups as "free" and writes new backups to these blocks. This results in extremely fast cleanup, with minimal resource consumption. The single-file backup format is not available when backing up to locations that do not support random-access reads and writes.

Site-to-site (S2S) connection

[Disaster Recovery] Connection extending the local network to the cloud, via a secure VPN tunnel.

T

Test IP address

[Disaster Recovery] An IP address that is needed in case of a test failover, to prevent duplication of the production IP address.

Test network

[Disaster Recovery] Isolated virtual network that is used to test the failover process.

U

USB devices database

[Device control] The device control module maintains a database of USB devices from which they can be added to the list of exclusions from device access control. The database registers USB devices by device ID, which can be entered by hand or selected from known devices in the service console.

V

Virtual machine

A virtual machine that is backed up at a hypervisor level by an external agent such as Agent for VMware or Agent for Hyper-V. A virtual machine with an agent inside is treated as physical from the backup standpoint.

VPN appliance

[Disaster Recovery] A special virtual machine that enables connection between the local network and the cloud site via a secure VPN tunnel. The VPN appliance is deployed on the local site.

VPN gateway (formerly, VPN server or connectivity gateway)

[Disaster Recovery] A special virtual machine providing a connection between the local site and the cloud site networks via a secure VPN tunnel. The VPN gateway is deployed on the cloud site.

Index