ALLIED ESM

HALO IMPLEMENTATION GUIDE

ITSM · ASSET DISCOVERY · CMDB

Virima Discovery Readiness Checklist

Is your environment ready to discover? A pre-deployment guide for IT and infrastructure teams.

PUBLISHED BY
Allied ESM Ltd

DATE
June 2026

CLASSIFICATION
Public

VERSION
1.0

HALO OFFICIAL PARTNER

HALO CERTIFIED PARTNER

BEFORE YOU BEGIN

What This Checklist Is For

Complete this before your Virima Discovery deployment begins. Virima gives you live, authoritative visibility across your entire IT estate — on-premises, cloud, and hybrid — so every team, and every AI agent you deploy, acts on accurate infrastructure data rather than stale records.

This checklist is for the IT or infrastructure lead responsible for the environment being discovered. Working through it in advance means fewer questions mid-project, a faster go-live, and discovery scans that return accurate, complete data from day one.

ARCHITECTURE

Virima uses three discovery methods: agentless scanning (no software on target devices), agent-based discovery (lightweight agents for Windows, Mac, and Linux), and API-based discovery for cloud environments including AWS and Azure. All three can be used in combination.

COVERAGE

Over 140 agentless probes cover Windows, Linux, Unix, macOS, network infrastructure, VMware, AWS, Azure, Active Directory, SQL databases, certificates, and more. Your deployment is scoped to the asset types relevant to your environment.

SECURITY

All credentials entered into the Discovery App are stored and encrypted locally on your Windows server. They are never transmitted to the Virima cloud. Scans are agentless by default — no persistent software is installed on target devices.

TIMELINE

Allied ESM typically completes Virima Discovery installation, configuration, and initial scans within the two-week delivery window. Having this checklist completed in advance is one of the key factors in keeping to that timeline.

Work through each step below and share your answers with Allied ESM at the start of the engagement. Steps 1 to 3 require input from your network or infrastructure team. Steps 4 and 5 require credentials to be gathered in advance.

1 Scope Your Environment

Answer these questions before we start — they determine how many Discovery App instances are needed

The number of Discovery App instances required depends on the size of your network, how it is segmented, and how frequently you want scans to run. A single Discovery App can scan over 20,000 IP addresses per day. Work through the questions below and share your answers with Allied ESM at the start of the engagement.

Environment Size

How many data centres or cloud environments need to be scanned?

Each physically or logically separated network may need its own Discovery App.

How many IP subnets are in scope, per location?

One Discovery App can simultaneously scan four /24 subnets (approximately 1,024 IPs).

Roughly how many devices or virtual servers in total?

Includes physical servers, VMs, network devices, storage, and cloud instances.

What is your desired scan frequency?

Daily scans are standard. Less frequent scans allow a single Discovery App to cover more IPs.

Network Connectivity

Is there full IP connectivity between your Discovery App server and all subnets in scope?

The Discovery App must be able to reach target devices directly. Firewalled segments may need additional instances.

Are there firewall rules or ACLs between data centres that would block scanning traffic?

These will need to be reviewed before scanning begins. Refer to the firewall requirements in Step 3.

Is outbound internet access available from the Discovery App server on port 443?

Required for the Discovery App to send discovery data to the Virima cloud and receive scan schedules.

2 Provision the Discovery App Server

One Windows server is required per Discovery App instance

The Virima Discovery App must be installed on a dedicated Windows server located within the network domain to be discovered. Virtual machines are fully supported. Provision the server to the specification below before the Allied ESM engagement begins.

REQUIREMENT	SPECIFICATION
Operating System	Windows Server 2012 or newer
Server Type	Dedicated physical or virtual machine
CPU	High-performance — 12 to 16 cores recommended
RAM	16 GB minimum
Disk	50 GB available storage
Browser	Google Chrome (required for Discovery App download and UI access)
Network	Persistent outbound connection to Virima cloud on port 443 (SSL)
Domain	Must be joined to the domain being discovered, or cross-domain trust enabled

Server Checklist

- [ ] **Windows Server 2012 or newer provisioned and accessible**
  Physical or virtual — either is fully supported.
- [ ] **12 to 16 core CPU and 16 GB RAM allocated**
  Lower specs will slow scan times, particularly for large environments.
- [ ] **50 GB disk space available**
  Used for Discovery App installation, logs, and temporary scan data.
- [ ] **Google Chrome browser installed on the server**
  Required to download the Discovery App installer from the Virima UI.
- [ ] **Server joined to the domain being scanned (or cross-domain trust configured)**
  Required for Windows agentless scanning via WMI.
- [ ] **Outbound port 443 open to Virima cloud URLs**
  Allied ESM will confirm the exact URLs for your region. UK/EU uses Frankfurt endpoints.

3 Prepare Network & Firewall Rules

Key ports that must be open for discovery to work

Discovery works by the Discovery App reaching out to target devices using standard protocols. No inbound connections from the internet are required. Review the table below with your network team and confirm which ports are open for the asset types in scope.

TARGET	PROTOCOL / PORT	PURPOSE
Virima cloud (outbound)	HTTPS / TCP 443	Discovery App sends scan data to Virima; receives scan schedules
Windows hosts	WMI / TCP 135, 139, 445	Agentless Windows scanning (batch method)
Windows hosts (alternate)	PowerShell / TCP 5985	PS Remoting — alternative to WMI batch
Linux / Unix / Mac	SSH / TCP 22	Agentless scanning of Unix-family systems
Network devices	SSH / TCP 22	Network infrastructure discovery including Cisco CDP
SNMP devices	SNMP / UDP 161	Edge devices and network infrastructure via SNMP
Discovery Agents	HTTPS / TCP 8191, 8190	Private agents reporting back to Discovery App
Public Agents	SSL / TCP 443, 8190	Work-from-anywhere agents via internet
AWS / Azure / VMware	API / TCP 443 or 80	Cloud and hypervisor discovery via API

ICMP Ping is used by default to check whether a target device is online before scanning. If ICMP Ping is blocked on your network, Allied ESM will enable NMAP port-check mode during configuration.

Firewall Checklist

- [ ] **Outbound port 443 open from Discovery App server to Virima cloud endpoints**
  Allied ESM will provide the exact URLs for your region. UK/EU: Frankfurt endpoints.
- [ ] **ICMP Ping permitted from Discovery App server to all target subnets**
  Or confirm with Allied ESM that NMAP mode should be used instead.
- [ ] **Required scan ports confirmed open between Discovery App and target devices**
  Review the table above with your network team and confirm which asset types are in scope.
- [ ] **Persistent connections permitted between Discovery App and Virima cloud**
  Stateful firewalls must allow the long-lived SSL connection to remain open.

4 Prepare Credentials

Gather the right credentials for each asset type in your environment

The Discovery App requires credentials to authenticate with target systems during scanning. These are entered once during setup, stored locally on your Discovery App server, and never transmitted to the cloud.

Only prepare credentials for the platforms present in your environment.

ASSET TYPE	CREDENTIALS REQUIRED	NOTES
Windows (Batch / WMI)	Domain admin account with elevated privileges	Must have remote file access to admin$ share and logon-as-a-service rights
Windows (PS Remoting)	Windows username and password	PowerShell Remoting must be enabled on target hosts and the Discovery App server
Linux / Unix / Mac / Solaris	SSH username + password or SSH private key	SUDO required for netstat/SS and dmidecode. Update sudoers to not require TTY.
Network Infrastructure	SSH username and password	SSH is required for relationship and dependency discovery on network devices
SNMP Devices	Community string (v1/v2) or username + password (v3)	SNMP alone cannot discover application relationships — SSH is preferred where possible
VMware vCenter	vCenter SSO User ID and password	Discovers the full vCenter hierarchy including ESXi hosts
Active Directory	AD host, Domain, Base DN, Bind DN, Password	Domain admin credentials required
MS SQL Server	Windows or SQL Server account	Account needs read rights on the sys.databases table
MySQL	MySQL user with SHOW DATABASES privilege	Remote MySQL access must be enabled; firewall rules must permit MySQL traffic
AWS	Account ID, Access Key, Secret Key	See Step 5 for IAM policy requirements
Azure	Client ID, Tenant ID, Secret Key, Subscription ID	See Step 5 for Azure App Registration and Reader role setup
Cisco Meraki	Meraki API key	Requires Meraki Cloud Dashboard API access to be enabled

5 Cloud Prerequisites

AWS and Azure require one-time setup before discovery can begin

If AWS or Azure environments are in scope, complete the steps below before Allied ESM runs the first cloud discovery scan. These are read-only permissions — Virima does not modify any cloud resources.

Only complete the sections relevant to your environment. If neither AWS nor Azure is in scope, skip to the summary on the next page.

AWS Prerequisites — AMAZON WEB SERVICES

- [ ] **Create an IAM user or role in your AWS account**
  This account will be used exclusively for Virima discovery scans.
- [ ] **Attach a read-only policy covering EC2, RDS, S3, ELB, Auto Scaling, IAM, DynamoDB, and ECR**
  Allied ESM will provide the exact IAM policy JSON during the engagement.
- [ ] **Note down: Account ID, Access Key ID, and Secret Access Key**
  These will be entered into the Discovery App during configuration. They are stored locally on your server, not in the cloud.
- [ ] **Confirm EC2 instances requiring OS-level discovery are reachable via SSH or WMI**
  Cloud API discovery covers resource metadata. Full OS discovery requires the server scan methods in Step 4.

Azure Prerequisites — MICROSOFT AZURE

- [ ] **Create a new App Registration in Azure Active Directory**
  Navigate to Azure Portal, then App Registrations, then New Registration.
- [ ] **Note down: Client ID and Tenant ID from the App Registration overview**
  Both are required when adding Azure credentials in Virima.
- [ ] **Generate a Client Secret under Certificates & Secrets**
  Copy the secret value immediately — it cannot be retrieved after leaving the page.
- [ ] **Assign the Reader role to your App Registration on your Azure Subscription**
  Navigate to Subscription, then Access Control (IAM), then Add Role Assignment, then select Reader and assign to your App Registration.
- [ ] **Note down: Subscription ID**
  Found on the Subscription overview page. Required alongside Client ID, Tenant ID, and Secret. Confirm Azure VMs requiring OS-level discovery are reachable via SSH or WMI.

AUTHORISED HALO & VIRIMA PARTNER

Allied ESM delivers Virima Discovery as a fixed-scope, two-week implementation.

Once this checklist is complete, share your answers with Allied ESM before the engagement begins. The more prepared your environment is on day one, the faster your discovery data will be live in Halo ITSM.

PRE-ENGAGEMENT CHECKLIST SUMMARY

01 Environment scoping questions answered and shared with Allied ESM

02 Discovery App server provisioned and accessible

03 Network and firewall rules reviewed and confirmed

04 Credentials prepared for all in-scope asset types

05 Cloud prerequisites complete (AWS and/or Azure if applicable)

Questions about any of the requirements above? Get in touch — we will guide you through it. Contact us at **info@alliedesm.com** or visit **alliedesm.com**