

Setup guide

From download to your first customer's devices reporting in: install TechSavve RMM on a Linux server or a Windows PC, then set it up in the order below. Most people are monitoring their first site within an hour.

On this page

1. [Before you start](#)
2. [Install it](#)
3. [Prepare DNS, Microsoft 365 and mailboxes](#)
4. [Sign in the first time](#)
5. [Set up the platform](#)
6. [Add your first customer](#)
7. [Install a collector at the site](#)
8. [Add devices and credentials](#)
9. [The rest of the first week](#)
10. [Keep it safe and up to date](#)
11. [Getting help](#)

1 Before you start

Choose where it runs. TechSavve RMM is the NOC: the console, the database and the alerting. It runs on one machine of yours:

Linux server (recommended)

- Ubuntu 22.04, 24.04 or 26.04, 64-bit
- 2 GB of memory (4 GB recommended), about 4 GB of free disk
- Root access (sudo)
- Runs around the clock as a normal server service

Windows PC

- Windows 11, or Windows 10 version 2004 or newer, 64-bit
- Virtualization turned on in the BIOS/UEFI (it almost always is)
- 4 GB of memory (8 GB recommended), about 10 GB of free disk
- Runs while a Windows user is signed in; for around-the-clock monitoring a Linux server is the better home

Everything is in the download. Docker, the application and (on Windows) WSL come with it: nothing else is installed first and nothing is downloaded during the install.

Decide on its address. Your technicians open the console at this address and your site collectors report to it. A name such as `rmm.yourcompany.com`, pointed at the machine in your DNS, lets you get a free trusted certificate later. Collectors at other offices or customers must be able to reach it over HTTPS (port 443).

2 Install it

Get the installer from the [Download page](#). The zip's SHA-256 is listed there if you want to check the file.

Linux

1. Copy the zip to the server and extract it there (no unzip needed):

```
python3 -m zipfile -e TechSavve-MSP-Suite-Linux-Installer-1.3.4.zip .
```

2. Install the installer package:

```
sudo apt install ./TechSavve-MSP-Suite-Linux-Installer-1.3.4.deb
```

3. Run it:

```
sudo techsavve-install
```

4. Accept the license agreement, choose *new installation*, and type the administrator's email address. That becomes the one account on the platform.

5. It finishes in a few minutes and prints the address to open, for example

```
https://192.168.1.50.
```

Useful options: `--url https://rmm.yourcompany.com` sets the address people will use; `--email you@yourcompany.com` and `--accept-eula` make it unattended. `techsavve status` shows what is running.

Windows

1. Extract the whole zip (keep every file and the `payload` folder together).
2. Double-click `TechSavve-MSP-Suite-Windows-Installer-1.3.4.exe`.
3. Windows asks once for an administrator's permission. If WSL isn't set up yet, the installer turns it on and asks to restart once; after you sign in again it carries on by itself.
4. Accept the license agreement, choose *new installation*, and type the administrator's email address.
5. When it finishes it opens the console in your browser at `https://localhost`.

Should other computers and site collectors reach it? Run it from a PowerShell opened with *Run as administrator*, in the extracted folder:

```
.\TechSavve-MSP-Suite-Windows-Installer-1.3.4.exe -AllowNetworkAccess
```

Without that, the console only answers on this PC.

3 Prepare DNS, Microsoft 365 and mailboxes

Get these ready before you set the platform up (step 5). None of it is needed for a first look, but sign-in with Microsoft accounts, email and trusted certificates all depend on it. *yourcompany.com* stands for your own domain below.

DNS records

- **The console**, for example `rmm.yourcompany.com`: an *A* record pointing at the server's public IP address (or your internal DNS, if only your own network uses it). Needed for the free certificate and for collectors at other sites.
- **Remote control (TechSavveRDP)**, for example `rdp.yourcompany.com`: an *A* record pointing at the same server's public IP address. The remote-control apps of your technicians and your customers connect to this name, and it can also host the customer support pages (<https://rdp.yourcompany.com/support>).
- **The password vault**, if you use it, for example `vault.yourcompany.com`: an *A* record pointing at the same server.
- **Email authentication** for the domain the platform sends from: an *SPF* record that includes your mail service, *DKIM* records and a *DMARC* record. Microsoft 365 domains usually have these already. A sending service such as Amazon SES gives you its own DKIM records to add (below).
- Firewall: port **443** (HTTPS) open to the server for people and collectors, and port **80** open from the internet while Let's Encrypt issues and renews the certificate.
- Firewall for TechSavveRDP (open and, behind a router, forward them to the server): TCP **21115**, **21116** and **21117**, and UDP **21116**. TCP 21118 and 21119 only for the optional web client; TCP and UDP **3478** plus UDP **49160–49360** let sessions connect directly (faster) instead of through the relay.

Microsoft 365 / Entra: three app registrations

Create them in the Microsoft Entra admin center under *App registrations* (you need the Application Administrator or Global Administrator role). They are entered in the NOC under **Admin** → **Platform settings** → **Single sign-on & mail (Microsoft Entra)**. First note your **Tenant ID** (the *Directory (tenant) ID* on any app's Overview page): every app uses it. The worksheet has a box for every value below.

1. NOC API App — create this one first

The console's back end. A Microsoft sign-in produces a token for this app, and the NOC checks it.

- **Register:** name *NOC API App*; supported account types *Accounts in this organizational directory only* (choose *any organizational directory* instead if your customers' own staff will sign in with their Microsoft accounts); no redirect URI.
- **Expose an API:** set the *Application ID URI* to the default `api://<client ID>`. Add a scope named `access_as_user`, *Who can consent: Admins and users*, with a display name such as "Use the TechSavve NOC". Under *Authorized client applications*, add the NOC App's client ID (after step 2) with that scope, so nobody is asked to consent.
- **Token version (required):** in the app's *Manifest*, set `requestedAccessTokenVersion` to 2 and save. The NOC accepts only version 2.0 tokens; with the default (empty), every Microsoft sign-in is refused.
- **Permissions:** none to add. **Secret:** none.
- **Save:** the *Application (client) ID* → NOC field *NOC API App - Client ID* (the Application ID URI follows from it).

2. NOC App

The sign-in page your staff see: *Continue with Microsoft Entra ID*.

- **Register:** name *NOC App*; the same account type as the NOC API App.
- **Authentication:** add a platform *Single-page application* with the redirect URI `https://rmm.yourcompany.com/` (your console address with the slash at the end). Add `https://localhost/` too if you also open the console on the server itself. Leave implicit grant (access and ID tokens) off.
- **API permissions (delegated):** Microsoft Graph `openid`, `profile`, `email` and `User.Read`; and under *My APIs*, the NOC API App's `access_as_user`. Then *Grant admin consent*.
- **Secret:** none (a single-page app never has one).
- **Save:** the *Application (client) ID* → *NOC App - Client ID*, and the *Directory (tenant) ID* → *Entra tenant ID*.

Microsoft sign-in only lets people in who have a role in the NOC: give each person access in the NOC as well. Customer staff can sign in with their own Microsoft accounts once their tenant's Entra tenant ID is set on that customer in the NOC.

3. NOC Mail App

Sends alerts, invitations, password resets and reports through Microsoft 365, as `noc@` and `noc-reports@`.

- **Register:** name *NOC Mail App*; Accounts in this organizational directory only; no redirect URI.
- **API permissions (application):** Microsoft Graph → *Application permissions* → `Mail.Send` (application, not delegated). Then *Grant admin consent* and check that it shows *Granted*.
- **Certificates & secrets:** *New client secret*, up to 24 months. Copy the secret's **Value** at once (not the Secret ID): it is shown only once. Put a reminder in your calendar before it expires; when it does, email stops until you enter a new one.
- **Limit what it can send as (recommended):** on its own, `Mail.Send` lets the app send as *any* mailbox in your organization. In Exchange Online, limit it to the NOC's mailboxes: put `noc@` and `noc-reports@` in a mail-enabled security group and create an application access policy for the app with that group (PowerShell `New-ApplicationAccessPolicy -AppId <client ID> -PolicyScopeGroupId <group> -AccessRight RestrictAccess`; check it with `Test-ApplicationAccessPolicy`), or the equivalent Exchange RBAC for Applications role. It can take up to an hour to apply.
- **Save:** *Directory (tenant) ID* → *NOC Mail App - Tenant ID* (or leave it blank to use the one above); *Application (client) ID* → *NOC Mail App - Client ID*; the secret *Value* → *NOC Mail App - Client Secret Value* (type it into the NOC; keep it in your password manager, not on paper); and the secret's expiry date. Then press *Send a test email through the NOC Mail App*.

Optional: Microsoft 365 SMTP app (large reports)

Microsoft Graph can't send a scheduled report larger than about 2.9 MB; those go through Microsoft 365 SMTP with this separate app. Without it, only very large reports fail.

- **Register:** a fourth app, for example *NOC SMTP App*, single tenant, with a client secret (save its Value and expiry).
- **API permissions (application):** *Office 365 Exchange Online* → SMTP.SendAsApp, then *Grant admin consent*.
- **In Exchange Online PowerShell:** `New-ServicePrincipal -AppId <client ID> -ObjectId <Object ID from Enterprise applications>`, then `Add-MailboxPermission -Identity noc-reports@yourcompany.com -User <that Object ID> -AccessRights FullAccess`. SMTP AUTH must be allowed for that mailbox.
- **Save:** Tenant ID, client ID and secret → **Scheduled report email (SMTP)** on the same page.

Not using Microsoft 365 for mail? Choose a standard SMTP server under **Email settings** and skip the NOC Mail App and the SMTP app; the NOC App and NOC API App are still what Microsoft sign-in needs. Scripts that work in Microsoft 365 use their own app registration, stored under **Credentials** as an *App registration (OAuth client credentials)*, with only the permissions those scripts need.

Mailboxes

- `noc@yourcompany.com`: sends alerts, invitations and password resets.
- `noc-reports@yourcompany.com`: sends scheduled reports and business reviews.
- `vault@yourcompany.com`: sends the password vault's invitations and new-device sign-in alerts, if you use the vault.

They can be **shared mailboxes**: no licence and no password needed, and replies land where your team can read them. A *distribution group* can't send, so don't use one as a sender (it is fine as a recipient, such as a list of your technicians). Put `noc@` and `noc-reports@` in the NOC Mail App's access policy group, then enter them under **Admin** → **Platform settings** → **Email settings** and use the test buttons.

How the password vault sends email

The vault sends through an SMTP server with a username and password. Microsoft 365 normally refuses that kind of sign-in (SMTP AUTH is off for new tenants and being retired), so use one of these for vault@:

- **In AWS: Amazon SES.** Verify your domain in SES (it gives you three DKIM records to add to DNS), create SMTP credentials, and use the SES SMTP endpoint for your region on port 587. Ask AWS to move the account out of the SES sandbox so it can send to any address. It costs cents a month at this volume.
- **On premises:**
 - a **Microsoft 365 SMTP relay**: an inbound connector in Exchange that accepts mail from your server's static public IP address, no password needed (port 25 must be open outbound);
 - a **mail relay service** such as SMTP2GO, SendGrid, Mailgun or Brevo, with its own SMTP username and password;
 - or your **own mail server** or your internet provider's relay, if you already run one.

Whichever you choose, add the sending service to the domain's SPF record and publish its DKIM records, so the mail isn't marked as spam.

4 Sign in the first time

1. Open the address the installer gave you. Your browser warns about the certificate the first time: the built-in one is self-signed. Continue past it for now (step 5 replaces it).
2. Sign in with the email address you gave the installer and the preset password `ChangeMe123!`
3. Choose your own password straight away. The console makes you, and you should do it before anyone else can reach the address, because the preset password is public.

The platform starts a **30-day free trial** (up to 100 devices, 100 monitors, 2 customers, 4 sites and 5 staff users). On day 31 it locks until a license is activated (step 5).

5 Set up the platform

Everything here is under **Admin** in the menu on the left. Do it in this order:

1. **A trusted certificate** – Admin → **SSL Certificates**: *Add a domain* with your console's name, then *Request certificate*. You get a free Let's Encrypt certificate that renews itself. It needs a real domain name (not an IP address) pointed at the machine and port 80 reachable from the internet. Collectors on other networks check this certificate, so do it before installing them. Already have a certificate? `sudo techsavve install-cert fullchain.pem privkey.pem` installs it.
2. **The platform's own address** – Admin → **Platform settings**, *Frontend URL*: the address people and collectors use, for example `https://rmm.yourcompany.com`. It goes into invitations, password-reset links and the install command each collector is given, so make sure it is right.
3. **Microsoft sign-in and email** – Admin → **Platform settings**: enter the Tenant ID and the three apps' IDs and secret from step 3 under *Single sign-on & mail (Microsoft Entra)*, choose Microsoft 365 or SMTP under *Email settings*, put `noc@` and `noc-reports@` in the send-address boxes, and use the *Send a test email* buttons. Alerts, invitations, password resets and reports all need this.
4. **Remote control address** – Admin → **TechSavveRDP**, *TechSavveRDP remote access server*: enter `rdp.yourcompany.com` (from step 3). Every TechSavveRDP client and support link is pointed at it.
5. **Your name and logo** – Admin → **Platform settings**: your company name and logo appear on the console, reports, status pages and the customer portal.
6. **Your license** – Admin → **License**: *Activate with a purchase code* (online) or *Activate a license key* (for a server with no internet). [Request a quote](#) if you don't have one yet.
7. **Your technicians** – Admin → **Local Account Users & Security**: *Invite user* for each person, with the role that fits.
8. **Two-step sign-in** – Admin → **Platform settings**: require it for staff. Your NOC holds the keys to every customer.

6

Add your first customer

1. **Tenants** – type the customer's name and click *Add tenant*. Every customer is its own tenant: their devices, alerts, tickets and reports stay separate.
2. Open the tenant, go to **Sites** and click *Add site* for each office or location. Devices and collectors belong to a site.
3. Moving from another tool? **Getting started** → *Import* brings customers, sites and devices in from your old RMM or a CSV file in one go.

7 Install a collector at the site

TechSavve RMM is agentless: nothing is installed on the customer's computers. A small **collector** at each site reaches the devices there (SNMP, SSH, WinRM, ping, SNMP traps and NetFlow) and reports to your NOC over HTTPS. Put it on any always-on Windows or Linux machine at the site.

1. **Admin** → **Collectors**: choose the customer in the box at the top right.
2. Under *Collector software*, download the collector for Windows or Linux and copy it to the machine at the site. Unzip it there.
3. Under *New collector*, give it a name, choose the site and click *Generate enrollment token*. The page shows the exact command, with the token and your platform's address filled in.
4. On the site machine, from the unzipped `ts-collector` folder, run that command:
 - Windows (PowerShell, *Run as administrator*): `.\install\install-windows.ps1 -Token ... -Api ...`
 - Linux: `sudo sh install/install-linux.sh --token ... --api ...`

It installs the collector as a service, connects it and starts it. Within a minute it shows *online* on the Collectors page.

A token works once and expires (the page shows when). If something goes wrong, generate a new one. On Linux, `systemctl status ts-collector` shows whether the collector is running.

A collector on the NOC's own server

When the NOC runs on a machine in an office it should also watch, that machine can be the office's collector too: no second computer needed. The two don't get in each other's way (the NOC uses ports 80 and 443; the collector listens on 162 for SNMP traps and 2055/4739 for NetFlow).

- **Linux server:** install the Linux collector on the server itself (not inside the NOC's containers), exactly as above, but point it at the NOC on the same machine. In the command the Collectors page shows, replace the address after `--api` with `http://127.0.0.1:8000`:

```
sudo sh install/install-linux.sh --token <token> --api http://127.0.0.1:8000
```

The collector then talks to the NOC inside the machine: no certificate needed and nothing leaves the server.
- **Windows PC:** install the Windows collector on Windows itself (not inside the TechSavve appliance), from an administrator PowerShell, with the command exactly as the Collectors page shows it. Windows is on the office network, so the collector sees the devices directly. Install the trusted certificate (step 5) first.

Worth knowing: the collector shares the machine's memory and processor with the NOC, which is fine for a small office; and if that machine goes down, the NOC and that office's monitoring stop together. A NOC in the cloud (AWS and similar) only sees itself, so customer sites still need their own collectors.

8 Add devices and credentials

1. Open the tenant's **Devices** and click *Add device*, or let the collector find them: run a discovery scan of the site's network from **Admin** → **Collectors**.
2. Give each device a way in: **WinRM** for Windows, **SSH** for Linux and macOS, **SNMP** for switches, firewalls, printers and other network gear. Stored credentials are encrypted and only the collector at that site uses them.
3. Within a few minutes each device shows up or down, with its health, disks, services and inventory.

9 The rest of the first week

Getting started in the console keeps a checklist of what is left and ticks each item off as it is done. In short:

- **Monitors** for the services that matter: websites, mail, VPNs and line-of-business apps
- **On-call paging** (Admin → On-call) and the TechSavve phone app for alerts on the go
- **Patching**: scan for missing updates, then set **maintenance windows** for when updates install and machines restart
- **Backups** your customers depend on, watched so you know the day a job stops
- **Microsoft 365 or Google Workspace**, endpoint protection and the customers' **DNS**, connected for security findings
- **Reports**: a first business review, scheduled monthly reports, status pages and the customer portal

10 Keep it safe and up to date

- **Backups** – Admin → Backup & Restore: the database is backed up every night. Set a *backup password* under *Full backups*, then *Download full backup* or add an *off-server copy* (cloud storage or a network share). A full backup brings the whole server back on a new machine; keep its password in a password manager.
- **Upgrades** – run the newer installer over the old one; data, settings and the certificate stay. Steps and what's new: [Updates & upgrades](#).
- **Day to day** – Linux: `techsavve status`, `techsavve logs api`, `techsavve restart`. Windows (PowerShell): `ws1 -d TechSavveRMM -u root -- techsavve status`.

11 Getting help

The **User Guide** in the console's menu explains every page. Stuck or want a hand with the first site? Email assistance@techsavve.com or call [\(214\) 430-9342](tel:2144309342).

Setup worksheet

Fill this in as you follow the setup guide (techsavve.com/setup), then keep it with your IT records. Every box can be typed into and saved. Do not write passwords, client secret values or the backup password here: write WHERE each is kept (for example "Password manager > TechSavve").

Company name

Prepared by

Date

1. The server

Where TechSavve RMM runs (guide step 1).

Runs on ☐ Linux server ☐ Windows PC

Hosted ☐ AWS ☐ Other cloud ☐ On premises

Server name

Operating system and version

Internal IP address

Public IP address

Install folder default /opt/techsavve

Administrator email (first account)

2. Addresses and DNS

Guide step 3. A records point at the server; email records protect the sending domain.

Console address <https://rmm.domain.com>

Password vault address <https://vault.domain.com>

TechSavveRDP address rdp.domain.com

Public IP the A records point at

TechSavveRDP server key public key shown under Admin > TechSavveRDP; safe to note

Domain the platform sends from domain.com

DNS is hosted at GoDaddy, Cloudflare, Route 53 ...

Done ☐ Console A record ☐ RDP A record ☐ Vault A record ☐ SPF ☐ DKIM ☐ DMARC

Open ☐ 443 ☐ 80 ☐ RDP TCP 21115-21117 ☐ RDP UDP 21116 ☐ 3478 + 49160-49360

Certificate ☐ Let's Encrypt (Admin > SSL Certificates) ☐ Own certificate

Certificate domain

Certificate renews / expires

3. Microsoft 365 / Entra

Guide step 3. Entered under Admin > Platform settings > Single sign-on & mail (Microsoft Entra).

Tenant ID (Directory ID)

NOC App - Client ID

NOC App redirect URI https://rmm.domain.com/

NOC API App - Client ID

NOC API App - Application ID URI api://<client ID>

NOC Mail App - Client ID

NOC Mail App - Tenant ID blank = same tenant

Mail App secret: where it is kept

Mail App secret expires on

NOC API App ☐ access_as_user scope ☐ Token version 2 (manifest) ☐ NOC App authorized

NOC App ☐ SPA redirect added ☐ Graph + access_as_user consented

Mail App ☐ Mail.Send (Application) granted ☐ Access policy set ☐ Test email sent

Access policy group (sender mailboxes)

SMTP app - Client ID (optional) reports over 2.9 MB

SMTP app secret: where it is kept

SMTP app secret expires on

4. Mailboxes

Shared mailboxes are fine for sending; a distribution group cannot send.

Address

Used for

Type (shared / user)

Email sent through ☐ Microsoft 365 (NOC Mail App) ☐ SMTP server

SMTP host (if SMTP)

SMTP port and security 587 STARTTLS / 465 SSL

5. Password vault email

The vault sends with an SMTP username and password (guide step 3).

Vault sends through ☐ Amazon SES ☐ Microsoft 365 relay ☐ Relay service ☐ Own mail server

SMTP host email-smtp.<region>.amazonaws.com

Port

SMTP username

SMTP password: where it is kept

Vault admin token: where it is kept

Vault sender address vault@domain.com

6. License

Guide step 5: Admin > License.

Activation ☐ Purchase code (online) ☐ License key (offline)

License / order number

Licensed for (devices, customers)

Trial started on

Activated on

7. Technicians

Admin > Local Account Users & Security > Invite user.

Name	Email	Role	2-step on
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

8. First customer and sites

Guide steps 6 and 7: Tenants > Add tenant, then Sites > Add site.

Customer (tenant) name

Site name	Address	Collector machine	Collector IP
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

9. Device access

Guide step 8: Write where each credential is kept, never the password.

Kind	Account / community	Where the password is kept

10. Backups and support

Guide step 10: Admin > Backup & Restore.

Backup password: where it is kept	Off-server copy goes to
	cloud storage / network share
Full backup tested on	Next upgrade check
TechSavve support	Your notes
assistance@techsavve.com · (214) 430-9342	