EVOLVE IP
THE CLOUD SERVICES COMPANY™

RMM/MDM

Quick Reference Guide

Contents

Getting Started

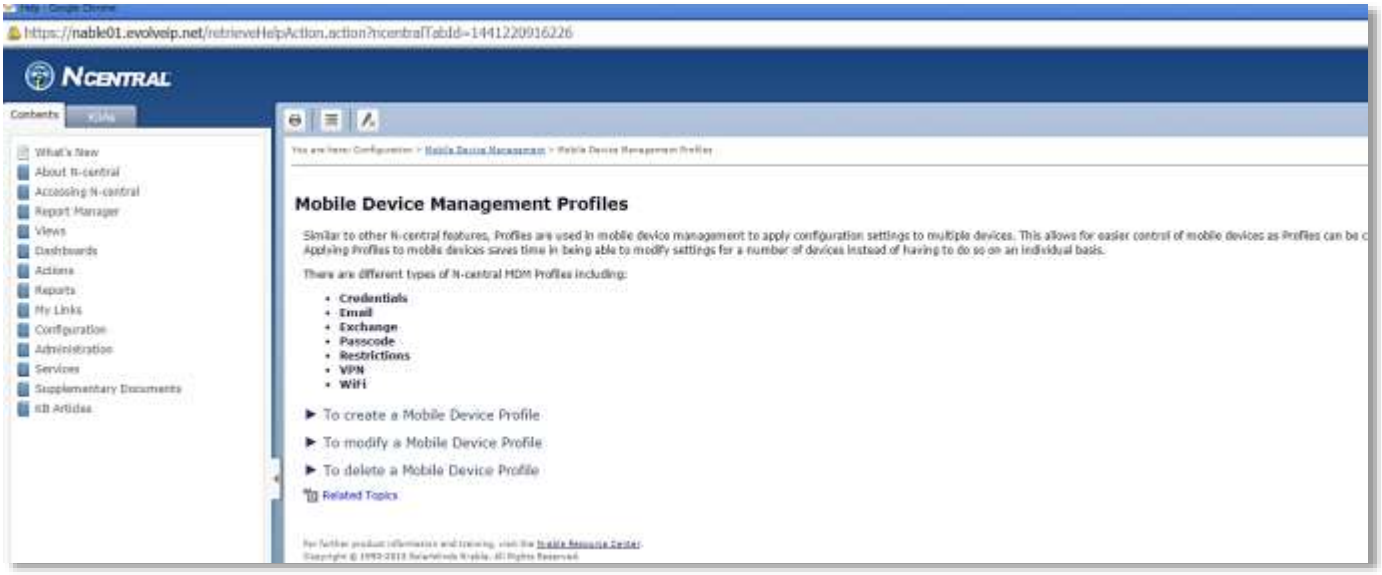
Evolve IP's RMM/MDM is powered by Solarwinds N-Able, the industry leader in remote monitoring and management for servers, workstations and mobile devices. You can access RMM/MDM from any web browser or mobile device. It is highly suggested to review this document for technical specs, instructions and best practices before attempting the tasks for the first time. If you have any questions accessing your account contact Evolve IP Support for assistance.

Accessing the Run Book and Training Videos

Evolve IP has found the N-Central Runbook to be extremely valuable for both initial setup and day to day RMM administration. Also, the N-Central Runbook is updated as the software is updated. Accessing the Runbook is easy and be found by following the steps below.

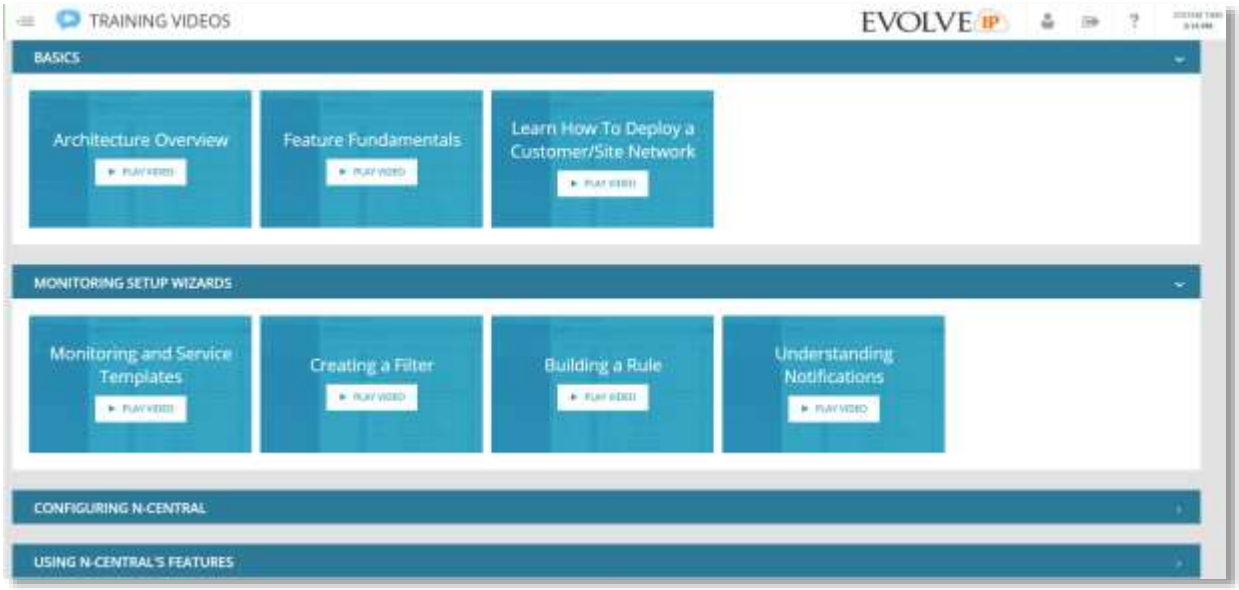
To Access the N-Central Runbook

1. In the navigation pane, scroll to the bottom and select **Help**
2.
3. Help window will appear as a pop-up.



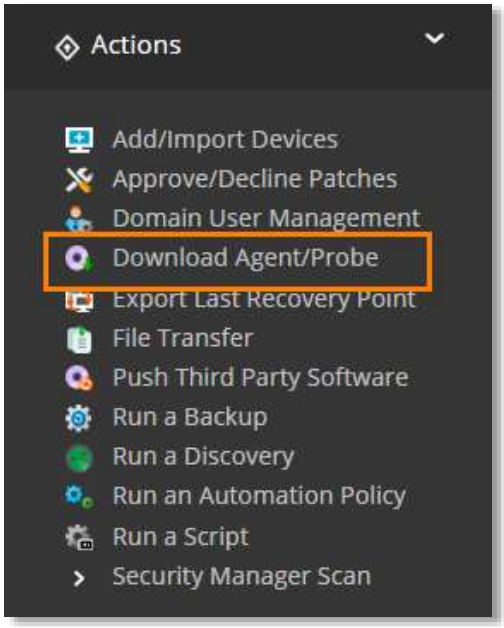
Accessing the Training Videos

The training videos in the Runbook are a great source of information on subjects ranging from Basics and Initial Setup to Patch Management and additional daily admin tasks. Most questions can be answered by reviewing the videos.



Probe and Agent Management

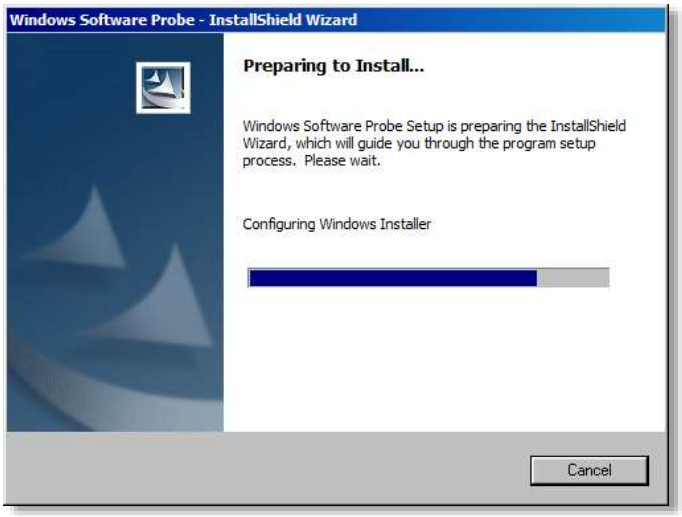
In order to monitor networks or workstations, you must install probes (for networks) and agents (workstations and mobile devices). RMM uses Windows probes and agents to monitor the status of services on your devices. The probes monitor WMI, ICMP, SNMP, syslog and TCP/IP services as well as run discovery jobs. They can either be installed while adding devices or downloading the probe directly through a wizard.

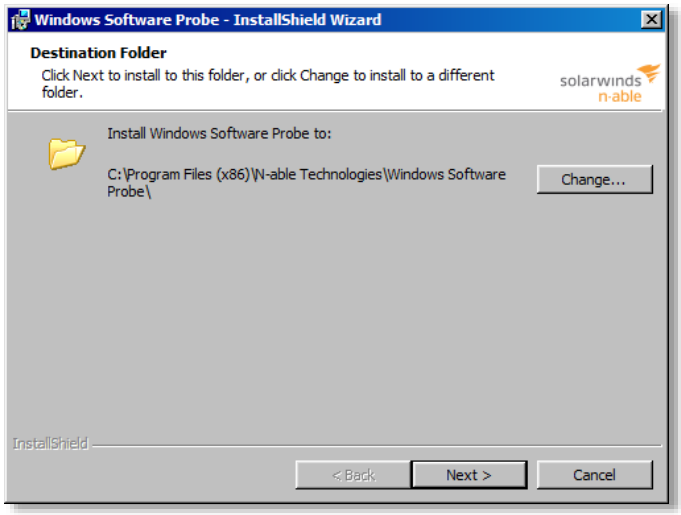


Installing a Windows Probe

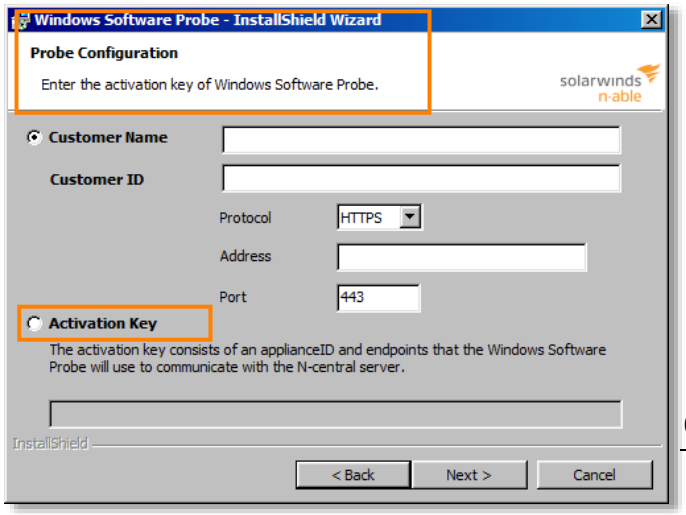
1. Select the **Download Agent/Probe** link under the **Actions** menu in your navigation pane.
2. There are two options available for your probe installation
    a. For customer or site specific installation software select the **Windows Probe** link in the **Customer Specific Software** section
    b. For generic system installation software, select the **System Software** tab than the **Windows Probe** link under **Windows Software**.

3. Selecting either link will open an **InstallShield Wizard** for the Windows Probe. The first window will ask you to accept the default folder the software will be saved to, click **Next** to keep the default folder or click **Change** to select a different folder destination.





4. You have two options for configuration:
   a. **Configure Customer** or **Site Information** - Select **Customer Name** and enter the name and the **Customer ID**.
   b. **Activation Key** – This is to install the generic probe software option. The key is generated by N-Central and can be found on the Probes screen with a key icon, and on the System Communication tab when you edit a probe. Select **Activation Key** and paste the key in the blank field.



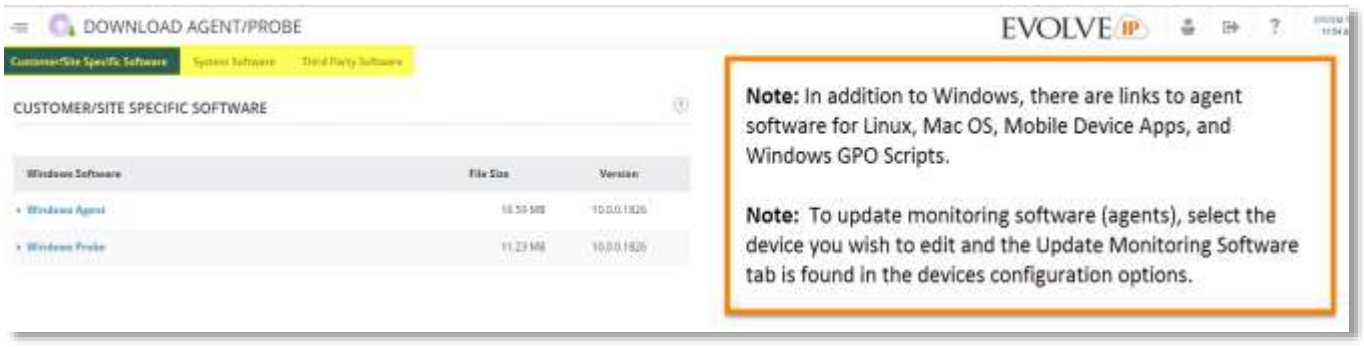
5. Click **Next.** Select an option in the credentials screen.
    a. **Local User** – Probe won't monitor remote WMI services or run asset-discovery tasks but will be able to monitor local WMI services and SNMP services
    b. **Domain User** – Specify the Domain, Username and password of the user account that will access the probe.
    c. **Workgroup User** – Specify the Username, Password of the user account that will access the probe. It need to be the same username/password of the devices that will be monitored in that work group. If the credentials don't match the probe will not be able to monitor the device properly.
6. After entering in your configurations, select **Next**.
7. Select **Install** and the **Windows Probe** setup wizard will appear after the installation. Select **Finish.**

Installing an Agent

In order to discover and import workstation devices, agents are installed so it can be monitored through the RMM portal. There are several ways to install an agent and they are compatible with multiple operating systems. For a list of supported operating systems, refer to the Help menu found on the bottom of the navigation menu.

Windows Agents

1. Go to **Actions > Download Agent/Probe Software.**
2. There are software options you can select:
    - For customer-specific installation software, click **Windows Agent** [Customer name] in the **Customer Specific Software** section.
    - For generic system installation software, click **Windows Agent** in the **System Software section.**
3. A window for the InstallShield Wizard will appear, click **Next.**
4. In the **Ready to Install** screen, click **Install.** After the agent is installed, click **Finish.**



Updating Monitoring Software - Manually

1. Select **All Devices** in the navigation page. Select the devices you wish to update.
2. Click **Update Monitoring Software.** In the **Update Monitoring Software** box, select **Upgrade Agent**.
    a. Update Actions include:
        i. **No Change** – the software is not updated at this time
        ii. **Always** –the software is always updated whenever new versions are available.
        iii. **Now** – the software is updated immediately.
        iv. **Never** – the software is not updated.

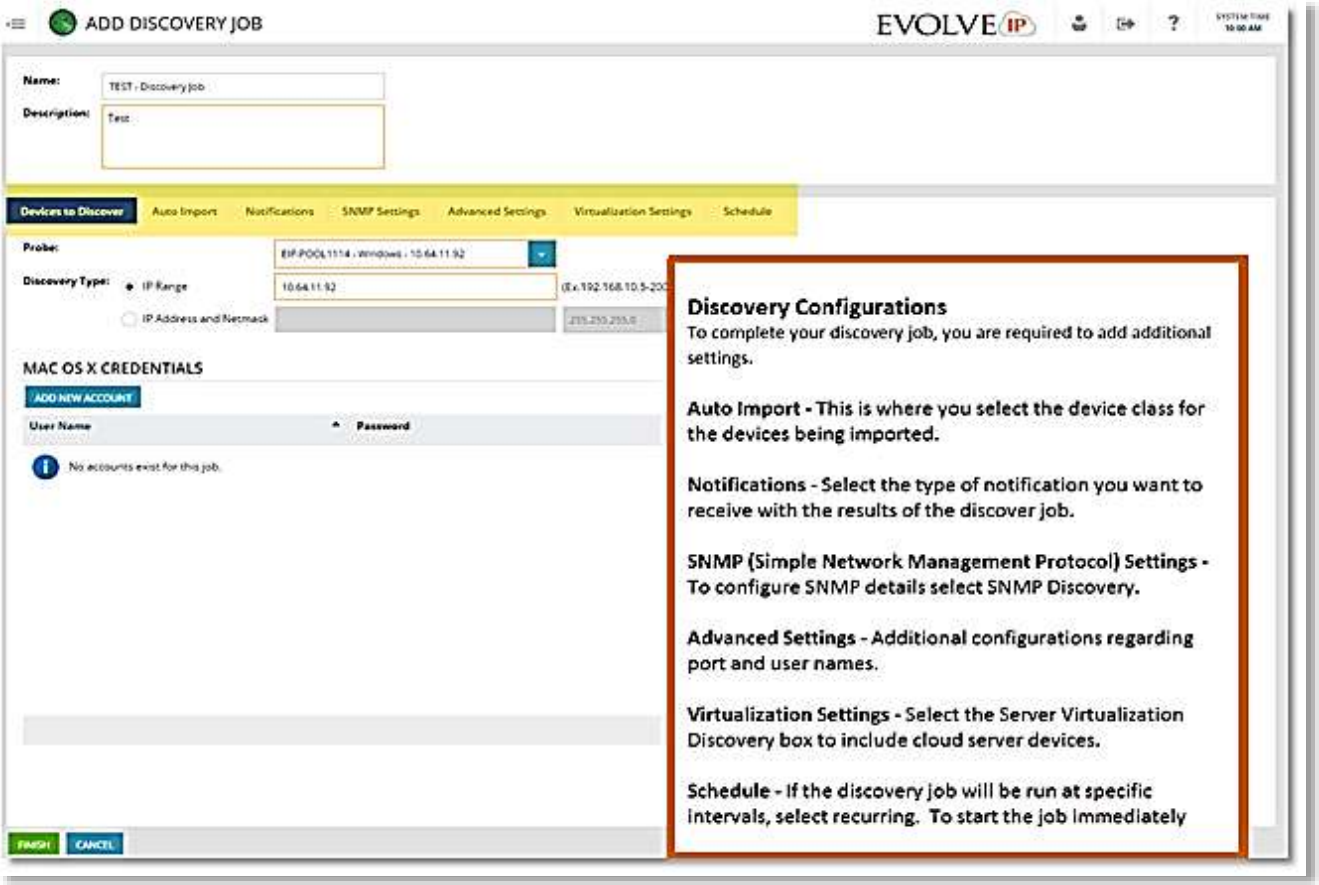
3. Click **Save.**

Best Practices

- **GPO's**: set GPO's using OU's in AD at the 'desktop level'. This will ensure that the entire environment isn't affected. This allows exception to RDP, Ping, and allows file and folder sharing.
- Do not upgrade all Windows Agents and Probes simultaneously. This may cause heavy traffic.

Running a Discovery Job

RMM's Discovery job feature is used to scan the network and locate devices. Once devices are located, they can be imported into RMM for monitoring. Asset discovery allows you to designate which devices can be ignored and which can be deleted.



Running a Discovery

1. Jump to **Navigation > Actions > Run a Discovery.** This will take you to the **Add Discovery Job** screen.
2. Type a name and other details to identify the new job. For specific information on the Additional Configurations and their purpose, refer to the Discover Job section in the Runbook found in the Help Menu.
3. Select **Finish.**

Importing Discovered Devices

Once devices are discovered, you will be able to run edit details, ignore and delete on these devices. There are two options for importing: global import or deploying a single asset-discovery job.

Asset Discovery – Global Import

1. Go to **Navigation > Configuration > Discovery Jobs**.
2. In the Discovery Jobs screen, click **Import Assets** for a global import of all devices located by all asset-discovery jobs.
3. Select the check boxes next to the devices that you would like to import or manage. To import the device, click **Import.** In the Import Devices dialog box, click **OK.** Click **Finish.**

Best Practices

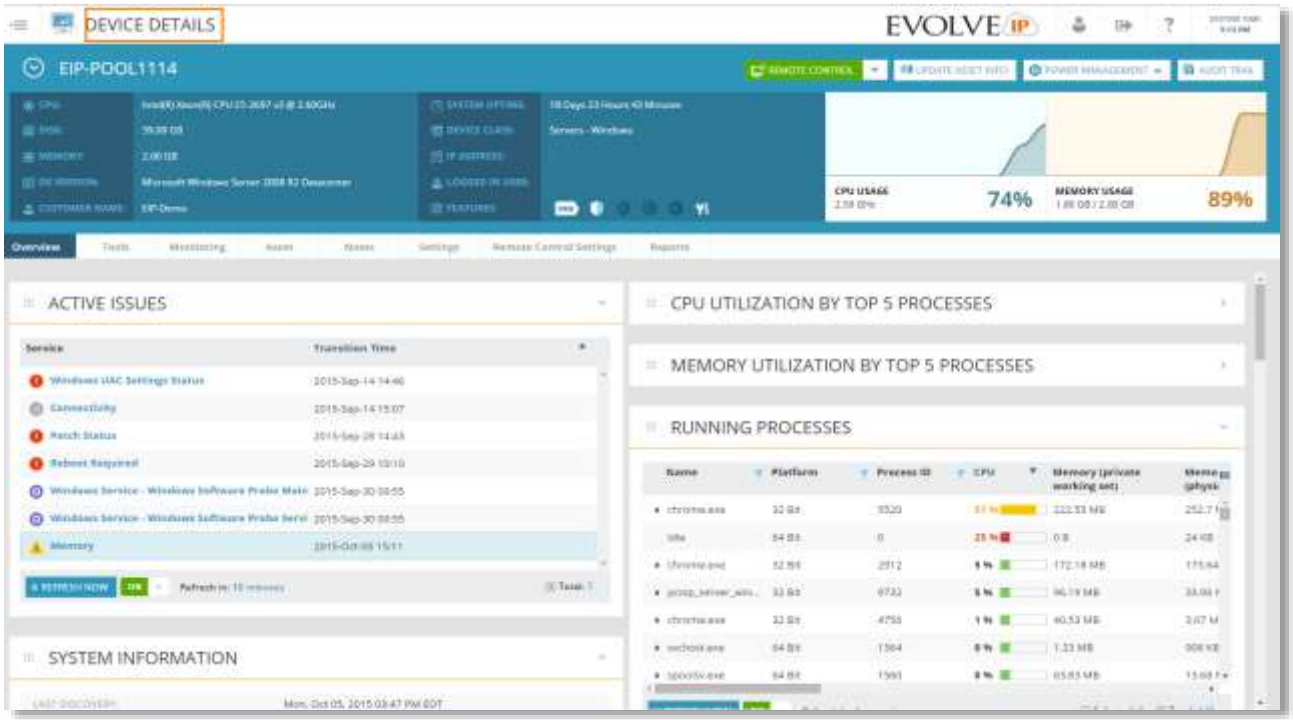
- Discovery jobs cause processor utilization spikes and is best scheduled during after-hours in order to avoid affecting an organizations running environment.

Device Details Page

RMM provides valuable information on your imported devices and this can be found by selecting your device and viewing the details within the tab.

What can I find in device details?

Overview: System info, Active Issues, CPU and Memory Utilization
Tools: Services, Processers, Applications, Printers, Command Prompt, File System and Automation Policies.
Monitoring: Agent Status, Connectivity, Patch Statuses etc...
Asset: Make and Model Numbers, Serial Numbers, Processer information.
Settings: Device name, OS, Class
Remote Control Settings: Set the remote connection type
Reports

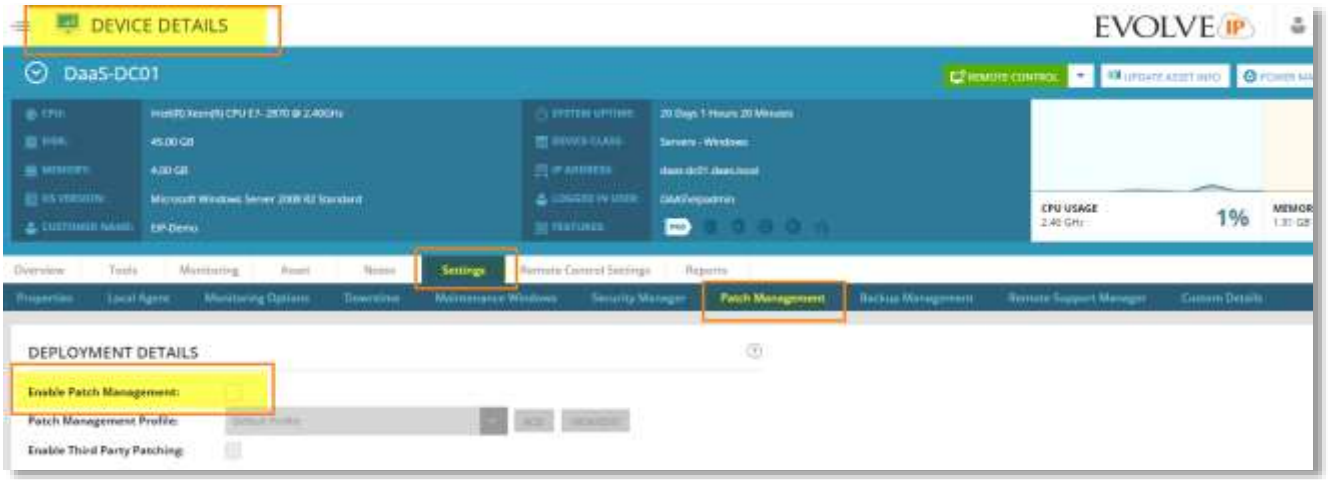


Patch Management

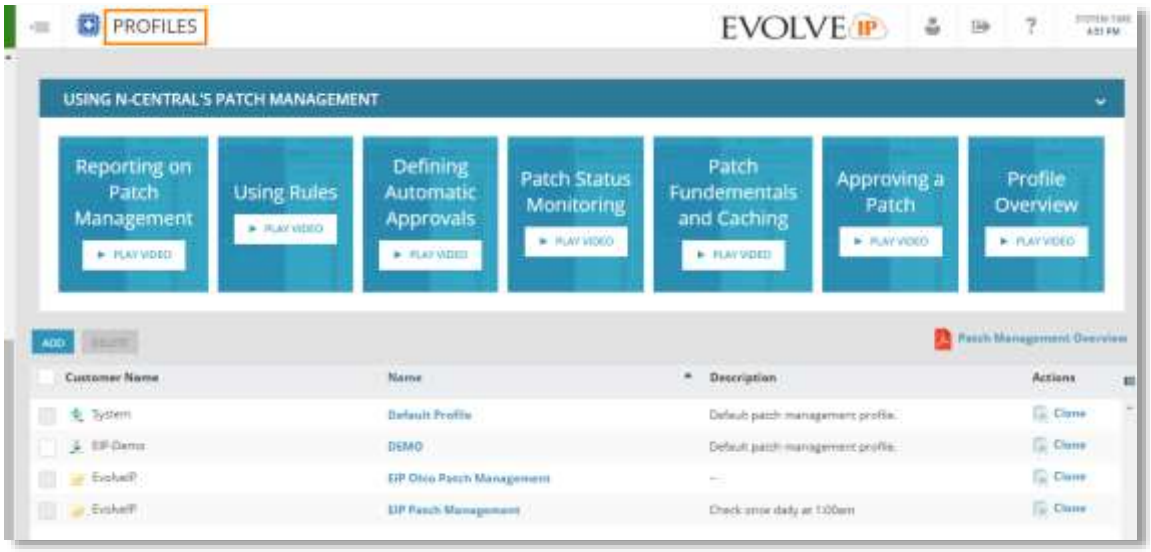
RMM's Patch Management module makes it easy to organize patch management functions. You can monitor patches, manage patches for third party software and Microsoft windows.

Editing devices for Patch Management

1. Go to the **All Devices** view screen, select the device using the check box and click **Edit.**
2. On the Device Details screen, select **Settings** then **Patch Management** below. Select **Enable.** Click **OK.**



Adding and Enabling a Patch Management Profile



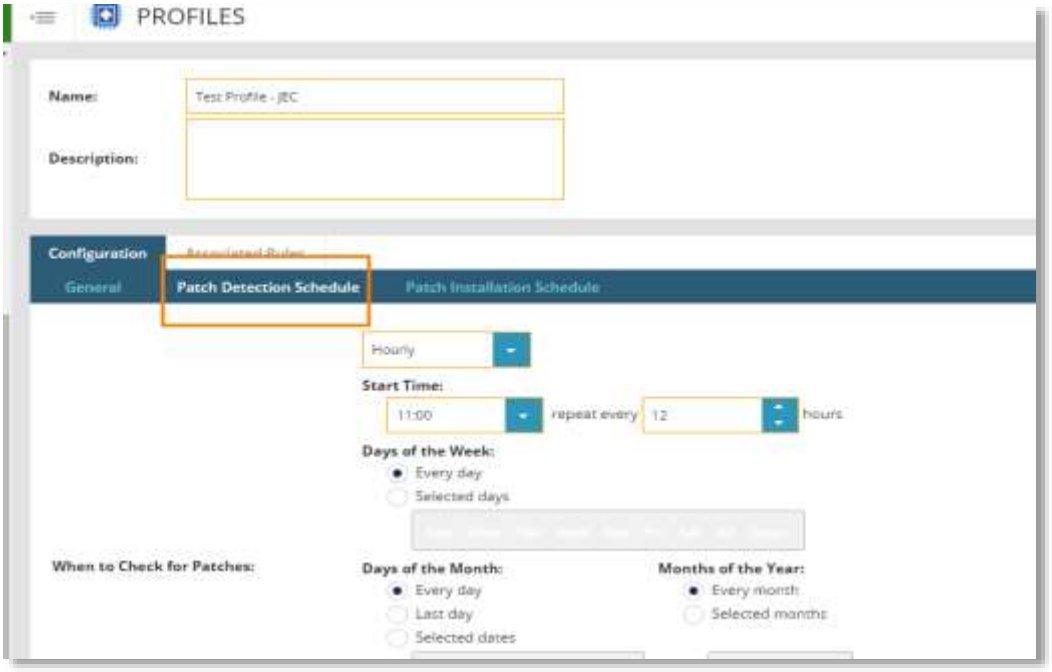
1. Under Configuration, select **Patch Management>Profiles**.
2. On the Profiles screen select **Add.** Define the profile settings as required. Click **Save.**

Patch Management Profile Configurations

Patch management Profiles have a number of different properties that will affect how patches will be automatically deployed. Below is a brief description of the General settings for profiles.

- **Property** – Configures the pop-up windows for the Windows agents. You have to options to display them, not display them or have them only displayed for admins.
- **Show Messages to Admins/Users/Before the Patch is scheduled to be installed** – all of these configurations are additional options for who will see message pop-ups.
- **Communicate with Windows Update if the Windows Probe is Inaccessible** – Configures the agent on the device to download software patches directly from Windows Update if it is unable to connect to the Windows Probe. Usually used if the device to be updated is in a different location.
- **Wait (minutes) before communicating with Windows Update** – Set a time interval before the Agent will attempt to download patches from Windows.
- **Download and wait for Scheduled Installation –** the profile will be able to download the update immediately but will only install based on the configured schedule.
- **Automatically wake up system for patch install –** if a device is asleep it will power on the machine to install the software updates.

Patch Detection Schedule

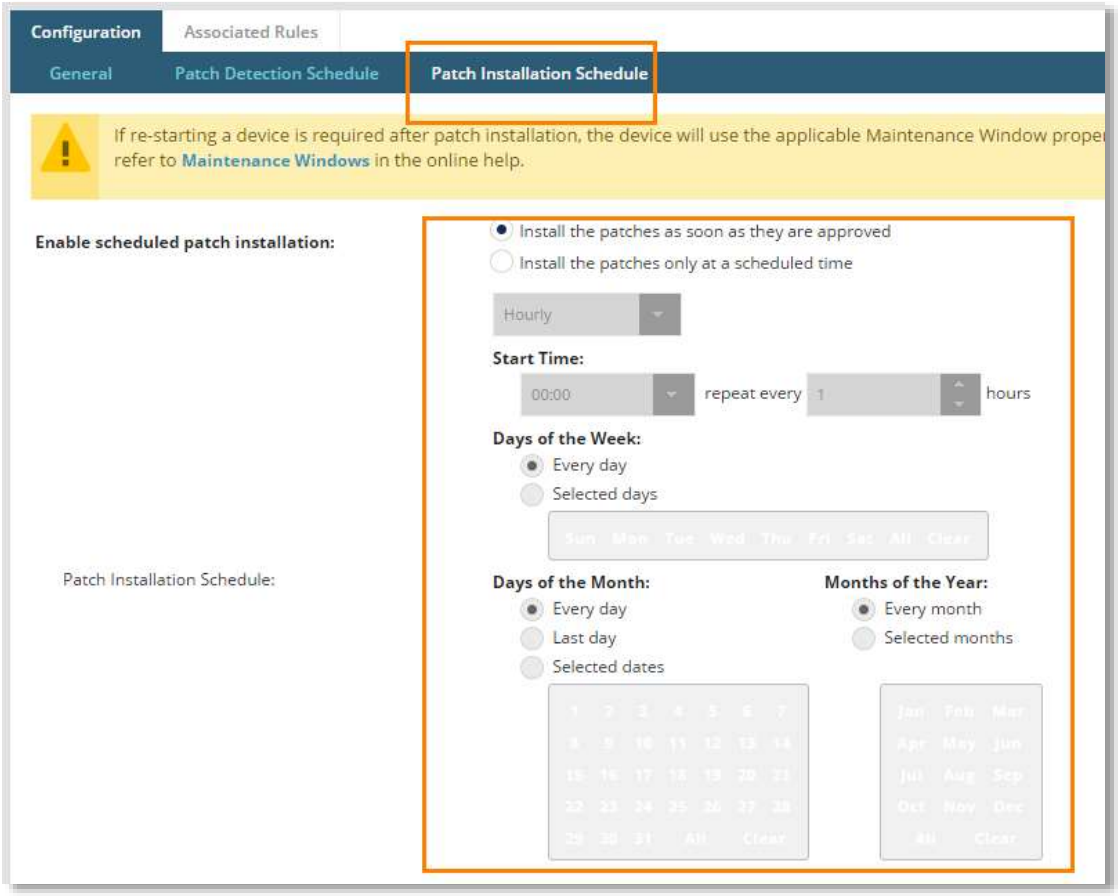


This allows you to detect what can be installed and report the information back to your RMM portal. You will be able to identify how often you want the device to communicate with Window Update or another 3rd party vendor.

1. Select the **Patch Detection Schedule** Tab.
2. Configure how often the patches need to be run, days of the week and month. Select **Save.**

Patch Installation Schedule

This feature allows you to specify when to install patches in the system, after the patches already are already detected.



1. Select the **Patch Installation Schedule** tab and select one of the installation options below:
    a. Install patches as soon as they're approved or,
    b. Install patches at a specific time
2. Configure the time, hour and monthly preferences. As well as start time, days of week and month and the months out of the year.
3. Click **Save**

Approving and Declining Patches

1. The **Approve/Decline Patches** menu is found under Patch Management.
2. Select either patches **By Device** or **By Patch.**
3. If By Device was selected, select your Devices. Click **Next**
4. Select **Perform Action Immediately** to have the patches deployed immediately.
5. In the New Approval column, select the pencil icon or right-click the current approval property to select the new approval property. Click **Next.**
6. In the EULA column, click **Read** to review the End User License Agreements for applicable software patches.
7. When the EULA is displayed, click **Accept or Decline** in the dialog box to indicate acceptance or refusal of the agreement.
8. Click **Next.** Review the list of approvals to confirm that the configuration is correct.
9. Click **Finish** in the Confirmation screen.

The status of each patch will be a combination of the individual status values of that patch across all applicable devices. The combined status value can be one of the following
(listed in order of importance):

- Failed
- Needed
- Installed
- Not Needed

Best Practices

- Patch management requires at least 20 gb free spaces.
- For patch detections, it's highly suggested to schedule them on Wednesday after 12AM. This will detect any Windows Updates that are released the day before.
- For patch installations, it's recommended to schedule them on Thursday to ensure there is enough time to approve/reject patches that may cause issues.
- Schedule Patch updates on Wednesdays at 12:00AM after Windows updates are released.
- Disable any GPO's that configure Windows Updates as they will conflict with the RMM settings.

Maintenance Windows

Devices with agents installed can be automatically configured to finish tasks set to a defined scheduled.

Creating a new Schedule Maintenance Window

1. Go to **All Devices** view in the navigation pane.
2. Perform one of the following:
    a. To configure an individual device, click the **Name** of the device, than **Settings>Maintenance Windows**
    b. To configure multiple devices, select the check box beside each of the device names you want to configure and click **Edit and scroll down to the Maintenance Windows.**
3. On the **Maintenance Windows** tab. Click **Add.** Then **c**lick **Scheduled Maintenance**. Type a descriptive name to identify the Scheduled Maintenance window.
4. Select the specific features you want to include in the schedule.

5. Select **Place device in Downtime during Reboot** so the device is down while it's being restarted. You are also able to select the amount of time to bring the device out of downtime after a restart – default time is 3 hours if the user isn't trying to use the device.
6. For the **Reboot Message,** select a **Default** or **Custom** warning message to show the user.
7. Select the **Action for the device,** either immediately or during the scheduled time.
8. After configuring the custom or monthly schedule times, click **Save.**

Schedule a Reboot Window

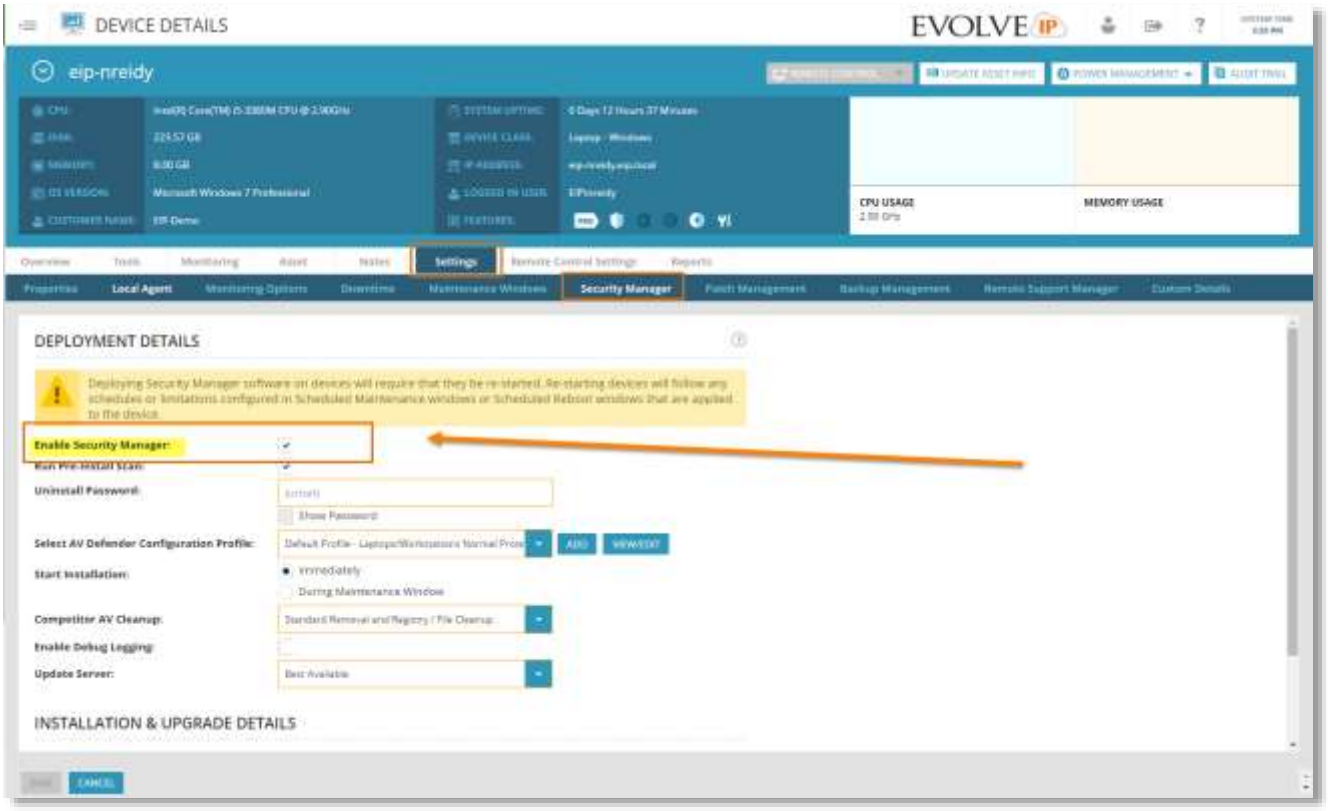
1. Go to **All Devices** and select either one device or a number of devices.
2. On the **Maintenance Windows** tab, click **Add** then **Schedule Reboot.**
3. Enter the name, amount of downtime, reboot messages and type of schedule (custom or monthly)
4. Click **Save.**

AV Defender

RMM's AV Defender uses N-Able's Bitdefender® technology to provide antivirus and anti-malware protection for network and work station devices. Note: AV Defender is not supported with Evolve IP DaaS because AV is already installed on the hypervisor level.

Enabling AV Defender

1. Go to **Device Details** and select the device you wish to use AV Defender on.
2. Go to **Settings > Security Manager**, then select **Enable Security Manager.**

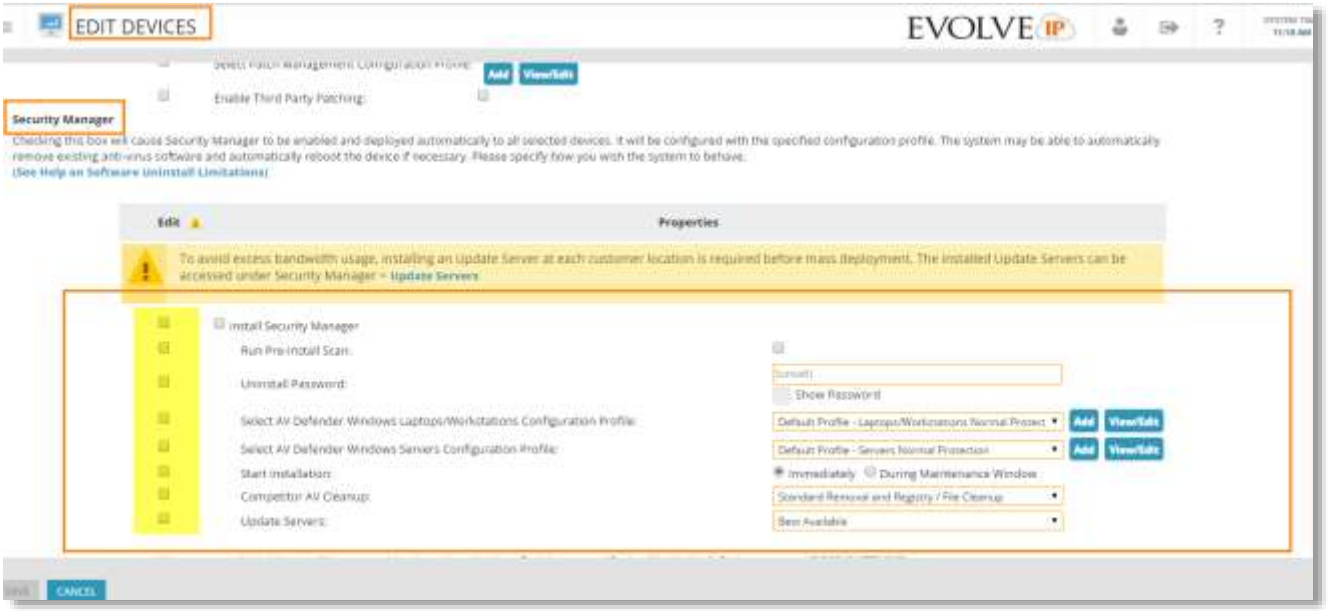


Installing on Multiple Devices

Installing AV Defender software on devices will require that they be re-started. Re-starting devices will follow any schedules or limitations configured in Scheduled Maintenance windows or Scheduled Reboot windows that are applied to the device.

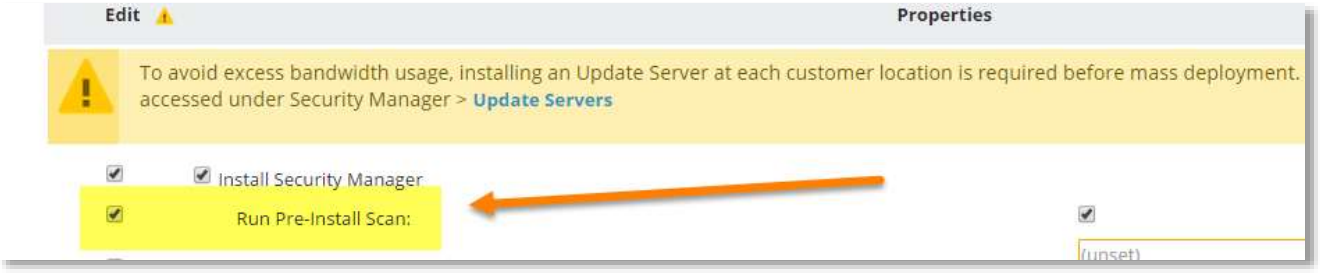
1. Go to **Navigation Menu > Views > All Devices.**
2. Select the check boxes beside each of the names of the computers to which you want to deploy AV Defender based on your deployment plan. Click **Edit.**

3. Scroll down to the **Security Manager settings.**



4. Click **Install Security Manager.**
    a. If there is no update server configured, a warning dialog box will pop up recommending you install an update server (at least 1 per customer) before deploying AV Defender to your device. Select either **Configure Update Server** or **Continue without Update Server** as appropriate and click **Save.**
    b. If you selected **Configure Update Server**, you will need to complete the update server configuration process before installing AV Defender on devices. For more information, refer to Update Servers in the Runbook.

5. Select **Run Pre-Install Scan** to perform a security scan of the device before installing AV Defender software.

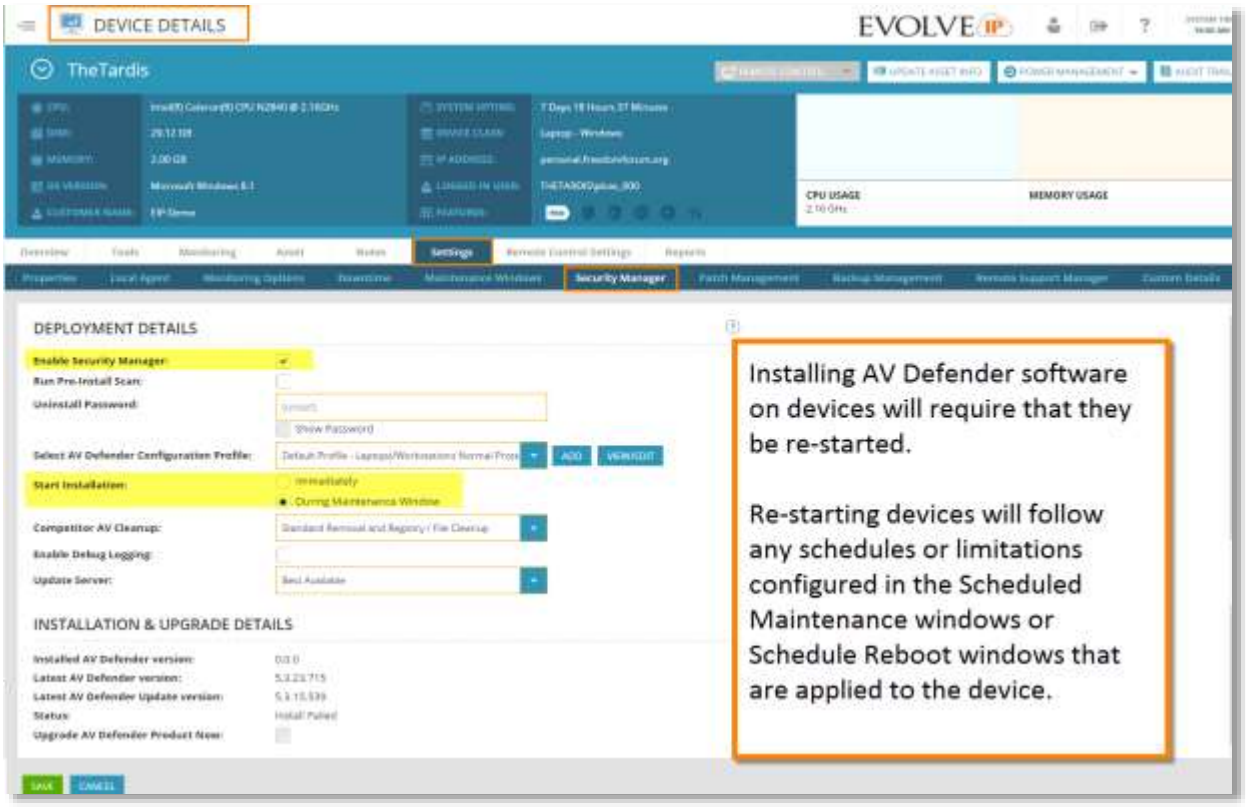


6. Type the **Uninstall Password** to provide security credentials required to remove any existing security software from the device. Select **Show Password** to display the password as it is typed.
7. Select the appropriate Profile to be applied to the devices from one of the following drop-down menus:
    a. Select AV Defender Windows Laptops/Workstations Configuration Profile
    b. Select AV Defender Windows Servers Configuration Profile
8. Under **Start Installation**, select either **Immediately** or **During Maintenance Window** depending on which is appropriate.

9. From the **Competitor AV Cleanup** drop-down menu, select the action that you want AV Defender to take with existing security software from one of the following:
    a. No Removal
    b. Standard Removal
    c. Standard Removal and Registry/File Cleanup

10. Click **Save.**

Deploying to a Single Device

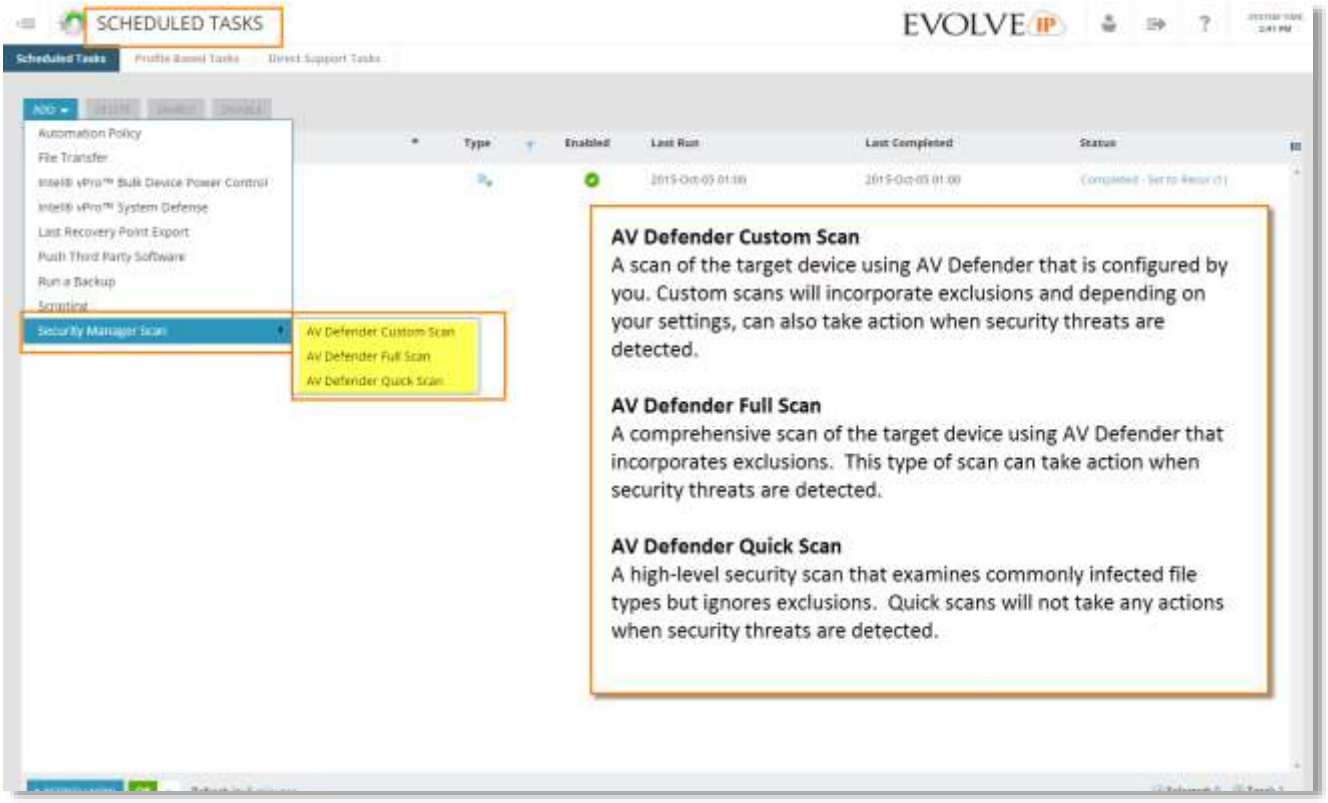


1. Click **All Devices** view in the navigation pane. Select the **Network Devices** tab.
2. Click the name of the computer to which you want to deploy AV Defender based on your deployment plan. Click **Settings**.
3. Click **Security Manager**. Configure the Security Manager properties as required. For more information, refer to Security Manager section in the Runbook.
4. Click **Save**.

Scheduling a Security Manager Scan Task

There are different types of security scans that can be performed on selected devices.

1. In the navigation pane, go to **Configuration > Scheduled Tasks > Add/Delete**. This feature may also be accessed through the **Actions** menu.
2. Click **Add** in the **Scheduled Tasks** screen. Select **Security Manager Scan** from the Scheduled Task Type list.
3. Select the type of scan task to be created from one of the following:
    a. AV Defender Custom Scan
    b. AV Defender Full Scan
    c. AV Defender Quick Scan
4. Type a descriptive **Task Name** by which to identify the task.
5. Configure the task properties as required. Click **Save.**

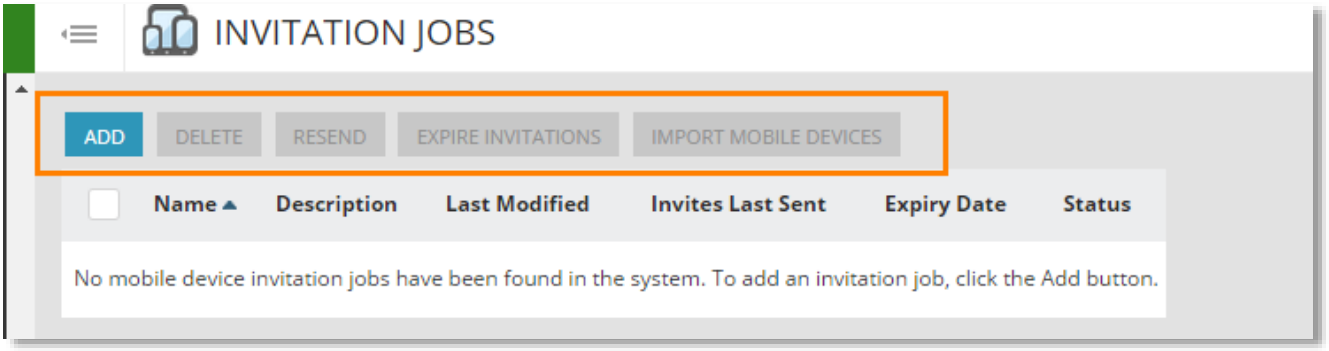


Best Practices

- Devices on which the AV Defender software is to be installed must have a minimum of 1 GB of free disk space.
- Devises that are to be configured as AV Defenders Servers must have a minimum of an additional 6 GB of free disk space.
- Steps to deploy AV Defender

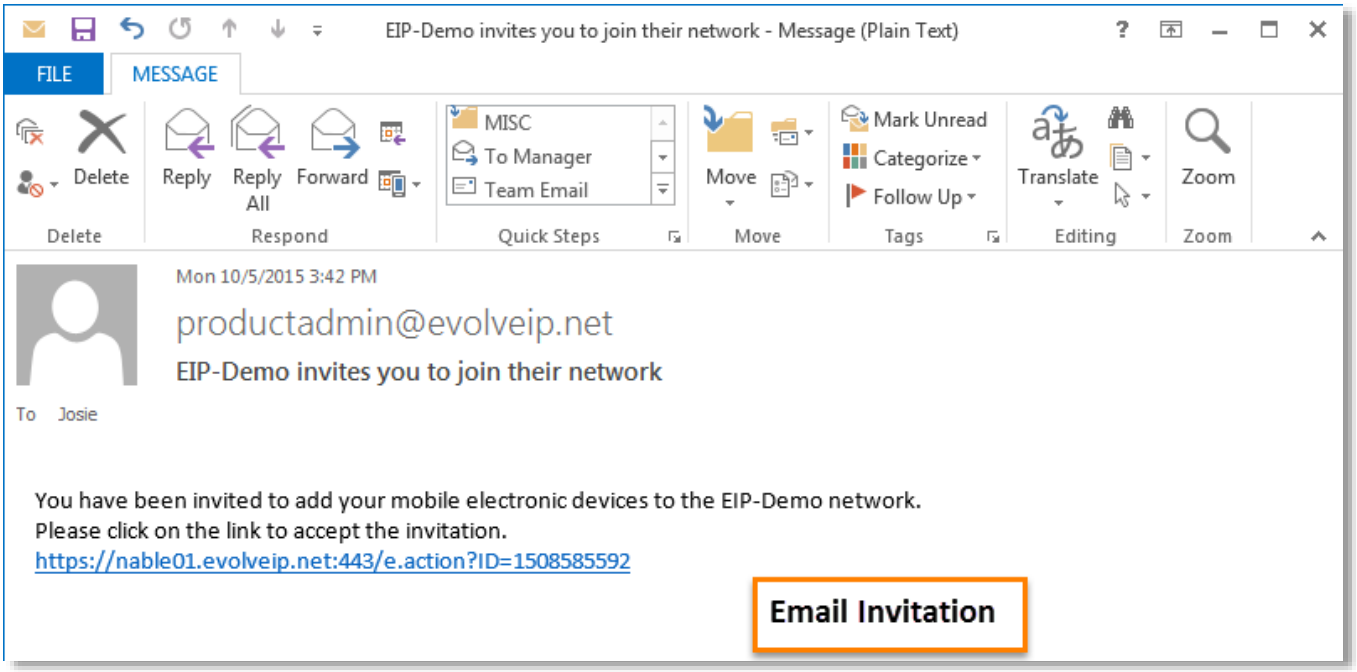
Mobile Device Management (MDM)

Registration invitations can be sent directly to the mobile device from the RMM platform. Once the mobile user is registered, the device can be monitored.



Sending a registration Invitation

1. Under the **Mobile** Devices tab (from Devices page) select the Invitation **link** and then **Add.**
2. Select **Text or Email.** You can also select both.
3. If a warning dialog box is displayed explaining requirements for managing mobile devices, click **OK.**
4. Enter a name and a description of the invitation.
5. Select **Save.** The user will than receive a link to install the agent and register the device.



Requirements for Mobile Device Management

- iOS 6.1x and later
- Android 2.2x and later
- For iOS devices, there must be an Apple Push Notification Service (APNS) certificate to work effectively on any Apple device. This can be found on https://appleid.apple.com.