Installing and Managing Avast AV

https://campus.barracuda.com/doc/93199706/

One of the most common questions the support team receives is how to mitigate issues deploying Integrated Avast Antivirus through Barracuda RMM. This article is intended to attempt to serve as a first step in resolving issues with your AV deployment. Much of what is developed for this Knowledge Base article is a combination of documentation from the User Guide, expertise within Barracuda RMM from the support team, knowledge from the Avast support team, and finally from the valuable feedback from our Partners. By the time you get through this article, you should have a better understanding of how Avast Antivirus works within Barracuda RMM and will be armed with basic tools to move on to troubleshooting the problems you might run into.

What is required to Install and Monitor Avast Antivirus?

The basics of what should be required to install Integrated Avast Antivirus through Barracuda RMM is covered in the user guide. That said, there are key additional steps that need to be considered. This also assumes that any previous or conflicting Antivirus solutions were uninstalled and cleared out. While Avast Antivirus attempts to do this automatically, it is also recommended to do this prior to installing a new Antivirus solution.

- **Exception for Geo-blocking**: because Avast is based in the Czech Republic, services from that country will need to have no geo-blocking interference
- The following need to be allowed through your firewall
  - *.avast.com
  - *.avcdn.net
  - *.mailshell.net (only if using Anti-Spam)
- **Port Forwarding**: 7206 and 7207 are used devices for the Onsite Manager / Service Center to communicate through for Integrated Avast deployments
- **TLS 1.2 must be enabled on the Onsite Manager** in order to push out Avast Antivirus
- Do not use special characters for accent (ie. umlaut) in device names

After this, you can set up the policies to deploy, maintain, and monitor Avast Antivirus. These are found here:

For Deployment and Maintaining

1. Click on **Configuration**.
2. Select **Policies**.
3. From the dropdown, click on **Avast Antivirus**.

From here you can set up your policy and can associate this to a service, groups, or apply directly to the devices as you see fit.

For Monitoring

1. Click on **Configuration**
2. Select **Policies**
3. From the dropdown, click on **Monitoring**
4. Find the **Avast Business Antivirus Monitoring Policy**

As above, you can associate this to a service, groups, or apply directly to the devices you wish to monitor.

There are a lot of different settings in the Avast Antivirus Policy and the Avast Business Antivirus Monitoring Policy that you might want to familiarize yourself with.

Manually Deploying Avast Antivirus

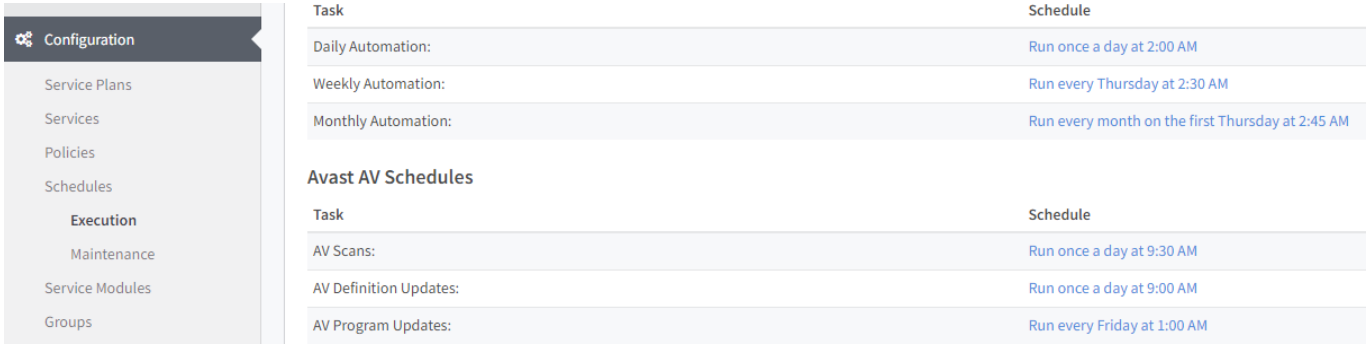
1. Click on **Antivirus**.
2. Select **Avast Antivirus**.
3. Then on the right hand, select **Deployment**.
4. Select the **Devices Needing Antivirus Installation**.
5. Now check the devices you wish to deploy Avast Antivirus on and then Install.

The Barracuda RMM team has noted that occasionally devices fail to install while pending the policy server. We believe the stub installer is bottlenecking on the installation. In these cases, we have developed Use Full Avast AV Installer Script Package to be deployed against Onsite Managers and Device Managers to bypass the stub installer. To learn more about script package importing, see the Export and Import Automated Tasks article.

Setting up an Execution Schedule

1. Click on **Configuration**.
2. Select **Schedules**.
3. From the dropdown, click **Execution**.
4. Select or create a new schedule.

The execution schedule includes when **AV Scans**, **AV Definition Updates** and **AV Program Updates** all occur. The devices should be on, accessible, and not in heavy use to ensure the smooth operation of these automated tasks.



Again, this needs to be applied to the service, groups or applied directly to the devices you wish to work on the schedule.

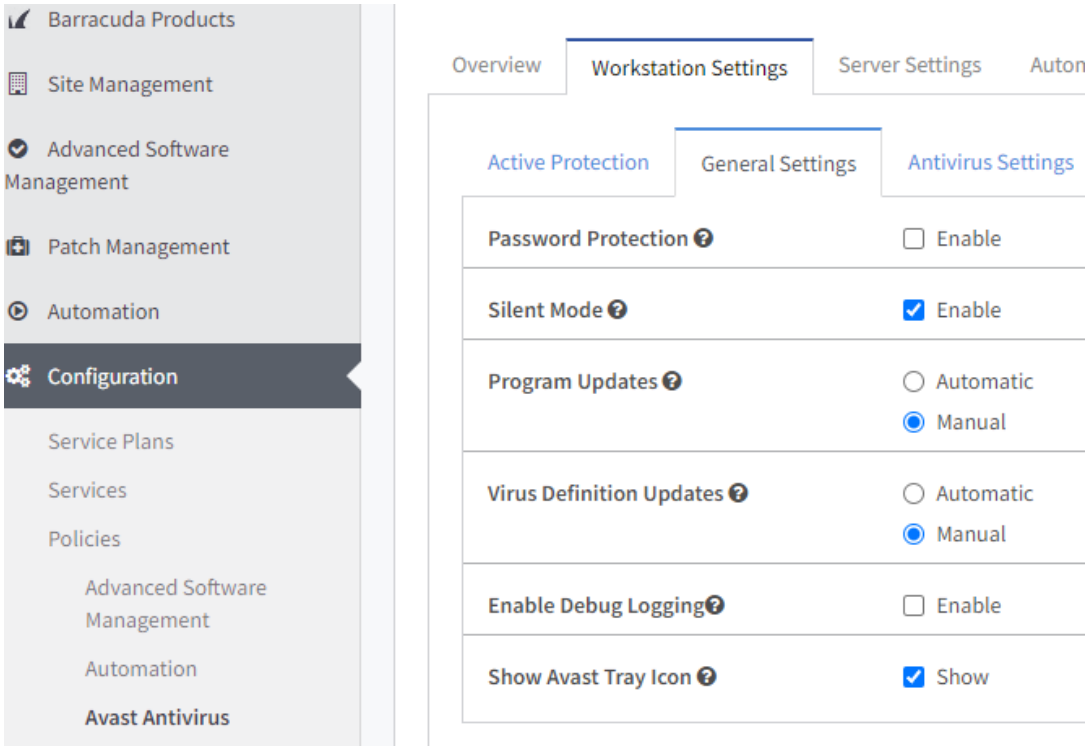
*If these are mobile devices, they should be on **Private Network Profiles** and not Public to both ensure installation and connection to the Avast policy servers occur.*

How does Avast Antivirus Update with Barracuda RMM?

Assuming that the above was done, Integrated Avast Antivirus is set up to deploy, be monitored, and managed within Barracuda RMM, but how does it scan and update? The Execution Schedule is now informed by how the Avast Antivirus Policy is set up. Follow the below to see if your environment is set up to Automatically or Manually update:

1. Click **Configuration**.
2. Select **Policies**.
3. From the dropdown, click **Avast Antivirus**.
4. Now choose the **Antivirus policy** that is set up for the devices.
5. Click on either **Workstation Settings** or **Server Settings**.
6. Now go to **General Settings**.
7. Observe the **Program and Virus Definition Updates** as the following:

- **Automatic**: if selected, Avast Antivirus will self-manage according to how Avast determines its update schedule.
- **Manual**: if selected, the Execution Schedule in Barracuda RMM will take over the management.



For common troubleshooting issues with Integrated Avast Antivirus in Barracuda RMM, see this article.

Figures

1. image2022-2-15 15:27:29.png
2. image2022-2-15 15:23:50.png