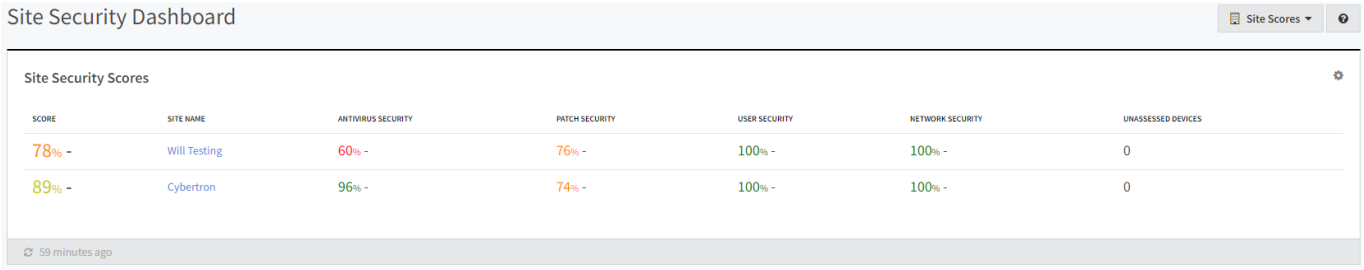
Understanding the Site Security Dashboard

https://campus.barracuda.com/doc/98209787/

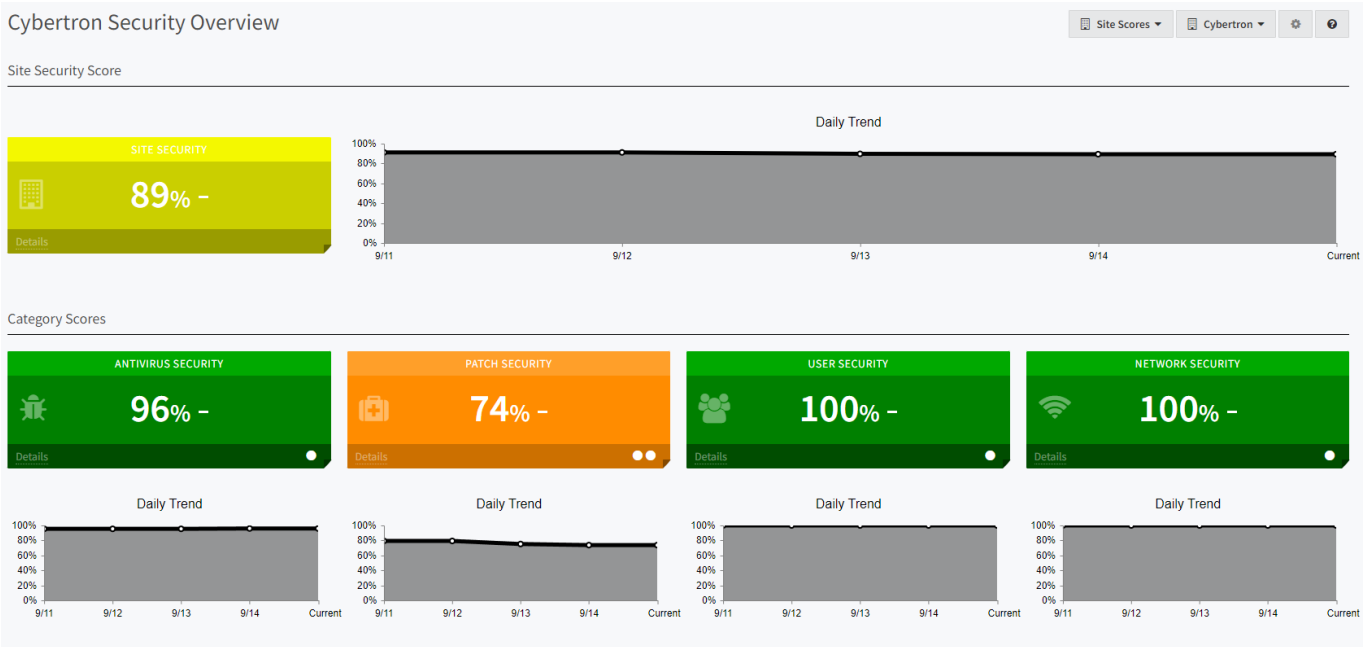
In Barracuda RMM, you can access the Site Security Dashboard to get an overview of **Antivirus Security**, **Patching Security**, **User Security** and **Network Security**. Please see the below image of an environment from one of our support team staff members.

To access your Site Security Dashboard

- Click on **Dashboards**
- Select **Site Security Dashboard**
- The following is an overview of all sites with a Site Security Schema applied



- Click the **hotlink of a Site Name** to open up an expanded view

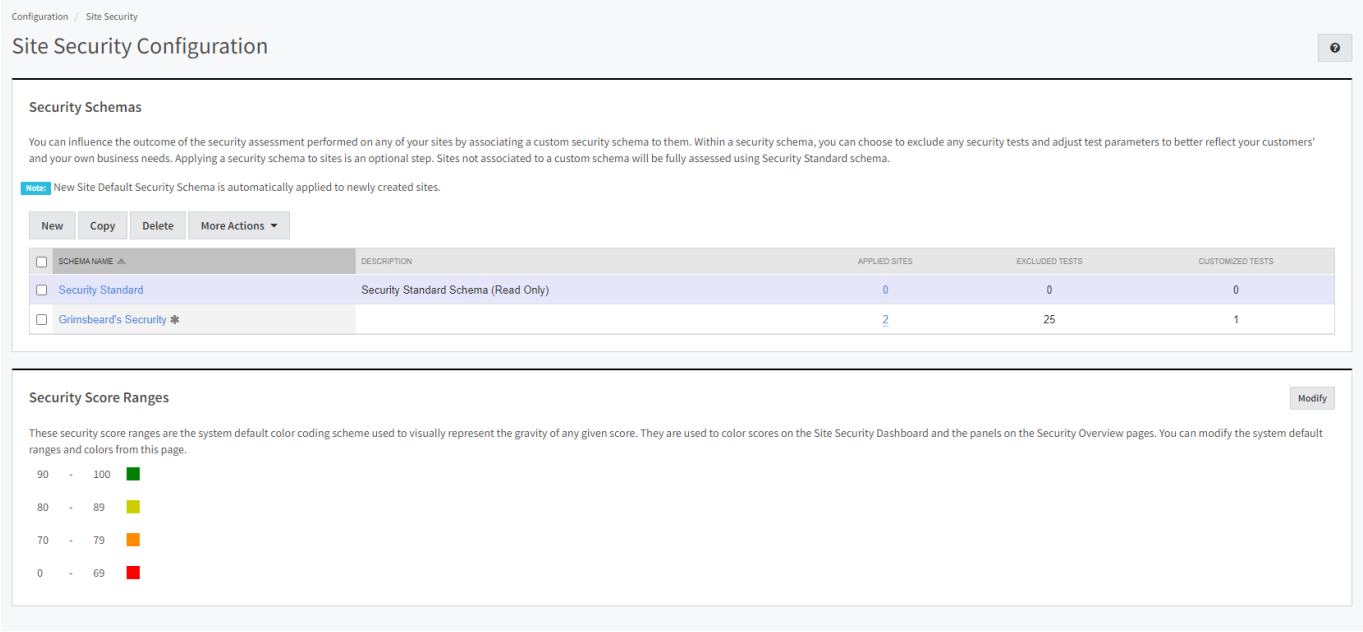


About Site Security Schemas

The data collected here come from a Site Security Schema and will provide a breakdown of issues on a given site to which the schema is applied. The Site Security Schema you can apply to a site will provide an overall glance at issues, but it needs to be fine-tuned for your needs/site. However, out of the box, you will have a default Security Standard that you can apply to sites as a demonstration. It is worth noting that this default schema has all options turned off and will include all tests, which is not ideal for sites and environments long term. You will want to create your schema. As Barracuda RMM collects data about devices scanned into the dashboard overall, the schema will help you determine what issues might be associated with **Antivirus**, **Patching Security** (both Windows and Third Party), **User Security** and **Network Security**. This will be displayed on the Site Security Dashboard and is intended to get an accumulated overview of your sites so that you may use Barracuda RMM to help mitigate and address any issues.

Accessing Site Security Schemas

- Click on **Configuration**
- Select **Site Security**
- You will have this page (or similar to this page)



Creating a New Custom Site Security Schema

- From the above steps, click on **New**
- Give the Schema a Name and description
- Each drop-down for **Antivirus Security**, **Patch Security**, **User Security**, and **Network Security** contains options to toggle
- Select which options you want to turn off, as all are on by default
    - *It is worth noting on the right-hand side, you can ungroup the test names to view all tests in one single pane*
- **Add a Site to the Schema** (you may have more than one site per schema, but to tailor the needs, it is recommended to set up their own schemas as need be)
- Hit **Save**

About Patching Security Score

A frequent request to the Barracuda RMM Support team is how to understand the Patching Security Score within the Site Security Dashboard. The critical factor to consider is that the Patching Security Score is not represented as patches missing from a device according to Patch Management, but rather what the device is reporting is missing according to its inventory. Patch management is thus designed to work on updating those devices so that the Site Security Dashboard can adequately reflect. However, one of the main issues is that the Site Security Dashboard does not represent which patches are missing on which devices, only that devices report that they are missing patches. We are working with our development team to implement a change to list missing patches.

Another quick note on missing patches, often we will see both Updates Rollups (which contain language packs), Office patches and patches not offered by WSUS factoring into patch security scores. The Barracuda RMM team recommends disabling the update rollups from the Site Security Schema as a best practice, as each language pack counts in the tabulation of the score rather than simply what your device uses. Equally, for Office patches, as there is no WSUS offering for those, We have an article on Patching Stand-alone MS Office and Office 365 that links to Microsoft's write-up on the topic. Finally, if you come across a patch not found in Patch Management, it is likely not available via WSUS. If a patch is not in WSUS, it is not automatically paginated in Patch Management. By searching the Microsoft Support site, you can find out if a patch is WSUS available or not. You need the patch's KB number or the patch's name.

A Final Note on the Site Security Dashboard

Now that you have the Site Security Schema set up, the Site Security Dashboard will accumulate data over several days and update throughout the week. It is important to note that this dashboard is not a real-time tool but a weekly snapshot of many data points compiled in one location. It is also very important to note that if you are seeing lower scores than you would like, it is essential to use

Barracuda RMM (or other tools) to make adjustments and deploy fixes. The Site Security Dashboard looks at your environment, sites and devices without factoring in how you have those set up in Barracuda RMM.

Figures