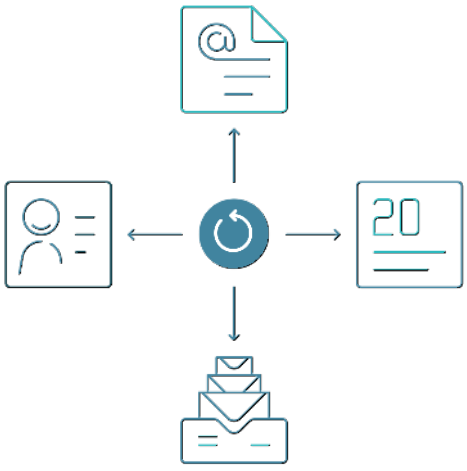
UNITRENDS SECURITY MANAGER

FREQUENTLY ASKED QUESTIONS

Unitrends Security Manager finds footholds that your anti-virus can't such as anomalous activity, suspicious changes and threats caused by misconfigurations. Unitrends Security Manager combines machine learning and intelligent tagging to detect keyloggers, trojans, spyware, unauthorized registry changes, and other malicious activity.



Unitrends Security Manager

1. **How does Unitrends Security Manager work?**

The Unitrends Security Manager process can be broken down into five steps:

- Install a single Unitrends Security Manager appliance on your network.
- Configure the appliance by activating a set of Security Policies using the security check list form. The policies turn off/on corresponding alerting. You can also take advantage of built-in templates or create your own for even easier configuration and standardization of service offerings.
- Unitrends Security Manager will run daily scans automatically and send an alert whenever it detects an unsanctioned change or threat to the network.
- For certain anomalous activity Unitrends Security Manager will send an email to you asking whether the detected issue needs to be investigated further or can be ignored.
- Your user friendly portal will offer step by step remediation suggestions for any security issue identified. Unitrends Security Manager also has integrations to all major PSA (professional services automation) software solutions if remediation requires their involvement.

Unitrends Security Manager subscribers who use ConnectWise, Autotask, or Tigerpaw as their ticketing system have the option of automatically or manually creating tickets based from alerts. Incidents showing up in the daily alert emails that require investigation can either be addressed through creating service tickets within the portal, or sending them directly to their PSA to automate the process.

2. **What are "Smart Tags"?**

Unitrends Security Manager uses 'smart tags', a feature that allows it to adapt to each unique environment. Smart Tags enrich the detection system by adding information about specific users, assets, and settings. These tags help Unitrends Security Manager gain intelligence about what it detects. Over time, the tags increase the quality of the alerts by displaying more potential threats and fewer false positives.

Examples of how you might use the Smart Tags to fine-tune Unitrends Security Manager alerts:

- Tag a computer as being "Restricted IT Admin Only." When any user logs in who hasn't been tagged as an "IT Admin", Unitrends Security Manager will send an alert.

- Tag a computer as "Locked Down," disabling changes from being made to it. If someone manages to install an application on this machine, Unitrends Security Manager will sense it and send an alert. This is one example of the way tagging removes false positives and increase the relevance of alerts.

- Tag a wireless network as a "Guest Wireless Network," alerting Unitrends Security Manager that it doesn't need to worry about new devices appearing on it. If a new device shows up on a network not tagged for guest access, Unitrends Security Manager will send an alert so you can determine the threat level.

Smart Tags can be added or modified on the fly at any time, allowing you to first see the alerts Unitrends Security Manager sends and then "tweak" the tags as needed. If you choose to ignore an alert, the system will automatically generate a new Smart Tag to prevent similar "false positives" from being generated. The more you use Unitrends Security Manager, the more it works with you to streamline your security.

3. **How do daily alerts and weekly notices keep you ahead of any internal threat?**

   Unitrends Security Manager keeps you posted of any potential internal security issues going on inside your network. Set the time for the daily scan and Unitrends Security Manager reports back with an email alert sent to any address you specify, including your own ticketing system. The daily alerts aggregate the issues that were detected during the past 24 hours and can be sorted either by priority/severity (high, medium and low) of the threat, or by the type of issue (threat, anomaly, change). There are dozens of alerts based on network changes, anomalous activity, vulnerabilities and misconfigurations..

4. **How does Unitrends Security Manager licensing work?**
   A Unitrends Security Manager subscription gets you an unlimited-use license to deploy Unitrends Security Manager at all of your sites for one, low, fixed cost per year (see license terms for details). Once deployed, Unitrends Security Manager scans a network, detects security threats, and alerts various stakeholders.

Unitrends increases uptime and confidence in a world in which IT professionals must do more with less. Unitrends leverages high-availability hardware and software engineering, cloud economics, enterprise power with consumer-grade design, and customer-obsessed support to natively provide all-in-one enterprise backup and continuity. The result is a "one throat to choke" set of offerings that allow customers to focus on their business rather than backup. Learn more by visiting unitrends.com or follow us on LinkedIn and Twitter @Unitrends.