SentinelOne Firewall Control

Firewall control allows the SOC to manage endpoint firewall settings from our SentinelOne Management Console. Use Firewall to define which network traffic is allowed in and out of endpoints.

Important to know when you enable Firewall:

- There are no default rules. All traffic is allowed if not explicitly blocked.
- The SOC does not offer any pre-built rules, all rules must be supplied by the partner.
- When SentinelOne Firewall is enabled on Windows endpoints, it becomes the active firewall. SentinelOne Firewall takes control but it does not change rules from other firewall solutions on the endpoint.
- SentinelOne will **not** inherit any existing firewall rules on the endpoint. All rules must be supplied and configured in the S1 management console.

SentinelOne Firewall Control FAQ

What happens to Windows Firewall rules if I enable SentinelOne Firewall Control?

A: When SentinelOne Firewall is enabled on Windows endpoints, it takes control over the Windows Firewall and registers as the active Firewall provider. Rules that were created directly on Windows Firewall or in GPO will become inactive, even if there are no enabled SentinelOne Firewall rules.

How does Firewall work with firewall rules from a GPO?

A: Firewall rules from GPO have the same status as Windows Firewall rules: they become inactive when the SentinelOne Firewall is enabled.

How does Firewall work with Third-Party Firewall Solutions?

A: There is a logic, managed by WFP (Windows Filtering Platform), to prioritize all firewall rules on the endpoint. This logic prioritizes all rules, those created by the SentinelOne Agent and by other firewall solutions on the endpoint. SentinelOne rules for blocking and allowing traffic, are created with highest weight allowed by WFP. If rules created by other firewall solutions have lower weight in WFP, the SentinelOne Rules will have priority.

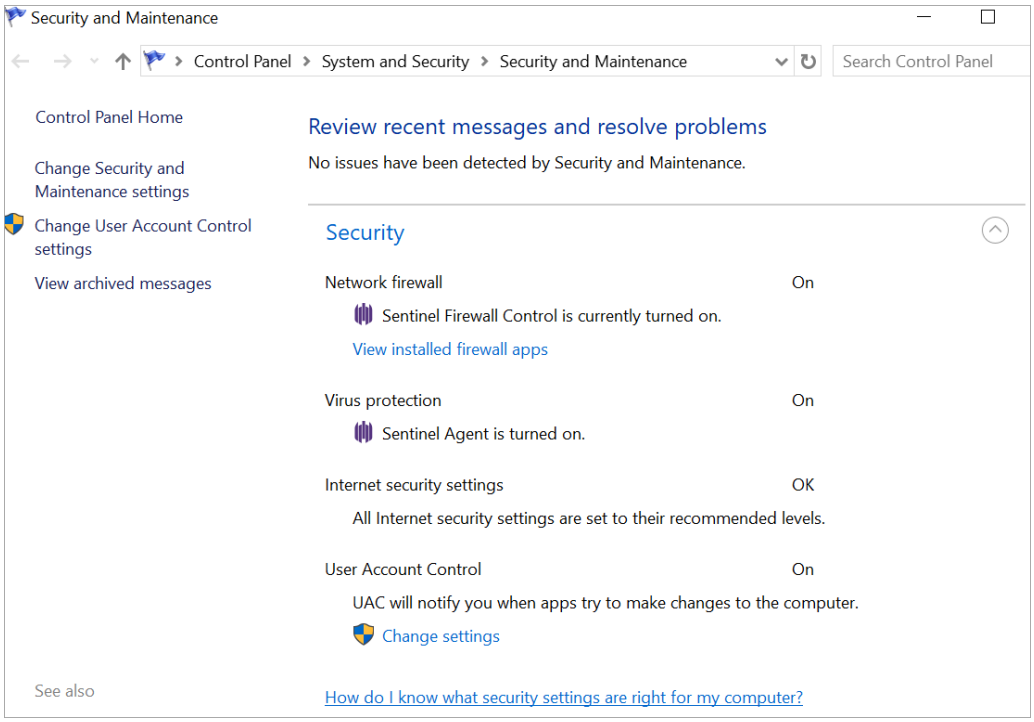
If endpoints have rules from a third-party firewall solution, these rules might not work if they contradict rules in the SentinelOne Firewall policy. This is configurable.

Firewall Control and Windows OS

In Windows Security Center, SentinelOne Firewall is registered in two Network Firewall categories:

- NET_FW_RULE_CATEGORY_FIREWALL
- NET_FW_RULE_CATEGORY_BOOT

The SentinelOne EPP registers as Virus protection.



SentinelOne Firewall does not register in these categories:

- NET_FW_RULE_CATEGORY_STEALTH
- NET_FW_RULE_CATEGORY_CONSEC

Windows Firewall can be registered in the other two categories.