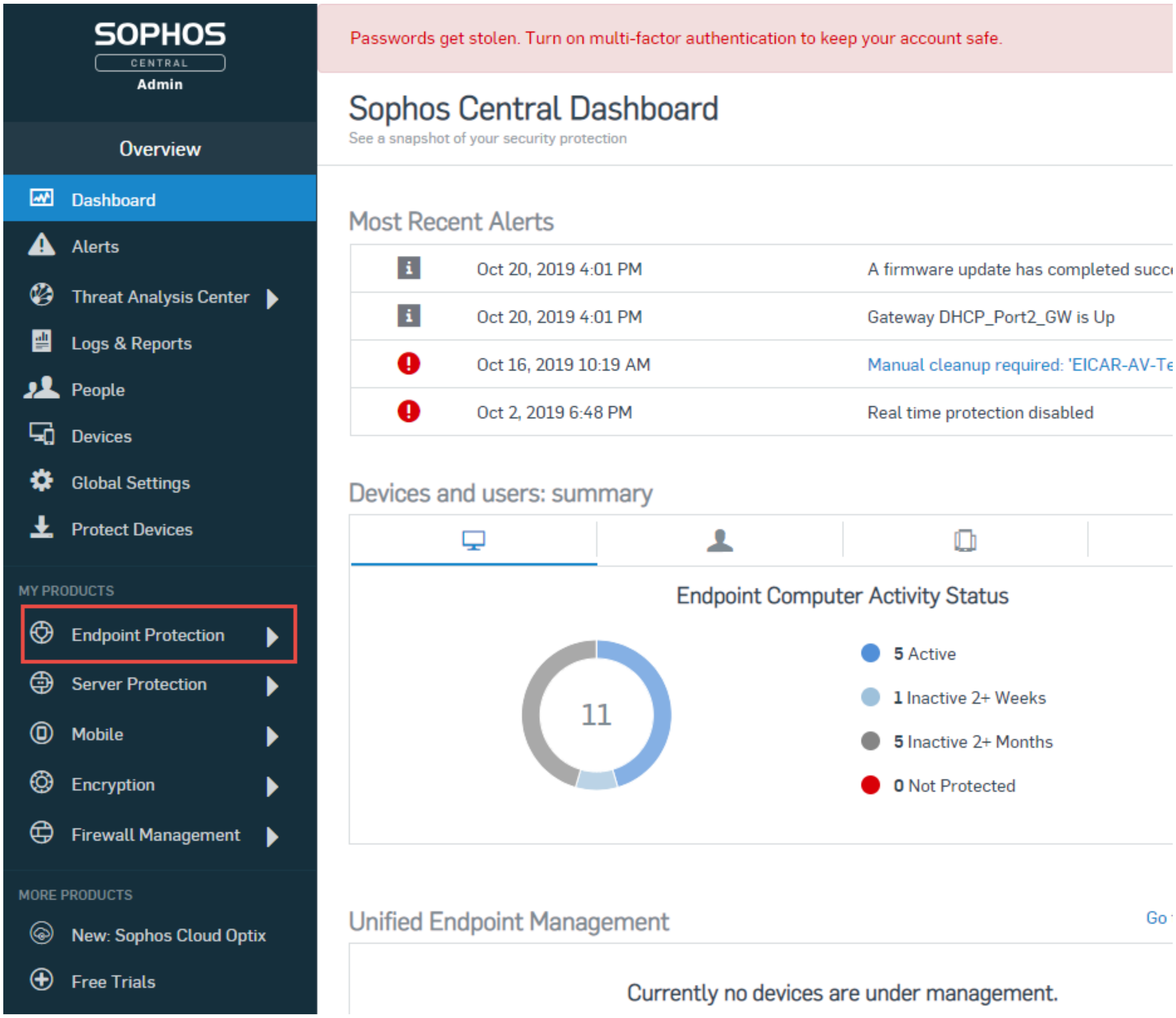
Where to find the IPS settings

1. Log in to Sophos Central
2. In the navigation panel on the left on the Sophos Central Dashboard, click on "Endpoint Protection"



SOPHOS
CENTRAL
Admin

Overview

Dashboard
Alerts
Threat Analysis Center
Logs & Reports
People
Devices
Global Settings
Protect Devices

MY PRODUCTS

Endpoint Protection
Server Protection
Mobile
Encryption
Firewall Management

MORE PRODUCTS

New: Sophos Cloud Optix
Free Trials

Passwords get stolen. Turn on multi-factor authentication to keep your account safe.

Sophos Central Dashboard
See a snapshot of your security protection

Most Recent Alerts

i	Oct 20, 2019 4:01 PM	A firmware update has completed succ
i	Oct 20, 2019 4:01 PM	Gateway DHCP_Port2_GW is Up
!	Oct 16, 2019 10:19 AM	Manual cleanup required: 'EICAR-AV-Te
!	Oct 2, 2019 6:48 PM	Real time protection disabled

Devices and users: summary

Endpoint Computer Activity Status

11

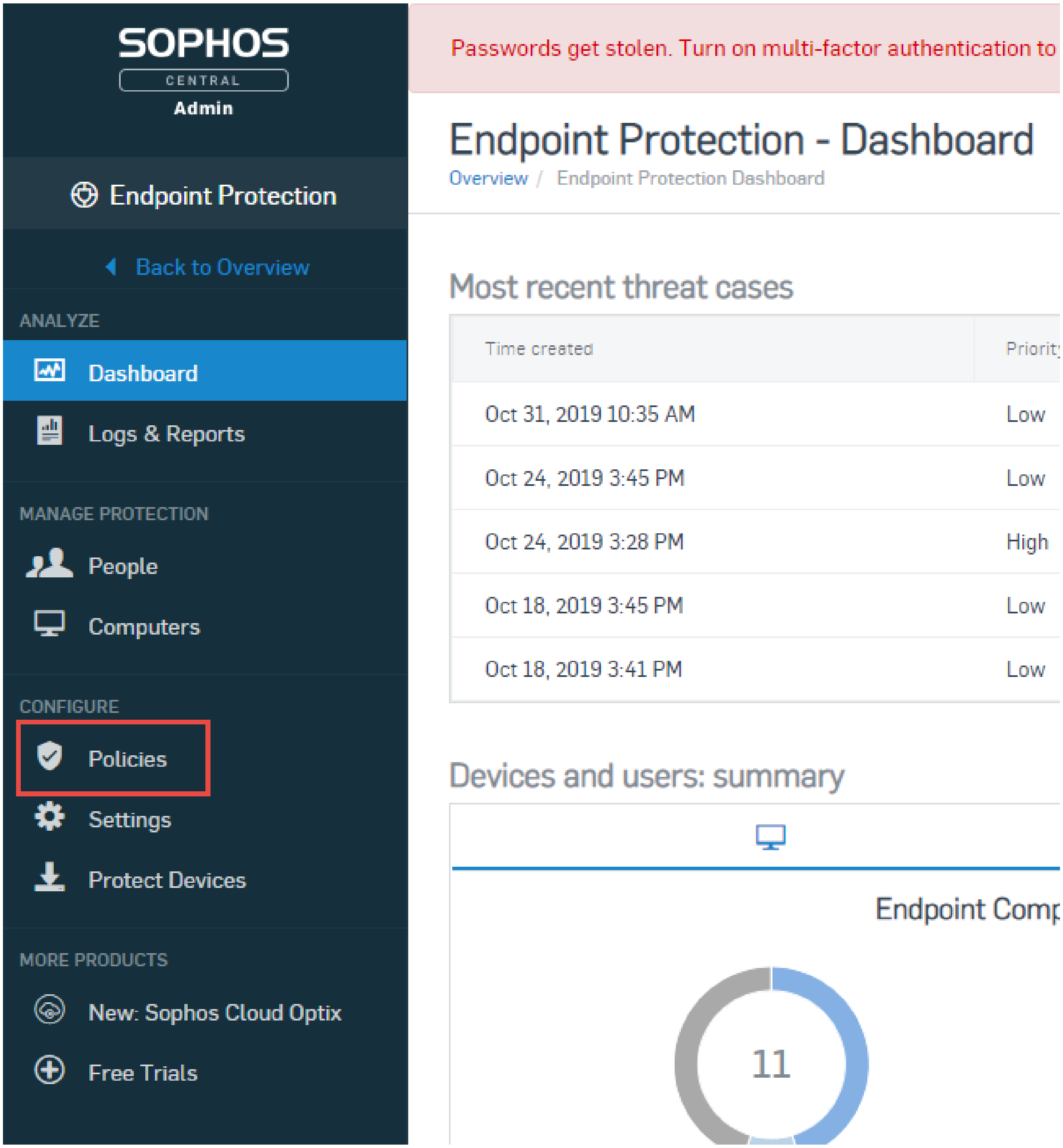
● 5 Active
● 1 Inactive 2+ Weeks
● 5 Inactive 2+ Months
● 0 Not Protected

Unified Endpoint Management

Go

Currently no devices are under management.

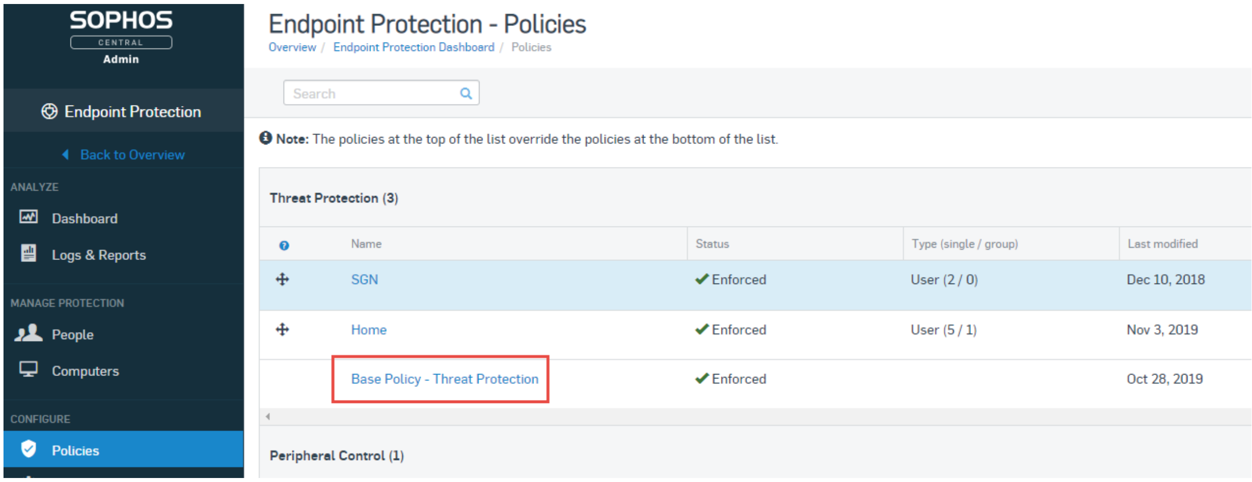
3. In the navigation panel of the Endpoint Protection, click on "Policies" under "Configure"



Passwords get stolen. Turn on multi-factor authentication to

Time created	Priorit
Oct 31, 2019 10:35 AM	Low
Oct 24, 2019 3:45 PM	Low
Oct 24, 2019 3:28 PM	High
Oct 18, 2019 3:45 PM	Low
Oct 18, 2019 3:41 PM	Low

4. You should now see a list of policies you can apply to endpoints. The first type should be "Threat Protection". Click the "Base Policy - Threat Protection" policy



Endpoint Protection - Policies

Overview / Endpoint Protection Dashboard / Policies

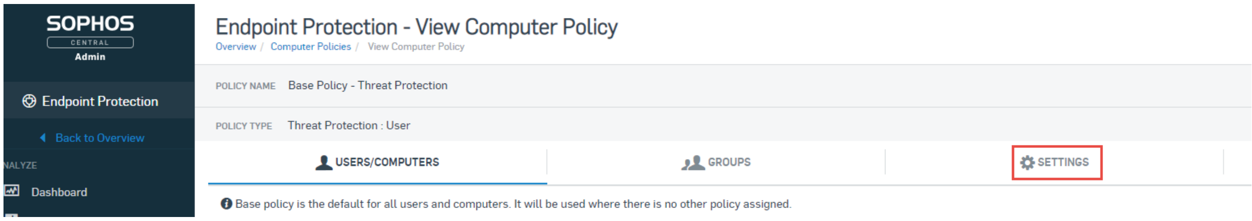
Note: The policies at the top of the list override the policies at the bottom of the list.

Threat Protection (3)

	Name	Status	Type (single / group)	Last modified
✣	SGN	✓ Enforced	User (2 / 0)	Dec 10, 2018
✣	Home	✓ Enforced	User (5 / 1)	Nov 3, 2019
	Base Policy - Threat Protection	✓ Enforced		Oct 28, 2019

Peripheral Control (1)

5. Click on "Settings"



Endpoint Protection - View Computer Policy

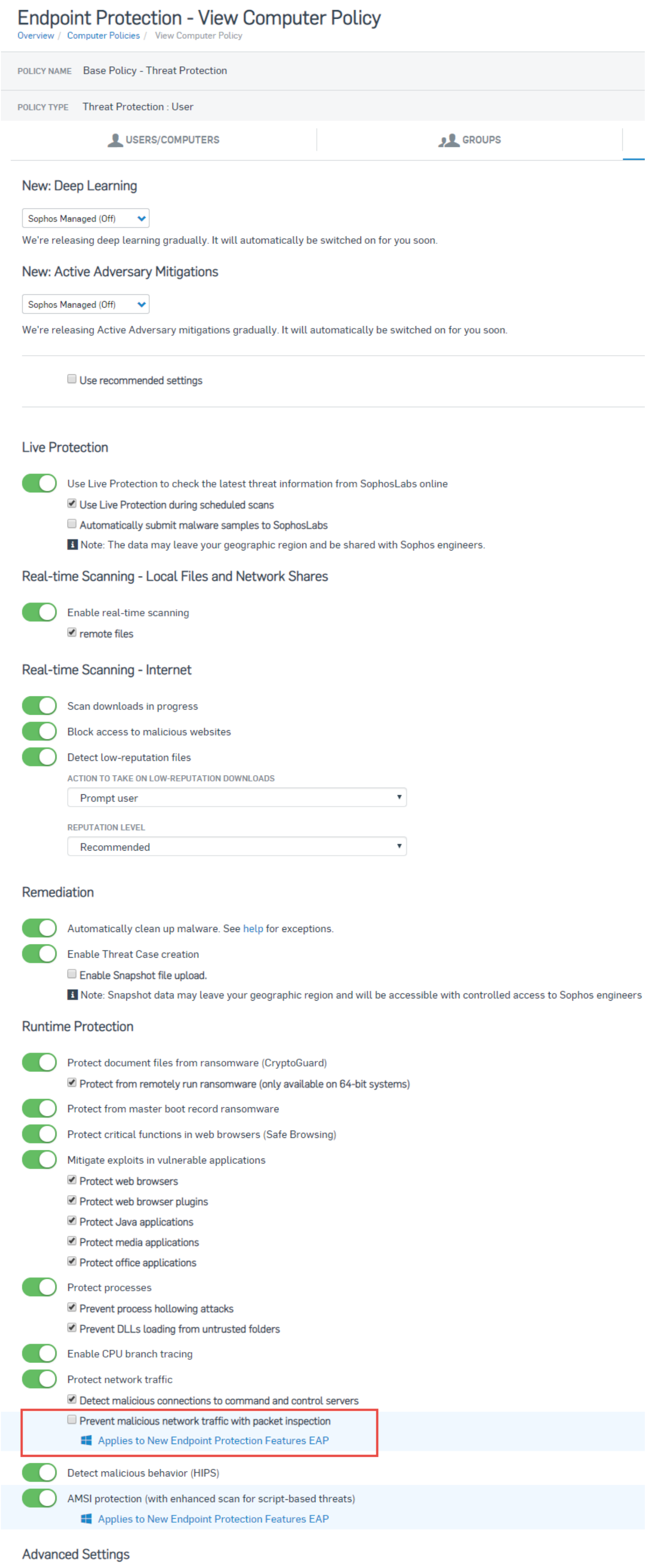
Overview / Computer Policies / View Computer Policy

POLICY NAME Base Policy - Threat Protection

POLICY TYPE Threat Protection : User

Base policy is the default for all users and computers. It will be used where there is no other policy assigned.

6. Scroll down to the section "Runtime Protection". You should see a few lines that have a blue background. The first one is "Prevent malicious network traffic with packet inspection", under "Protect network traffic"



Endpoint Protection - View Computer Policy

Overview / Computer Policies / View Computer Policy

POLICY NAME Base Policy - Threat Protection

POLICY TYPE Threat Protection : User

New: Deep Learning

Sophos Managed (Off)

We're releasing deep learning gradually. It will automatically be switched on for you soon.

New: Active Adversary Mitigations

Sophos Managed (Off)

We're releasing Active Adversary mitigations gradually. It will automatically be switched on for you soon.

☐ Use recommended settings

Live Protection

● Use Live Protection to check the latest threat information from SophosLabs online
- ☑ Use Live Protection during scheduled scans
- ☐ Automatically submit malware samples to SophosLabs
- ℹ Note: The data may leave your geographic region and be shared with Sophos engineers.

Real-time Scanning - Local Files and Network Shares

● Enable real-time scanning
- ☑ remote files

Real-time Scanning - Internet

● Scan downloads in progress

● Block access to malicious websites

● Detect low-reputation files

ACTION TO TAKE ON LOW-REPUTATION DOWNLOADS: Prompt user

REPUTATION LEVEL: Recommended

Remediation

● Automatically clean up malware. See help for exceptions.

● Enable Threat Case creation
- ☐ Enable Snapshot file upload.
- ℹ Note: Snapshot data may leave your geographic region and will be accessible with controlled access to Sophos engineers

Runtime Protection

● Protect document files from ransomware (CryptoGuard)
- ☑ Protect from remotely run ransomware (only available on 64-bit systems)

● Protect from master boot record ransomware

● Protect critical functions in web browsers (Safe Browsing)

● Mitigate exploits in vulnerable applications
- ☑ Protect web browsers
- ☑ Protect web browser plugins
- ☑ Protect Java applications
- ☑ Protect media applications
- ☑ Protect office applications

● Protect processes
- ☑ Prevent process hollowing attacks
- ☑ Prevent DLLs loading from untrusted folders

● Enable CPU branch tracing

● Protect network traffic
- ☑ Detect malicious connections to command and control servers
- ☐ Prevent malicious network traffic with packet inspection
  - Applies to New Endpoint Protection Features EAP

● Detect malicious behavior (HIPS)

● AMSI protection (with enhanced scan for script-based threats)
- Applies to New Endpoint Protection Features EAP

Advanced Settings