

Meraki Network Access Control

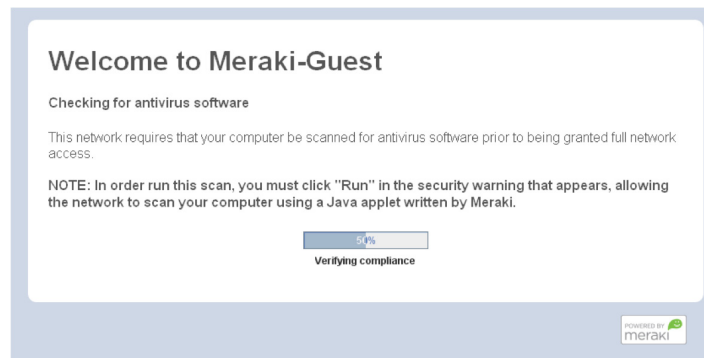
Wireless Client Compliance Enforcement

Integrated Access Control

Meraki Network Access Control provides powerful endpoint compliance assessment and enforcement capabilities to administrators without requiring any additional hardware, software or licenses. Wireless clients are evaluated to determine whether they are protected by anti-virus software. Compliant clients are then allowed onto the network while others sent to a quarantine and remediation area. Unlike many NAC solutions, no LAN reconfiguration or integration is required.

Key Benefits:

- One-click installation
- Easy, scalable management across 1000's of sites
- No VLAN reconfiguration or client agent installation required
- Touchless remediation
- No new hardware or software required
- Included with the Meraki Enterprise license



When clients connect to a Meraki network with NAC enabled, their browser runs a java applet to determine if they are compliant with security policies.

Today's Open Network Bring New Challenges

Consumer devices are appearing in business environments as a result of workers bringing in devices from home. In addition, IT administrators are now often expected to offer secure wireless access to visitors and their devices, over which an IT department has no control. And even trusted users can unintentionally introduce viruses into a corporate environment, wreaking havoc on network infrastructure and requiring days or even weeks to recover. As a result of these threats, effective network access control has become essential to protect today's modern, open enterprise network. Meraki Network Access Control offers administrators a simple, no-hassle means to ensure their network is protected.

Network access control *	Check clients for antivirus software
Remediation *	Show custom URL
	URL: <input type="text" value="www.mcafee.com"/>

Deploy Across Multiple Sites in Minutes

Most traditional network access control products require installation of expensive hardware appliances, servers and software and are complex to deploy and manage. In addition, often products that perform well at the pilot stage turn out to be unscalable to a production deployment, requiring weeks to deploy with the assistance of expensive third party installers. Meraki's Network Access Control does not require any new hardware or software to be installed in your network and can be enabled with one-click per SSID. No per user or per device licensing is required.

Automated Compliance Assessment and Remediation

Devices that connect to your network will be quarantined behind a captive portal using the AP's stateful firewall. They will then be scanned by a dissolving agent to check that anti-virus software is installed and running. If found to be compliant, the user will then be allowed onto the network and their device will be whitelisted for a specified time period before a rescan will be required. If found to be non-compliant, they will be redirected to a remediation site. This could be either a Meraki default splash page that will allow them to download free anti-virus software, an internal corporate site where anti-virus software is hosted or a public URL in a walled garden such as www.mcafee.com where clients can download the desired anti-virus software. Once remediated, clients will be rescanned and then given access to the network.

Complete User and Device Visibility and Control

Combined with the endpoint posture assessment and enforcement of Meraki Network Access Control, the Meraki Dashboard offers full device and user visibility and control across your entire network. Device and OS fingerprinting, traffic analysis, detailed event logging and summary reports offer granular, drill-down capable visibility into who is using your network and how. Enterprise-grade authentication, application-aware traffic shaping, content filtering and guest account management provide administrators granular access control and powerful tools to manage exactly how the network is used.

Specifications

> Anti-Virus Software Compatibility

Most leading anti-virus software including:

- McAfee Total Protection
- Symantec Endpoint Protection
- Kaspersky Anti-Virus
- Norton Anti-Virus
- Microsoft Security Essentials
- AVG Anti-Virus
- Sunbelt VIPRE Anti-Virus

- New anti-virus software fingerprints added from the Meraki Cloud Controller
-

> Client Compatibility

- Compatible with all operating systems
 - Scanned operating systems: Windows XP, 7 and Vista
 - All other operating systems are whitelisted
-

> Other Features

- Works with any LAN infrastructure
 - Dissolving agent requires no client software installation
 - Self-remediation with no administrator intervention required
-

> Ordering Information

- Available on all Meraki Enterprise networks at no additional cost
 - No per user or per device licensing required
-