eyeExtend for Advanced Compliance Configuration Guide v1.4.5

31 August 2023

eyeExtend for Advanced Compliance Configuration Guide v1.4.5

About the Advanced Compliance Integration

This topic describes the Advanced Compliance integration.

The Forescout eyeExtend for Advanced Compliance integration greatly simplifies the effort required to enforce compliance on network endpoints and devices by automating compliance scanning and reporting. Security Content Automation Protocol (SCAP) content is downloaded from known public repositories and then uploaded to the Forescout Platform. The Forescout Platform uses SCAP benchmarks to assess the compliance status of endpoints and devices.

In addition to scanning Windows endpoints, eyeExtend for Advanced Compliance scans Linux and Mac OS X endpoints and Cisco IOS devices to ensure that they are configured according to the company standard. Examples of Cisco network gear includes switches and routers. Examples of Linux operating systems include CentOS and Red Hat.

Endpoints and devices can be scanned and assessed according to a schedule or based on a specific event, such as an attempt to gain access to the network. The Forescout Platform uses the scan results to identify device compliance based on customizable thresholds. Forescout Platform policies can be used to isolate non-compliant devices, and to notify the security officer or network administrator so that appropriate actions can be taken.

Supported Forescout Platform Version

The following table lists the Forescout Platform version that works with each version covered by this guide.

Version	Forescout Platform Version
1.4.5	Minimum version: 8.3

About Certification Compliance Mode

Forescout eyeExtend for Advanced Compliance supports Certification Compliance mode. For information about this mode, refer to Certification Compliance in the *Forescout Platform Installation Guide*.

Use Cases

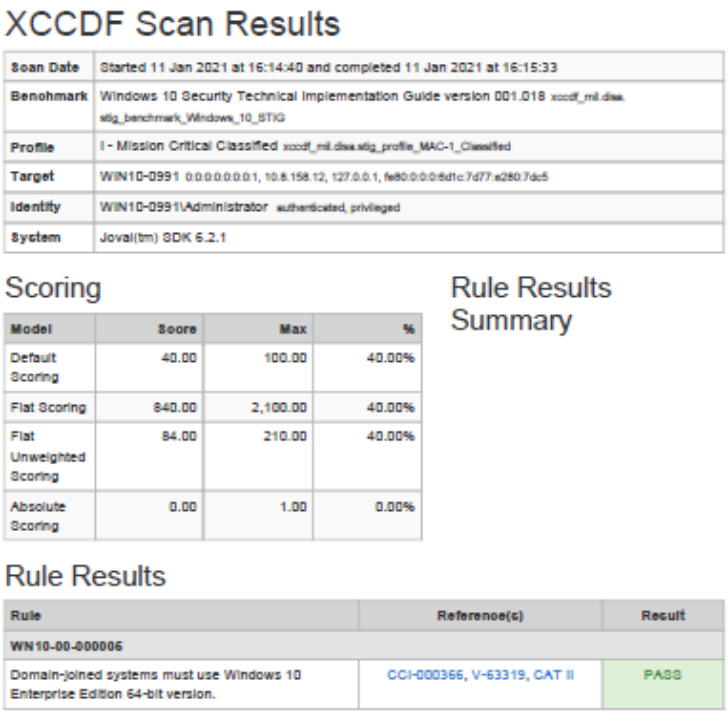
This section describes important use cases supported by Forescout eyeExtend for Advanced Compliance. To understand how this module helps you achieve these goals, see About eyeExtend for Advanced Compliance Module.

Continuous Configuration Management

- Ensure that Windows, Linux, and Mac OS X endpoints and Cisco IOS devices are compliant with regulatory requirements, such as PCI or government standards, such as the Secure Technical Implementation Guide (STIG) before they are granted full network access.
- Confirm that all endpoints and devices remain compliant while they are on the network.

Report and Quarantine Non-Compliant Endpoints and Devices

- Create and email a detailed report of any Windows, Linux, and Mac OS X endpoint or Cisco IOS device that fails to meet a defined compliance level for any given SCAP Compliance benchmark. Use the Email Compliance Report action in Forescout Platform policies to email a report of Advanced Compliance results in HTML, XML, or PDF format.
- Quarantine all Windows, Linux, and Mac OS X endpoints and Cisco IOS devices that fall below a minimum compliance level.



XCCDF Scan Results

Scan Date	Started 11 Jan 2021 at 16:14:40 and completed 11 Jan 2021 at 16:15:33
Benchmark	Windows 10 Security Technical Implementation Guide version 001.018 xccdf_mil.disa.stig_benchmark_Windows_10_STIG
Profile	I - Mission Critical Classified xccdf_mil.disa.stig_profile_MAC-1_Classified
Target	WIN10-0991 0.0.0.0:0.0.0.1, 10.8.158.12, 127.0.0.1, fe80:0:0:0:6d1c:7d77:e280:7dc5
Identity	WIN10-0991\Administrator authenticated, privileged
System	Java(tm) SDK 6.2.1

Scoring

Model	Score	Max	%
Default Scoring	40.00	100.00	40.00%
Flat Scoring	840.00	2,100.00	40.00%
Flat Unweighted Scoring	84.00	210.00	40.00%
Absolute Scoring	0.00	1.00	0.00%

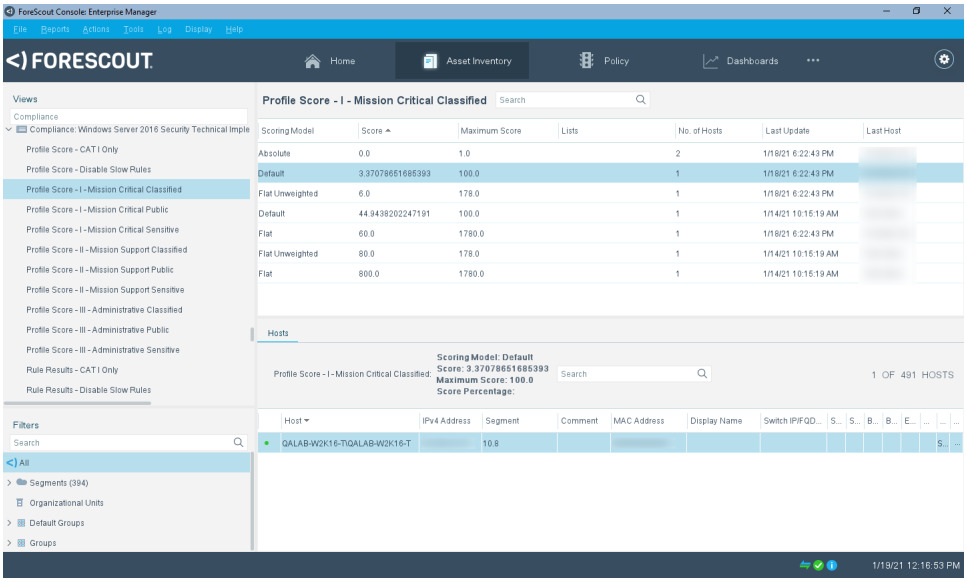
Rule Results Summary

Rule Results

Rule	Reference(s)	Result
WN10-00-000006		
Domain-joined systems must use Windows 10 Enterprise Edition 64-bit version.	CCI-000366, V-63319, CAT II	PASS

Measure the Organizational Compliance Level Against Known Benchmarks

- Obtain an overview of the compliance of all Windows, Linux, and Mac OS X endpoints and Cisco IOS devices for a given benchmark.
- Drill down to compliance rules of interest to understand the compliance level among Windows, Linux, and Mac OS X endpoints and Cisco IOS devices.



Generate Standard Security Compliance Reports

Information Security Officers can use the Reports portal to generate detailed reports in Asset Report Format (ARF). A report template provided by Forescout eyeExtend for Advanced Compliance generates XML reports of XCCDF profile evaluation results. Each report created with this template reports the scores for a specified benchmark profile for selected Windows, Linux, and Mac OS X endpoints and Cisco IOS devices in the network.

You can use the Reports portal to generate individual reports, or more typically, to define a schedule for regular report generation.

For each report job, you can define a target server on which the Forescout Platform places report files. This supports automated submission/deposit of data to external ARF compatible applications.

Additional Documentation

For more information about SCAP 1.1, refer to: http://csrc.nist.gov/publications/nistpubs/800-126-rev1/SP800-126r1.pdf

For more information about SCAP 1.2, refer to: http://csrc.nist.gov/publications/nistpubs/800-126-rev2/SP800-126r2.pdf

For more information about SCAP 1.3, refer to: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-126r3.pdf

For more information about JovalTM SCAP 1.3 documentation, refer to: Joval SCAP 1.3 Documentation