QSC18

QUALYS SECURITY CONFERENCE 2018

Policy Compliance & Security Configuration Assessment

Automate the Assessment of Technical Controls & Mandate-based Security Requirements

Compliance Challenges

Continuing Expansion of Industry & Regulatory Mandates

Ensuring Coverage of Technical & Non-Technical Controls

Maintaining Visibility Across Silos

Due Diligence Beyond Regulated Environment

Qualys.

Necessities to Support Digital Transformation:

Complete Visibility across Business Units, Technologies, and Environments

Simplified Processes, So they can focus on improving security rather than running products

Flexibility options for capturing required compliance data

Support for emerging technologies and capabilities

Qualys.

Necessities to Support Digital Transformation:

Tight integration across security technologies to support complex mandates and audit requirements

Automation and process integration to support DevSecOps

Comprehensive reporting against regulations, mandates & audit objectives

Qualys.

Use Case:

FedRAMP/NIST Compliance via unified security program

Customer: Cloud-based Infrastructure solution Provider

- Digital Transformation underway
- FedRAMP certification driving compliance unification
- Leveraging NIST for control objectives company wide

Goals:

- Address **FedRAMP compliance** as a bi-product of good cybersecurity practices
- Consolidated cybersecurity dashboard based on the NIST objectives

Requires:

- Security Vendor Consolidation
- Integrated Solutions
- Strong Regulatory Content
- End-End mandate reporting
- Breadth & Depth of Coverage

NIST Control	NIST Control Objective	Qualys Applications
CM	Information System Component Inventory	AI SYN
CM	Inventory of Authorized and Unauthorized Software	AI SYN VM PC
CM	Secure Configuration for Hardware and Software	TP
RA-5	Continuous Vulnerability Assessment & Remediation	VM PC TP CM
AC, IA	Controlled Used of Administrative Privileges	PC
AU	Maintenance, Monitoring and Analysis of Audit Logs	PC FIM
AC	Email and Web Browser Protection	VM PC SAQ
SI-4	Malware Defense	PC IOC WAS WAF FIM
CM, SA	Limitation and Control of Network Ports	VM PC CM WAF
CP	Data Recovery Capability	PC SAQ
CM, RA	Secure Configurations for Network Devices	VM PC

NIST Control	NIST Control Objective	Qualys Applications
AC, SI	Boundary Defense	VM PC CS WAS WAF
AU	Maintenance, Monitoring, and Analysis of Audit Logs	PC FIM
AC, IA	Controlled Access Based on the Need to Know	PC CS
AC-17, AC-18	Wireless Access Control	VM
AC, IA	Account Monitoring and Control	PC SAQ
AT	Security Skills Assessment and Appropriate Training to Fill Gaps	SAQ
RA, CM	Vendor Controls Assessment	IOC CS WAS WAF
IR	Incident Response and Management	PC IOC FIM
CA	Penetration Tests and Red Team Exercises	VM TP IOC

Qualys.

They started with critical requirements for Quick Wins…

1. Inventory Your Systems — AI, SYN
2. Inventory and Restrict Software — AI, SYN, PC, VM
3. Secure Configurations — PC, FIM, SCA
4. Continuous Vulnerability Management — VM, CM, TP, SCA
5. Review Rights & Permissions — PC
6. Definition, Automated Evaluation & Review of Processes — SAQ

Qualys.

Complete Visibility

Assessment for Out-of-band Configurations

Expanded UDC Support

- Agent Support for OS UDC's
- Database UDC
- Windows File Content
- Command UDC

PC Dashboard

Qualys.

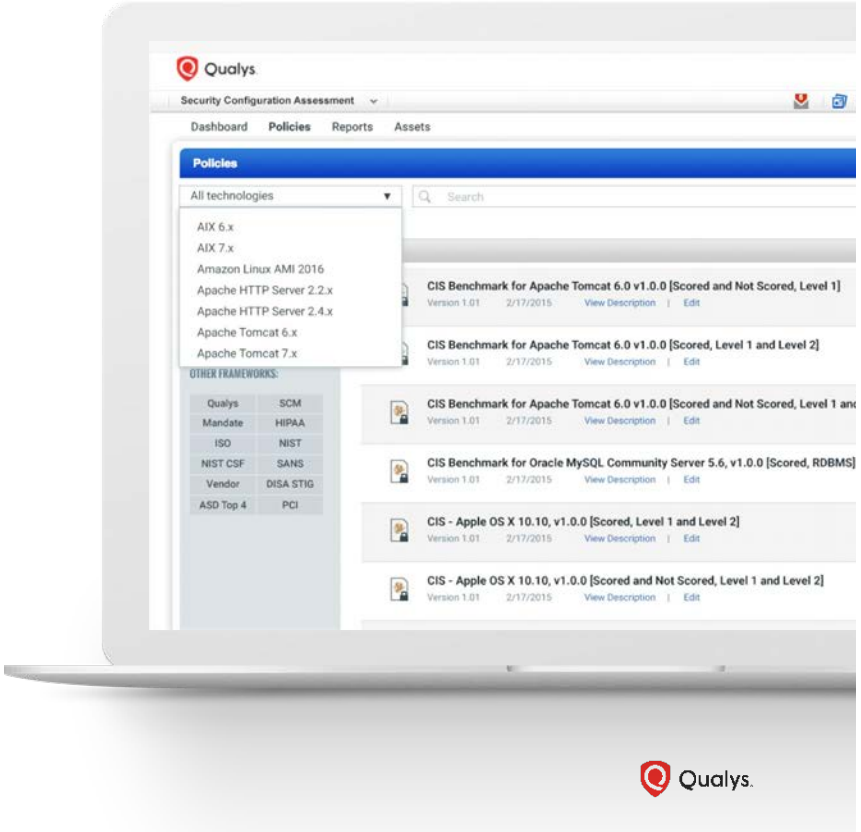
Assess ALL your assets against CIS

With Qualys Security Configuration Assessment

Security Configuration Assessment

Lightweight add-on to VM
Broad platform coverage
Accurate controls & content
Simple assessment workflow
Scan remotely or via agent
Powered by the Qualys Cloud Platform

Support for NIST Reporting coming soon!



Broad Technology & Control Coverage
to support Emerging Technologies & Digital Transformation

Network Devices
Applications
Operating Systems

Emerging Technologies

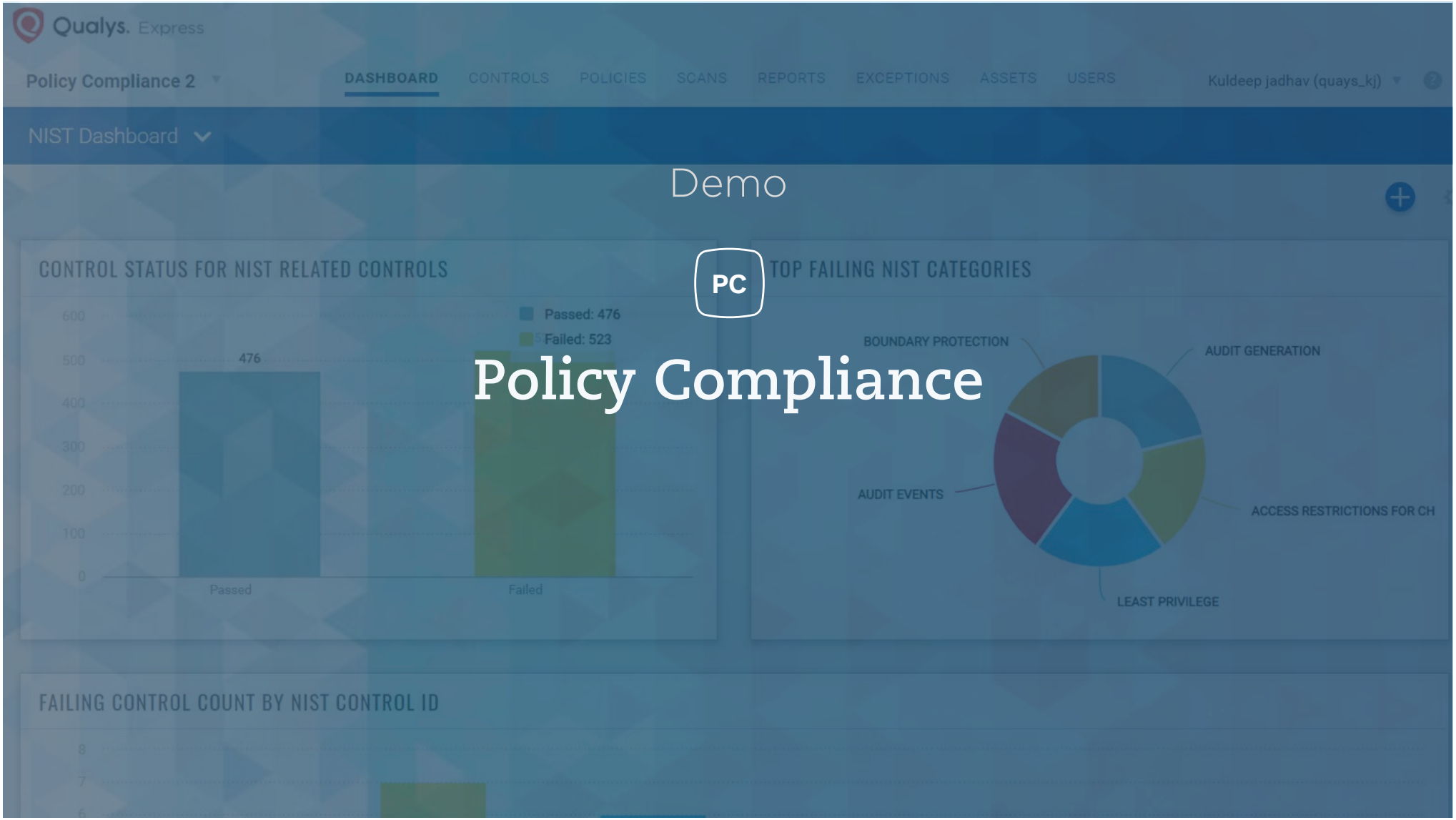
Containers
Cloud Security

Qualys Platform Security Report
Security Gap Assessment

Demo

PC

Policy Compliance

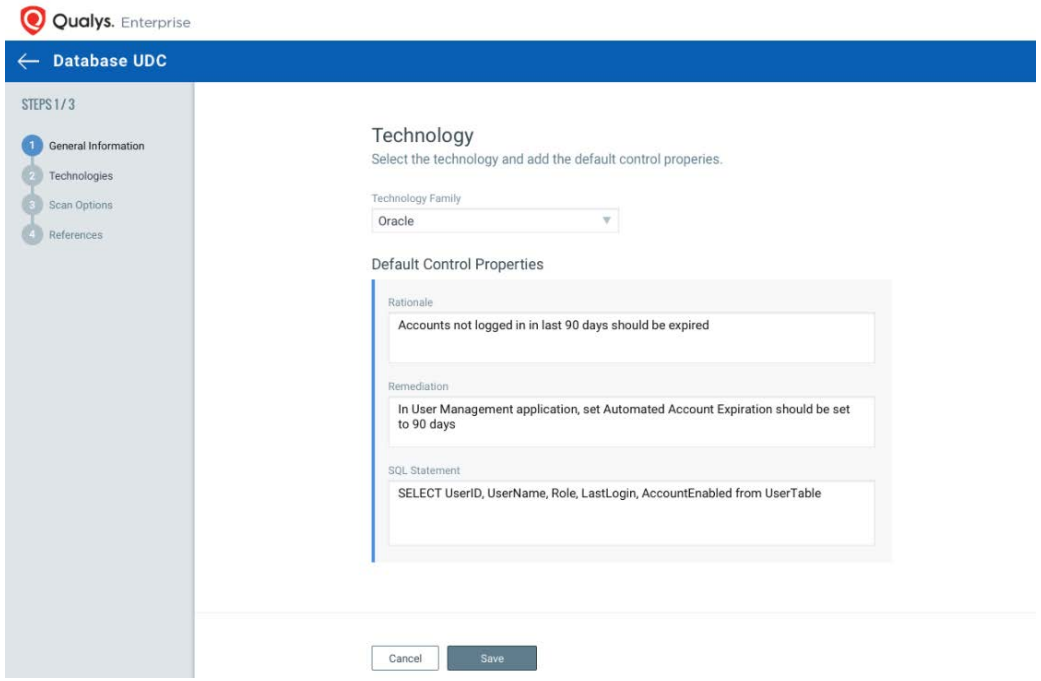


Database UDC

Initial Support: MSSQL, Oracle, MongoDB

Define DB Query (read only), Customizable by DB Version

Set a query to return tabular data to evaluate (which can include evidence)

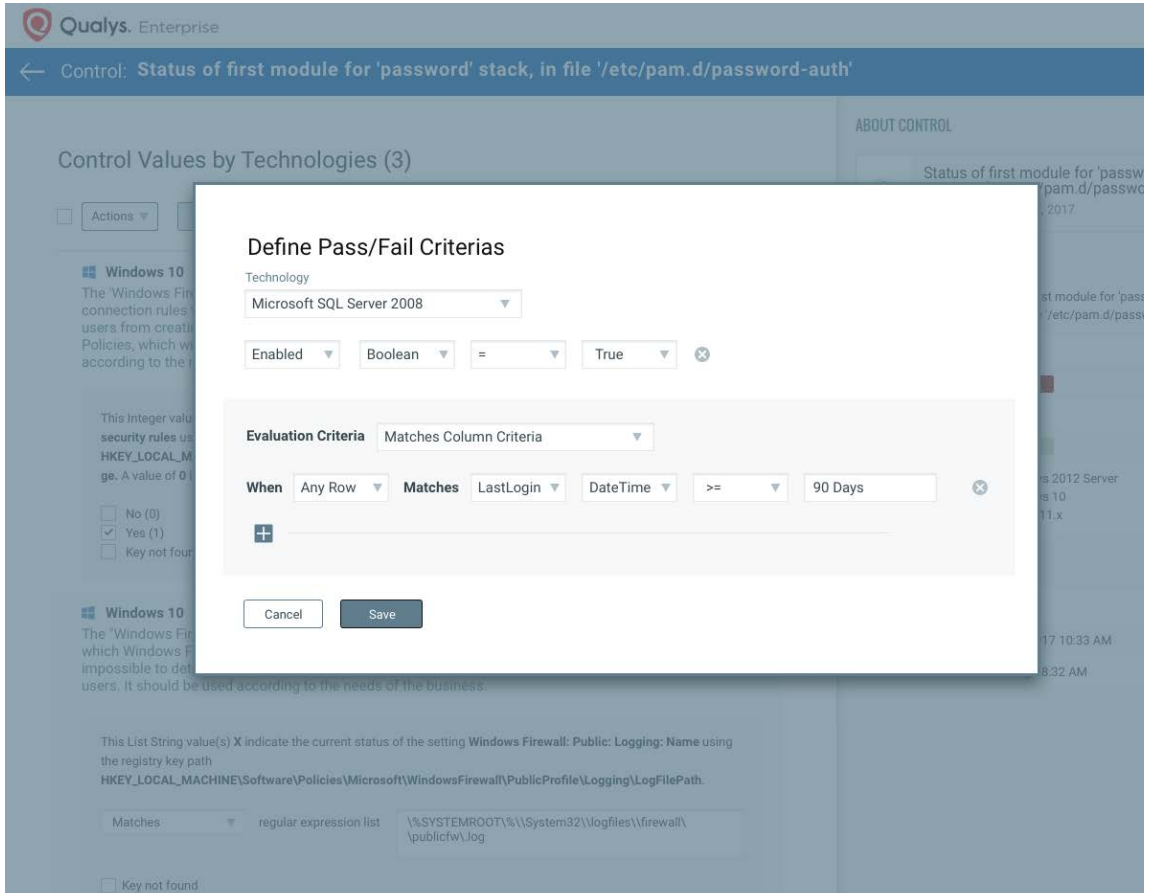


Qualys.

Then, Configure Pass/Fail Criteria

Define a Post-Filter, Then Evaulate based on:

- Empty Result Set
- Row Count Threshold
- Always Pass/Fail (for data gathering)
- Match Column Criteria



Simplifying Processes

Expanded Library Content

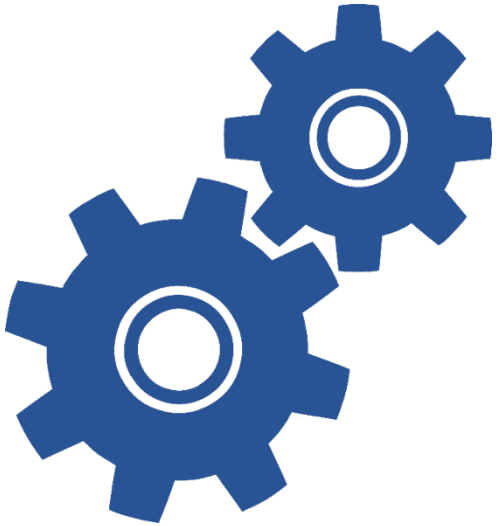
Instance Discovery & Controls

Migration to New UI – Up First:

- PC Dashboard
- Policy & Control Library
- Reporting

Mandate-based Policy Configurator

Leverage Asset Inventory for Asset Lifecycle Management



Qualys.

Mandate Policy Configurator

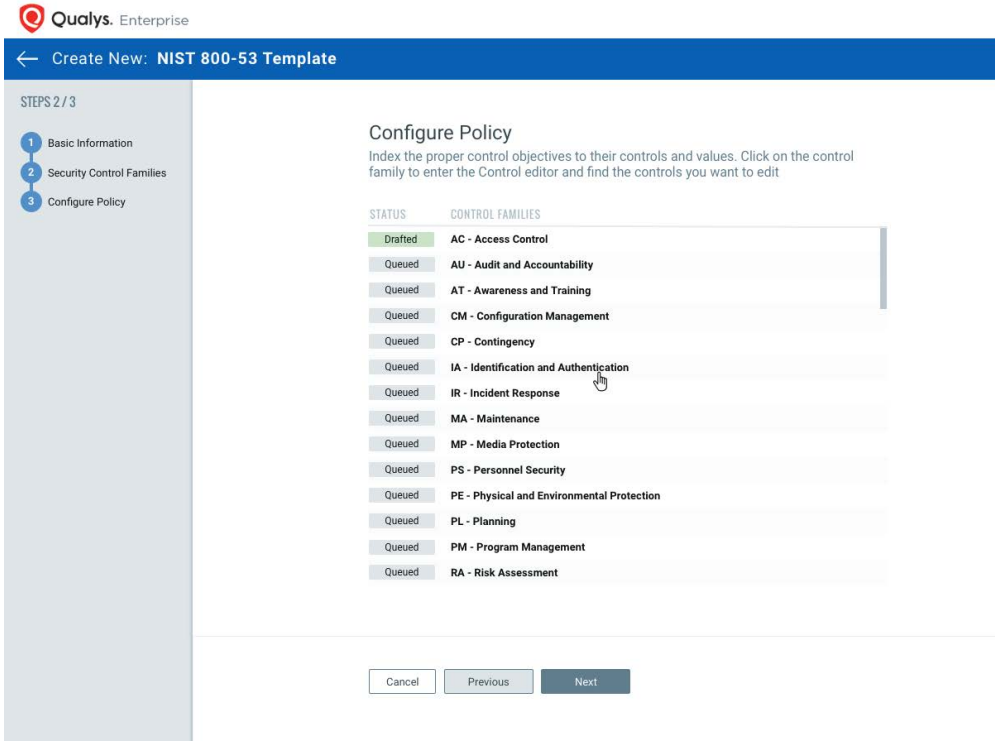
More Granular, Customizable Control Objectives

Custom & Library Mandates

Generate Policies from Mandate

Mandate-specific Reports

Gap Analysis Reports



Qualys.

Qualys. Enterprise

← Create New: **NIST 800-53 Template**

STEPS 1 / 3

1. Basic Information
2. Security Control Families
3. Configure Policy

Basic Information

Name and select the mandate for this template.

TITLE:

MANDATE:

NIST Special Publication 800-53

Security Controls and Assessment Procedures for Federal Information Systems and Organizations

DESCRIPTION:

Cancel | Previous | Next

Qualys. Enterprise

← Create New: **NIST 800-53 Template**

STEPS 2 / 3

1. Basic Information
2. Security Control Families
3. Configure Policy

Security Control Families

Select all or just the security controls families you want to configure in this template.

CONTROL FAMILIES:

(●) Select Families ( ) Minimum Security Controls

BUILD LIST OF CONTROL FAMILIES:

Search...

There are no security control families selected, yet.

Here is where you'll see the control families for this template.

Cancel | Previous | Next

Qualys. Enterprise

← Create New: **NIST 800-53 Template**

STEPS 2 / 3

1. Basic Information
2. Security Control Families
3. Configure Policy

Security Control Families

Select all or just the security controls families you want to configure in this template.

CONTROL FAMILIES:

- (●) Select Families
- ( ) Minimum Security Controls

BUILD LIST OF CONTROL FAMILIES:

Search...

- [ ] Select all (14 families)
- [ ] AC - Access Control
- [ ] AU - Audit and Accountability
- [ ] AT - Awareness and Training
- [ ] CM - Configuration Management
- [ ] CP - Contingency
- [ ] IA - Identification and Authentication

OK

Cancel | Previous | Next

Qualys. Enterprise

← Create New: **NIST 800-53 Template**

STEPS 2 / 3

1. Basic Information
2. Security Control Families
3. Configure Policy

Security Control Families

Select all or just the security controls families you want to configure in this template.

CONTROL FAMILIES:

(●) Select Families ( ) Minimum Security Controls

BUILD LIST OF CONTROL FAMILIES:

Search...

10 CONTROL FAMILIES — Remove all

- AC - Access Control
- AU - Audit and Accountability
- AT - Awareness and Training
- CM - Configuration Management
- CP - Contingency
- IA - Identification and Authentication

Qualys. Enterprise

← Create New: **NIST 800-53 Template**

STEPS 2 / 3

1. Basic Information
2. Security Control Families
3. Configure Policy

Configure Policy

Index the proper control objectives to their controls and values. Click on the control family to enter the Control editor and find the controls you want to edit

STATUS	CONTROL FAMILIES
Drafted	**AC - Access Control**
Queued	**AU - Audit and Accountability**
Queued	**AT - Awareness and Training**
Queued	**CM - Configuration Management**
Queued	**CP - Contingency**
Queued	**IA - Identification and Authentication**
Queued	**IR - Incident Response**
Queued	**MA - Maintenance**
Queued	**MP - Media Protection**
Queued	**PS - Personnel Security**
Queued	**PE - Physical and Environmental Protection**
Queued	**PL - Planning**
Queued	**PM - Program Management**
Queued	**RA - Risk Assessment**

Qualys. Enterprise

Objective: **IA - Identification and Authentification**

Cancel | Done

Search Options

Search...

11
Total Control Objectives

Actions

MINIMUM SECURITY CONTROLS

High	3.01K
Moderate	982
Low	89

PRIORITY

P0 - Priority Level 0	3.01K
P1 - Priority Level 1	982
P2 - Priority Level 2	89
P3 - Priority Level 3	89

TECHNOLOGY

Windows 2012 Server	25
Windows Server 2012 R2	16
Debian GNU/Linux 9.x	5
Docker 1.x	23
F5 BIG-IP 11.x	15

10 more

NAME	PRIORITY	SECTIONS	CONTROLS
IA-5 Authenticator Management The organization manages information system authenticators by: a. Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, or device receiving the authenticator;	P1	15	384
IA-5(1) Authenticator Management | Password-Based Authentication		6	242
IA-5(2) Authenticator Management | PKI-Based Authentication		4	48
IA-5(3) Authenticator Management | In-Person or Trusted Third=Party Registration			1
IA-5(4) Authenticator Management | Automated Support for Password Strength Determination			31
IA-5(5) Authenticator Management | Change Authenticators Prior to Delivery			1
IA-5(6) Authenticator Management | Protection of Authenticators			8
IA-5(7) Authenticator Management | No Embedded Unencrypted Static Authenticators			4
IA-5(8) Authenticator Management | Multiple Information System Accounts			0

Qualys. Enterprise

Objective: **IA - Identification and Authentification**

Cancel | Done

Search Options

Search...

11
Total Control Objectives

MINIMUM SECURITY CONTROLS

High	3.01K
Moderate	982
Low	89

PRIORITY

P0 - Priority Level 0	3.01K
P1 - Priority Level 1	982
P2 - Priority Level 2	89
P3 - Priority Level 3	89

TECHNOLOGY

Windows 2012 Server	25
Windows Server 2012 R2	16
Debian GNU/Linux 9.x	5
Docker 1.x	23
F5 BIG-IP 11.x	15

10 more

Actions

NAME	PRIORITY	SECTIONS	CONTROLS
IA-5 Authenticator Management The organization manages information system authenticators by: a. Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, or device receiving the authenticator; ...	P1	15	384
IA-5(1) Authenticator Management | Password-Based Authentication		6	242
The information system, for password-based authentication:			
IA-5 (1)(a) Enforces minimum password complexity of [Assignment: organization-defined requirements for case sensitivity, number of characters, mix of upper-case letters, lower-case letters, numbers, and special characters, including minimum requirements for each type];			36
IA-5 (1)(b) Enforces at least the following number of changed characters when new passwords are created: [Assignment: organization-defined number]			11
IA-5 (1)(c) Stores and transmits only cryptographically-protected passwords;			27
IA-5 (1)(d) Enforces password minimum and maximum lifetime restrictions of [Assignment: organization-defined numbers for lifetime minimum			63

Qualys. Enterprise

← Controls: **NIST 800-53 for Windows**

36
Controls

IMPACT BASELINE

HIGH	3.01K
MODERATE	982
LOW	89

TYPE

ANSSI	3.01K
Qualys	982
CIS	89
DISA	89

TECHNOLOGY

Windows 2012 Server	25
Windows Server 2012 R2	16
Debian GNU/Linux 9.x	5
Docker 1.x	23
F5 BIG-IP 11.x	15

10 more

Search Options

Search...

Actions

CID	STATEMENT / TECHNOLOGIES	TYPE	CATEGORY	BASELINE
3376	**Status of the 'Maximum Password Age' setting (expiration)** Windows 2012 Server, Windows Server 2012 R2, Solaris 11.x	CIS	IA-5 (1)(a)	HIGH
10734	**Status of the 'number of days before a [Prompt user] password expiration warning prompt is displayed at login' for 'users with a password' setting** Ubuntu 11.x, Windows 2000 Active Directory, Docker 1.x	DISA	IA-5 (1)(a)	MODERATE
10965	**Status of first module for 'password' stack, in file '/etc/pam.d/password-auth'** Windows 2012 Server, Windows Server 2012 R2, Solaris 11.x	CIS	IA-5 (1)(a)	HIGH
11468	**Status of the 'try_first_pass' setting for pam_cracklib.so module in PAM configuration file '/etc/pam.d/common-password'** Docker 1.x, Windows 2012 Server	Qualys	IA-5 (1)(a)	HIGH
11524	**Status of 'fail_interval' setting in the file '/etc/pam.d/password-auth'** Windows 2012 Server	CIS	IA-5 (1)(a)	HIGH
10911	**Status of 'turn off certificate revocation list (CRL) checking at the Key Distribution** Windows 2012 Server, Windows Server 2012 R2	DISA	IA-5 (1)(a)	HIGH

Qualys. Enterprise

← Control: **Status of first module for 'password' stack, in file '/etc/pam.d/password-auth'**

Control Values by Technologies (3)

Actions ▼ | Technology: **All** ⊗ ▼

Windows 10

The 'Windows Firewall: Apply local connection security rules (Domain)' setting enables domain-based connection rules that govern IPSec connections. As this setting enables or restricts local administrative users from creating such local connection rules, in addition to the connection security rules in Group Policies, which will increase the exposure of the system to remote attacks, this should be configured according to the needs of the business.

This Integer value **X** indicates the current status of the setting **Windows Firewall: Domain: Apply local connection security rules** using the registry key path **HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\WindowsFirewall\DomainProfile\AllowLocalIPsecPolicyMerge.** A value of **0** indicates the setting is set to **No**, A value of 1 indicates the setting is set to **Yes**.

- [ ] No (0)
- [x] Yes (1)
- [ ] Key not found

Windows 10

The "Windows Firewall: Public: Logging: Name" setting is used to specify the path and name of the file in which Windows Firewall will write its log information. If events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users. It should be used according to the needs of the business.

ABOUT CONTROL

CIS

Status of first module for 'password' stack, in file '/etc/pam.d/password-auth'

Last modified: Apr 12, 2017

Identification

Statement:	Status of first module for 'password' stack, in file '/etc/pam.d/password-auth'
CID:	10965
Baseline:	HIGH
Reference:	17.15.2.1
Status:	Active
Technologies:	Windows 2012 Server Windows 10 Solaris 11.x

Activity

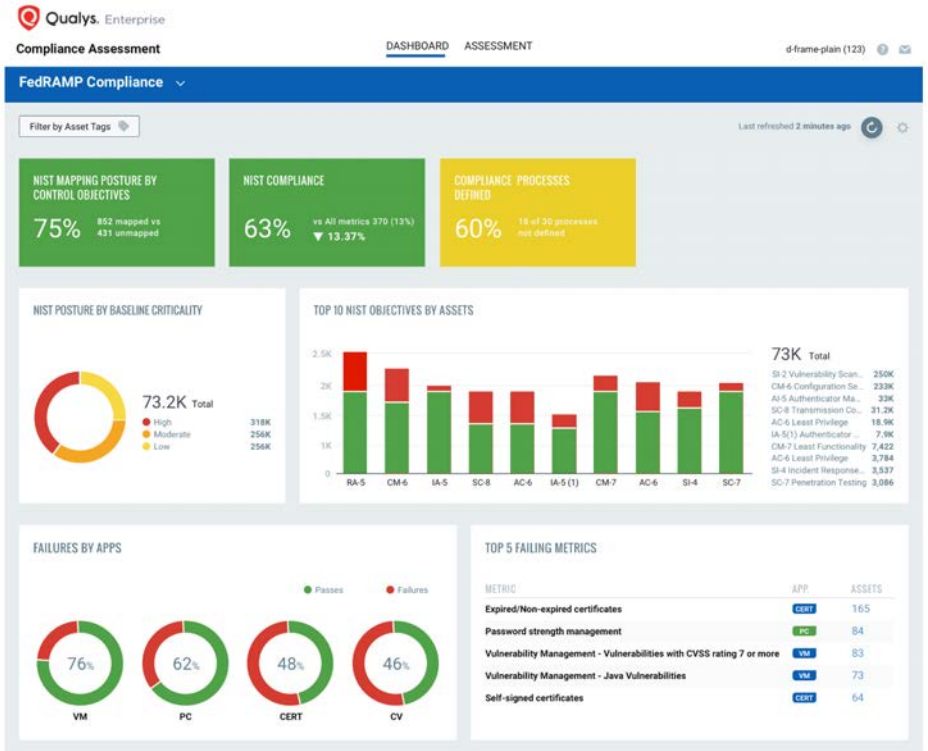
Last User Login:	.\KCtech
Created on:	March 1, 2017 10:33 AM
Last Modified on:	8 Mins ago 8:32 AM

Integration Across the Platform: Unified Compliance Assessment

Out of the box Library of Metrics
- SAQ Self-Assessments
- Vendor Risk Violations
- VM & PC Remediation SLA Failures

Customizable! Map back to Control Objectives & Custom Mandates

Result: Single Pane of Glass for Reporting Metrics & Compliance Violation Tracking across the platform!



Qualys.

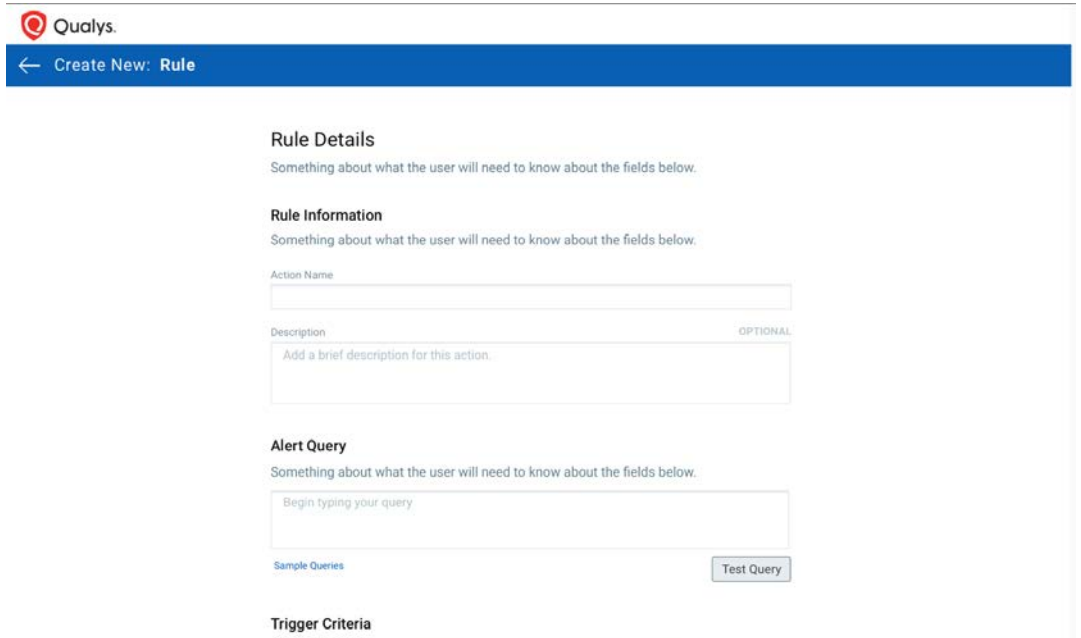
Defining Metrics & Mappings

Leverages new Alerting feature as exposed in apps

Define ANY QQL Query

Action is Log a Compliance Metric

Metrics are then mapped to Control Objectives, which are cross-mapped to regulations




```
vulnerabilities.vulnerability.severity:"5" and vulnerabilities.vulnerability.patchAvailable:"true" and vulnerabilities.firstFound > now-90d
```

Security Metric Examples

High Severity Vulnerabilities/ Patching

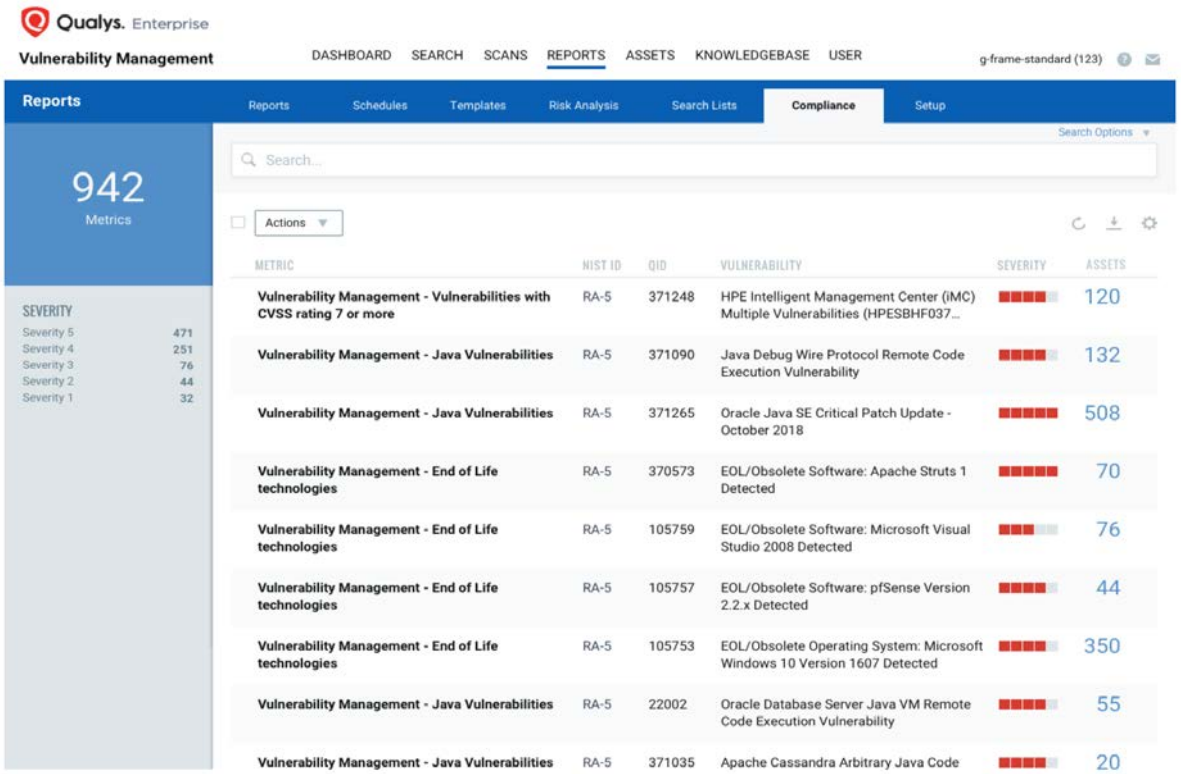
FIM Incident Review Expired

Cloud Security Configuration Issues

Expired or Self-Signed Certificates

Vendor Risk – Failure to Respond

Procedural Control Gap Identified



Qualys.

Demo

PC

Policy Compliance

File Integrity Monitoring

Log and track file changes across global IT systems.

Validating Integrity

Why do organizations need File Integrity Monitoring solutions?

Change control enforcement
Compliance & audit requirements
Explicit mandates like PCI
Security best practices
Compromise detection

Qualys.

Use Case:

File Integrity Monitoring for PCI

Customer: Retail

- Distributed network environment that benefits from cloud-based model
- 20k+ Windows systems
- Large Linux back end infrastructure on-prem and in the cloud

Goals:

- Monitor for change control enforcement
- PCI auditor requirements

Requires:

- Scalable, cloud-based solution
- Hands-off management of distributed agents
- VM+PC+FIM at the Point of Sale
- Broad Linux platform support

What Are Customers Monitoring?

Critical Operating System Binaries

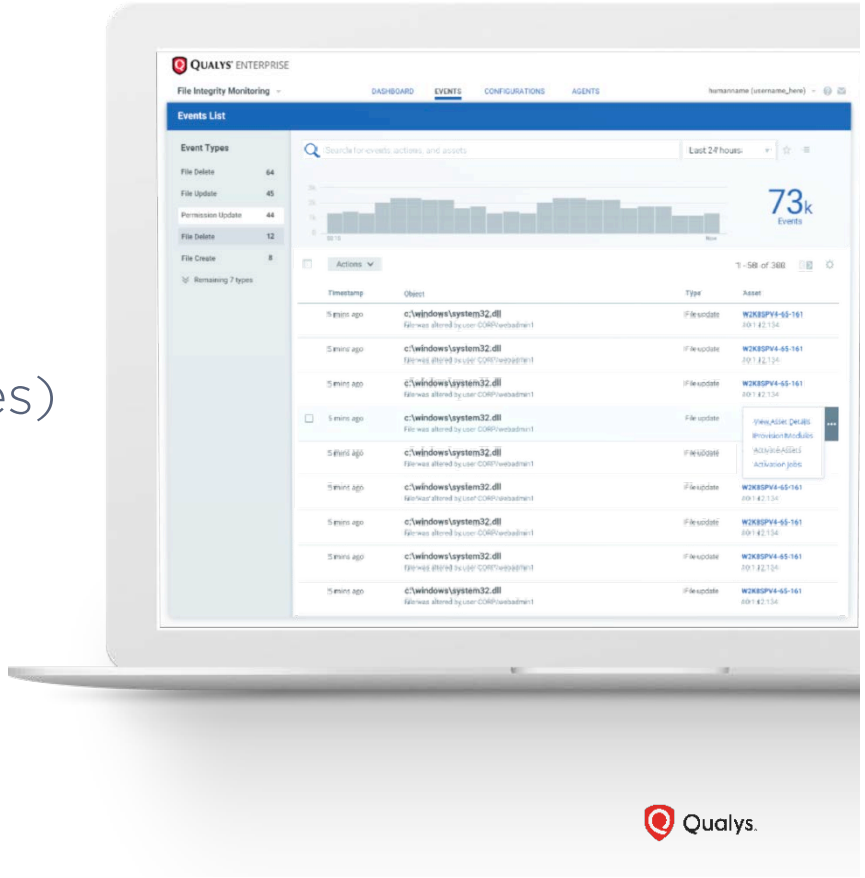
OS and Application Configuration Files

Content, such as Web source

Permissions (such as on Database Stores)

Security Data (Logs, Folder Audit Settings)

User & Authentication Configurations



Qualys.

FIM Challenges

Deciding what depth to monitor

Tuning out noise, but not missing important events

Scalability of legacy solutions

Meeting auditor event review requirements

Improvements since GA

Event Review & Incident Management Workflow

Library Content Improvements

AuditD Compatible Windows Agent (2.1.x)

Windows Feature Expansion & Updated Driver (2.1.x)

Several back-end releases for operational improvements & feature support

Focus for 2019

Simplest tuning in the industry!

Secondary Event Filtering and Automated Correlation

API access to data

Rule-based Alerting

Reporting

Expanded data collection & whitelisting features

Expanded Platform Support

Qualys.

Demo

FIM

Policy Compliance

FIM Feature Roadmap

Q4 2018
1.9
Agent Health UI Improvements
Tune from Event View
Initial Reporting - Change Incident Report
Monitoring Profile Editor Phase II

Q1 2019
2.1
Incident Management UI & Workflow Improvements
Library Improvements
FIM Mgmt API features
External Change Control Integration

Q3 2019
2.3
Show File Text Change Details
Windows Registry Change Detection
Monitoring Profile Import/Export
Streaming Event API

Late Q4 2018/Early Q1 2019
1.10
Incident List API
Incident-Event List API
Event Query API
Management Queries API

2.0
Automated Incident Correlation
Expand Reporting
Basic Notification

Q2 2019
2.2
Process Whitelisting
Dashboard Expansion &
AssetView Integration

* Roadmap items are future looking; timing and specifications may change

Qualys.

Thank You

Tim White
twhite@qualys.com