UAE Information Assurance

Keeping sensitive data and assets safe is the goal of regulatory cybersecurity frameworks such as the United Arab Emirates (UAE) Information Assurance Standard.

Mitigating cyber threats and ensuring the development of a secure national information and communications infrastructure and cyberspace is a strategic priority for the UAE. To this end, the UAE Information Assurance (IA) Standard acts as a critical element to provide requirements for elevating the level of IA across all implementing entities in the UAE.

However, the benefits of this technology adoption come with a rapidly-evolving set of cyber threats. These threats stem from a wide range of sources— hacktivists, issue-motivated groups, and organized cybercrime syndicates—and represent national security concerns that can potentially disrupt critical national services and compromise critical information assets.
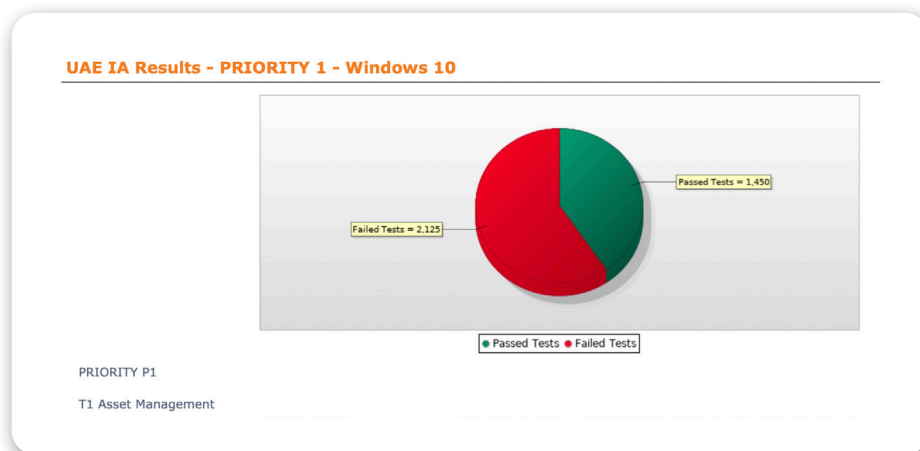
Compliance with these standards will raise the level of national IA and help the UAE progress towards a more resilient national information and communication infrastructure and cyberspace.

The purpose of the UAE IA Standard is to provide requirements to raise the minimum level of protection of information assets and supporting systems across all implementing entities in the UAE. The following pages show how Tripwire solutions map to its technical controls.
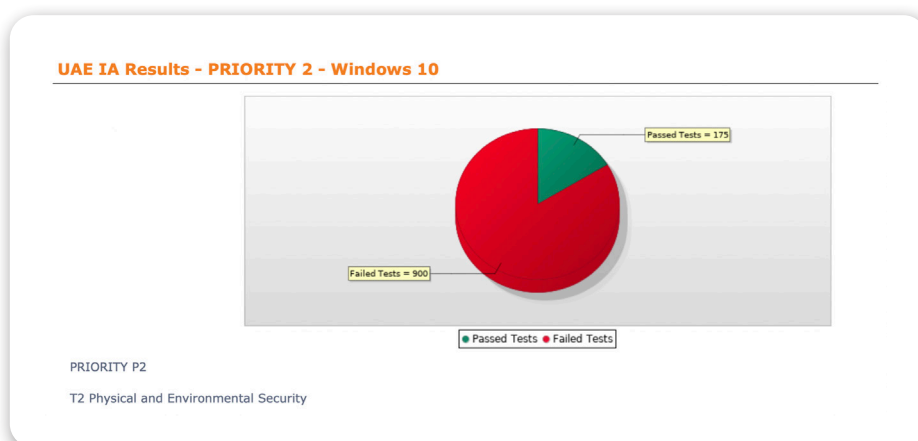
Asset Management

The technical control covered in Tripwire® Enterprise will assist in the compliance auditing and management of removable media policies. This establishes the baseline for the general use and connection of IT networks.

UAE IA Results - PRIORITY 1 - Windows 10

Passed Tests = 1,450
Failed Tests = 2,125

● Passed Tests ● Failed Tests
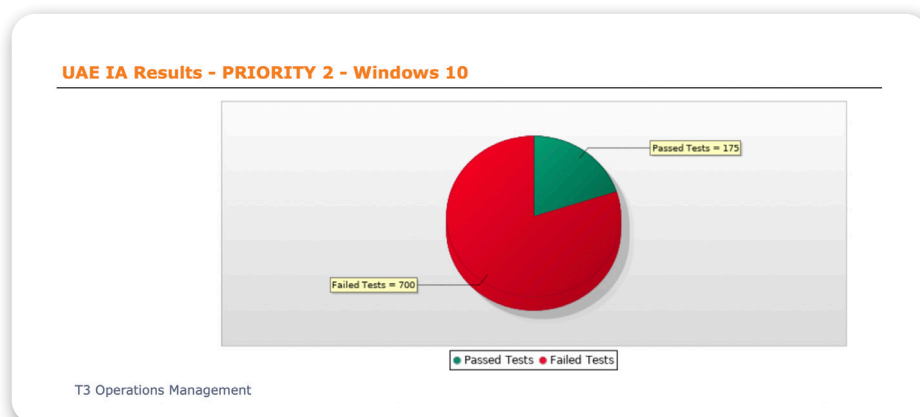
PRIORITY P1

T1 Asset Management

Physical and Environmental Security

The objective of this policy is to prevent loss, damage, theft or compromise of assets and interruption to the entity's activities. The technical control covered in Tripwire Enterprise will ensure that unattended equipment has appropriate protection.

UAE IA Results - PRIORITY 2 - Windows 10

Passed Tests = 175
Failed Tests = 900

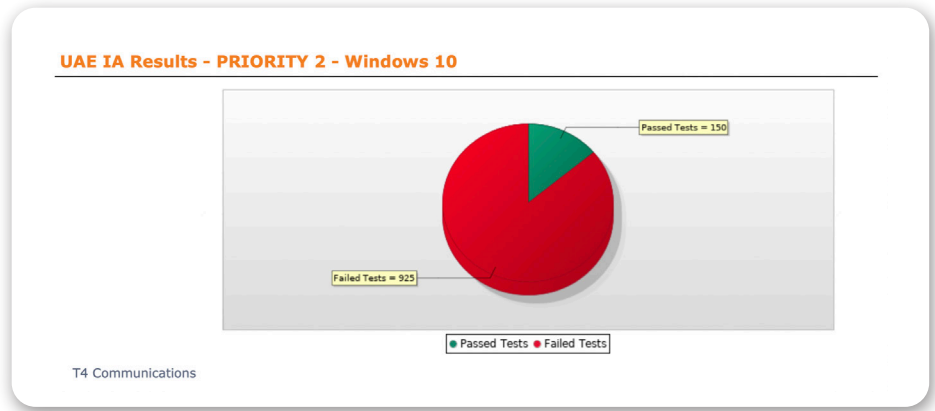● Passed Tests ● Failed Tests

PRIORITY P2

T2 Physical and Environmental Security

Communications

This policy establishes the protection of information being changed within and between entities.

UAE IA Results - PRIORITY 2 - Windows 10

Passed Tests = 175
Failed Tests = 700

● Passed Tests ● Failed Tests

T3 Operations Management

Operations Management

The purpose of this policy is to ensure the effective operational control of the security functions related to information and information systems.

UAE IA Results - PRIORITY 2 - Windows 10

Passed Tests = 150

Failed Tests = 925

● Passed Tests ● Failed Tests

T4 Communications

Access Control

The objective of this policy is to institute access control at the user, application, network and operating system level as well as for mobile computing.

UAE IA Results - PRIORITY 3 - Windows 10

Failed Tests = 75

● Failed Tests

T5 Access Control
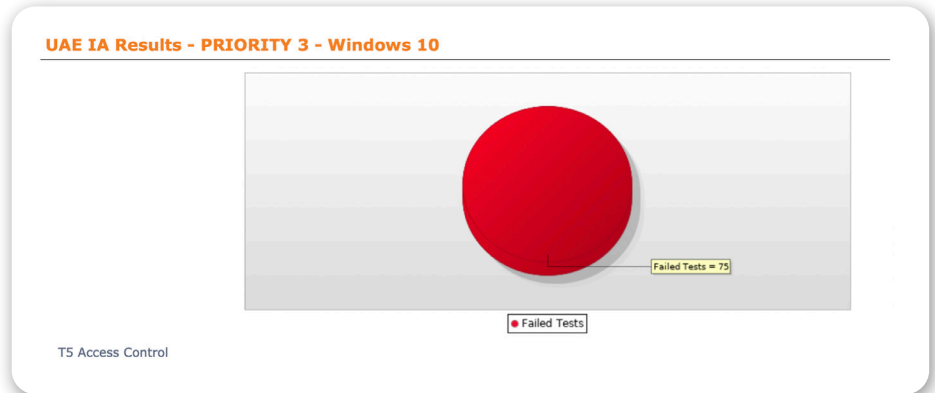
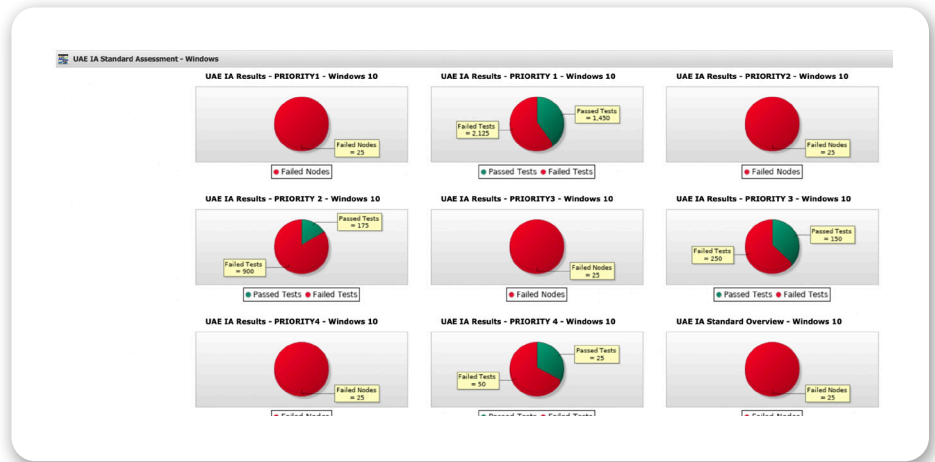## Information Systems Acquisition, Development and Maintenance

The objective of this policy is to prevent information misuse or unauthorized modification and to elevate security levels in applications during development, as well as to manage technical vulnerabilities.

UAE IA Results - PRIORITY 2 - Windows 10

Failed Tests = 25

● Failed Tests

T7 Information Systems Acquisition, Development and Maintenance
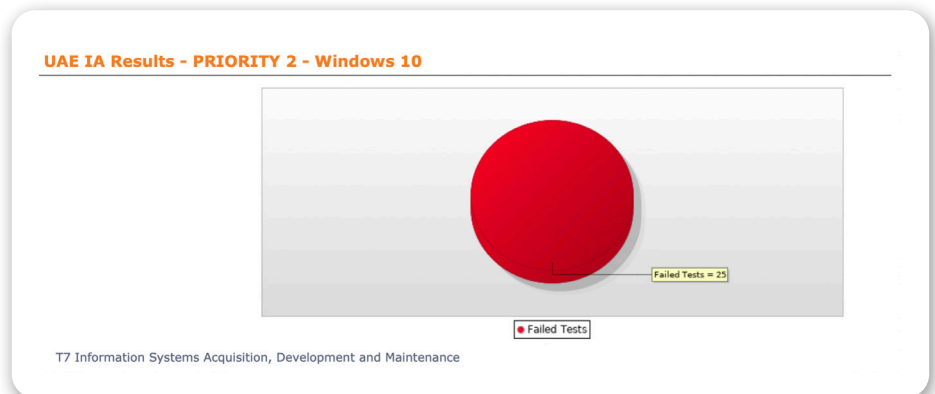
UAE Information Assurance Dashboard in Tripwire Enterprise

UAE IA recommends checking the integrity of the assets and the regular review of system security, system logs and the integrity of system configurations.

UAE IA Standard Assessment - Windows

UAE IA Results - PRIORITY1 - Windows 10 — Failed Nodes = 25

UAE IA Results - PRIORITY 1 - Windows 10 — Failed Tests = 2,125; Passed Tests = 1,450

UAE IA Results - PRIORITY2 - Windows 10 — Failed Nodes = 25

UAE IA Results - PRIORITY 2 - Windows 10 — Passed Tests = 175; Failed Tests = 900

UAE IA Results - PRIORITY3 - Windows 10 — Failed Nodes = 25

UAE IA Results - PRIORITY 3 - Windows 10 — Failed Tests = 250; Passed Tests = 150

UAE IA Results - PRIORITY4 - Windows 10 — Failed Nodes = 25

UAE IA Results - PRIORITY 4 - Windows 10 — Failed Tests = 50; Passed Tests = 25

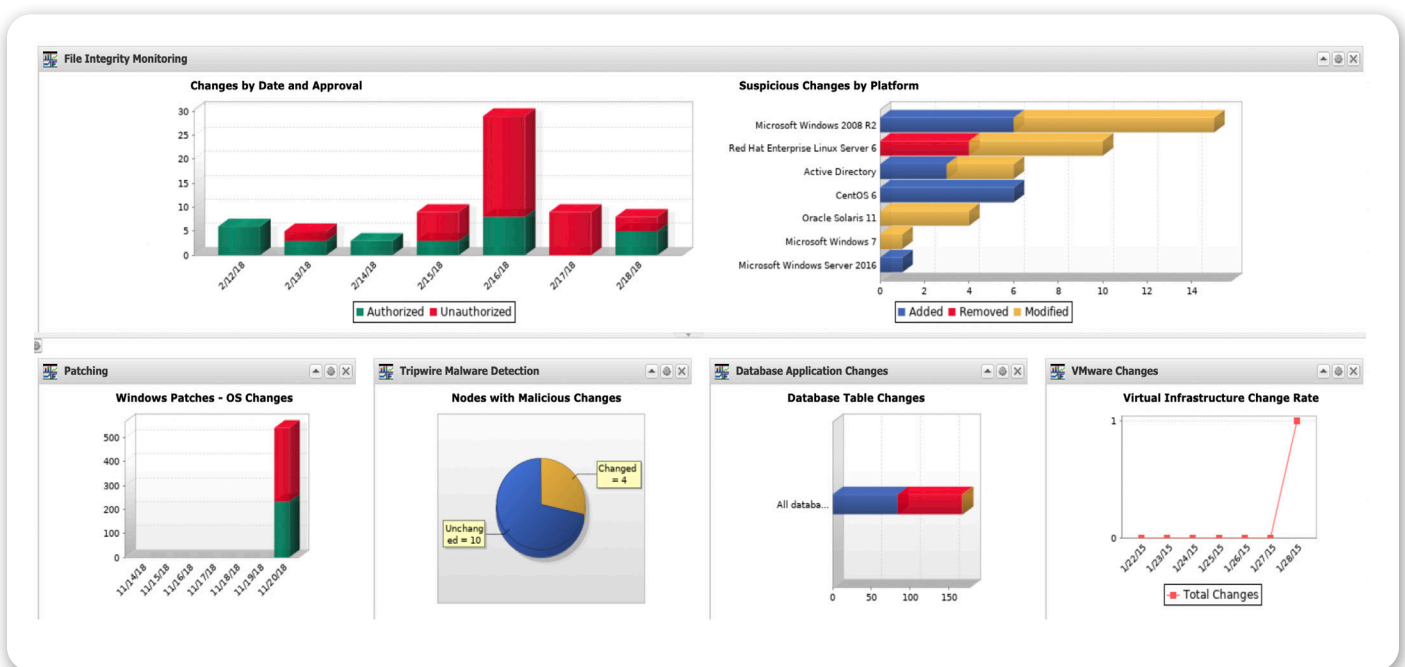UAE IA Standard Overview - Windows 10 — Failed Nodes = 25

What is Tripwire Enterprise?

Tripwire Enterprise is a security configuration management (SCM) suite that provides fully integrated solutions for policy, file integrity and remediation management. Organizations can use these solutions together for a complete end-to-end SCM solution, or use its file integrity monitoring or policy management solutions on their own to address today's pressing security and compliance challenges—while building a foundation that positions them to address tomorrow's.

The suite lets security, compliance and operations teams rapidly achieve a foundational level of security across your entire enterprise, including on-premise, cloud and industrial assets, by reducing the attack surface, increasing system integrity and delivering continuous compliance.

Tripwire has taken its original host-based intrusion detection tool, which could simply detect changes to files and folders, and expanded it into a robust file integrity monitoring (FIM) solution, able to monitor detailed system integrity: files, directories, registries, configuration parameters, DLLs, ports, services, protocols, etc. Additional enterprise integrations provide granular endpoint intelligence that supports threat detection and policy and audit compliance.

File Integrity Monitoring

Changes by Date and Approval — Authorized, Unauthorized

Suspicious Changes by Platform — Added, Removed, Modified
Microsoft Windows 2008 R2, Red Hat Enterprise Linux Server 6, Active Directory, CentOS 6, Oracle Solaris 11, Microsoft Windows 7, Microsoft Windows Server 2016

Patching — Windows Patches - OS Changes

Tripwire Malware Detection — Nodes with Malicious Changes — Changed = 4; Unchanged = 10

Database Application Changes — Database Table Changes — All databa...

VMware Changes — Virtual Infrastructure Change Rate — Total Changes

Tripwire is the trusted leader for establishing a strong cybersecurity foundation. We protect the world's leading organizations against the most damaging cyberattacks, keeping pace with rapidly changing tech complexities to defend against ever-evolving threats for more than 20 years. On-site and in the cloud, our diverse portfolio of solutions find, monitor and mitigate risks to organizations' digital infrastructure—all without disrupting day-to-day operations or productivity. Think of us as the invisible line that keeps systems safe. **Learn more at** tripwire.com

The State of Security: **News, trends and insights at** tripwire.com/blog
Connect with us on LinkedIn, Twitter **and** Facebook