

EMC Ionix IT Compliance Analyzer—Application Edition

Part of the Ionix Data Center Automation and Compliance Family

Automatically validates application-related compliance with IT governance policies

The Big Picture

- Ensure IT compliance with requirements outlined in version 1.1 of the PCI Data Security Standard
- Enforce best practices for planning and maintaining an optimized VMware environment
- Address IT compliance violations before other problems occur
- Identify unauthorized applications and servers
- Ensure applications are configured for maximum performance
- Detect unauthorized communication between unrelated applications
- Verify that all sensitive applications use only secure communications
- Validate that servers are configured for high availability at all times

The size and complexity of information infrastructures continue to increase—as do the number and rate of changes occurring within these IT environments. Data center sprawl, complicated IT interactions, and the dizzying pace of change combine to create tremendous pressure on IT operations to improve performance, security, and reliability across networks, applications, storage systems, and servers. In some cases the pressure comes in the form of industry regulations (such as Sarbanes-Oxley for financial services, HIPAA for healthcare, and PCI for retail) that mandate IT compliance. In other cases, pressure stems from sources inside an enterprise or organization—such as:

- Complying with industry best practices
- Adhering to internal governance initiatives aimed at enhancing operational efficiency, improving security, reducing costs, and increasing service levels (or some combination thereof)

Regardless of the source, these pressures are forcing IT operations to ensure and maintain IT compliance—all while still having to manage the dynamic nature of the information infrastructure and the rapid pace of change in the IT environment. However, a lack of automated solutions for this challenge leaves many IT organizations relying on traditional internal audits—done manually and periodically to provide a “snapshot” at a particular point in time—as their primary approach to gauging IT compliance.

Periodic, manual audits can’t ensure IT compliance

This type of approach introduces significant risk to ensuring IT compliance for many reasons. These include:

- Manual processes may not collect all information needed about the configurations, application and infrastructure dependencies and changes.
- People can collect the wrong information.
- People can collect the right information, but make data entry errors.
- People can make mistakes when trying to determine whether an IT compliance violation exists.
- Periodic snapshot audits offer limited value because the rapid pace of change means that the IT environment you certified as compliant isn’t the same one that exists right now.

Because they can’t ensure IT compliance on an ongoing basis, traditional audits are increasingly becoming unacceptable to enterprises and organizations—as well as third-party auditors. And without having constant, continuously updated information about application configurations and dependencies—as well as any changes made to these—IT operations can’t ensure IT compliance. In short, what’s needed is an automated solution that gives IT operations the capability to proactively:

- Address compliance violations before other problems occur
- Ensure that third-party audits go smoothly

- Roll out new applications with confidence
- Manage the application infrastructure relationships within and across physical and VMware®-enabled environments

An automated solution for ensuring IT compliance

EMC® Ionix™ IT Compliance Analyzer—Application Edition supports compliance analysis for applications in and across physical and VMware-enabled environments.

IT Compliance Analyzer—Application Edition automatically identifies IT configuration violations in a networked environment—based on user-defined policies—and alerts IT operations in real time of any violation of these policies. By automating the validation of application-related configurations, changes, and dependencies, this solution eliminates the risk associated with manual audits and process, while also ensuring realtime compliance for applications on an ongoing basis. With IT Compliance Analyzer—Application Edition, IT operations can validate business-critical applications for compliance with internal governance, external regulatory requirements, industry best practices, or a combination of these. In addition to ensuring IT compliance, this EMC solution can also support and improve operational processes. For example, you can use IT Compliance Analyzer—Application Edition to model and determine whether deployment of a new application would create an IT compliance violation—before you add the application to your IT environment—and without impacting business operations or other IT services.

Harnessing the insight provided by EMC Ionix (formerly Smarts®) Application Discovery Manager

IT Compliance Analyzer—Application Edition leverages the automated discovery power of EMC Ionix™ Application Discovery Manager—an agentless, comprehensive, application discovery, change-impact, and dependency-mapping solution.

Application Discovery Manager, with full support for VMware environments, automatically discovers and captures all critical configuration information—including change details, as well as the critical dependencies that exist between applications and the servers on which they rely. Its unique discovery methods and appliance packaging yield rapid time to value and deliver deep insight that supports the automation of configuration-based operational processes.

When paired with Application Discovery Manager, IT Compliance Analyzer—Application Edition adds unique compliance monitoring, analysis, and policy-violation alerting that help identify violations of external regulations, internal governance policies, and best-practice guidelines.

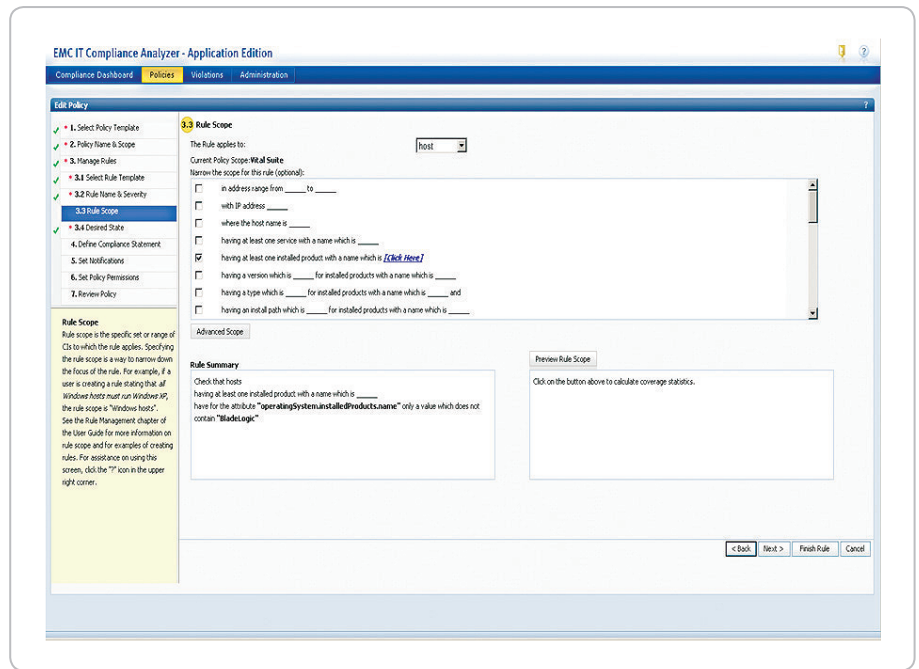
Ensuring IT governance by automating policy-violation processes

IT Compliance Analyzer—Application Edition enables you to create policies that automate the process of identifying, monitoring, and alerting IT operations to policy violations that stem from application configurations, changes, and dependencies. By leveraging automation and customizing policies to manage IT governance, you gain the ability to identify and correct policy violations before they potentially create serious problems.

Policies—which can align with regulatory definitions, internal IT organization definitions, industry best practices, or some combination of these—are correlated with automatically discovered and updated configuration, change, and dependency-mapping data to determine IT compliance on an ongoing basis.

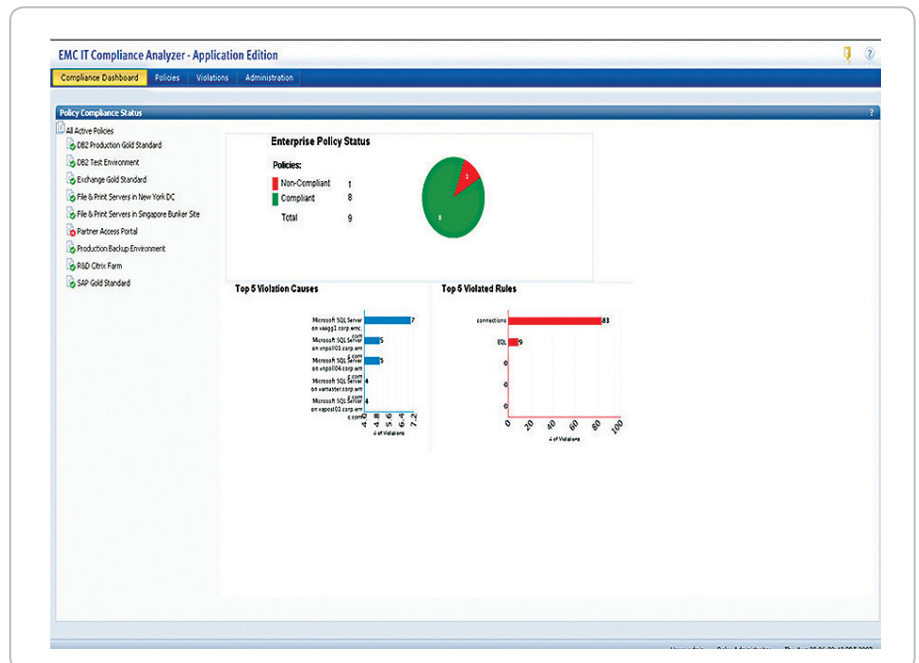
IT Compliance Analyzer—Application Edition defines policies using a simple graphical interface. An easy-to-use policy builder lets you construct your own custom policies or modify the included library of standard policy templates to meet your individual needs. (See the “examples of compliance policies.”) The library of templates includes policies for VMware® best practices and for validating IT compliance against the requirements outlined in version 1.1 of the PCI Data Security Standard. When a policy violation occurs, IT operations immediately receives an alert about the change that caused the violation.

The simple graphical interface in EMC IT Compliance Analyzer—Application Edition’s policy builder allows you to easily create custom policies or modify existing policies or templates to meet specific needs.



Not all conditions affect a policy equally. Some can be critical, while others are minimal. IT Compliance Analyzer—Application Edition allows you to take this variability into account by assigning priorities to your conditions. By evaluating each priority according to its thresholds, IT Compliance Analyzer—Application Edition can more accurately measure overall policy compliance. For example, high-priority critical violations can generate a policy compliance exception easily, while multiple low-priority violations might be needed to generate a policy compliance exception. And because thresholds are configurable for each policy, you can customize IT Compliance Analyzer—Application Edition to meet your specific needs.

The interface was designed to be simple, intuitive, and easy to use.



Easy-to-use interface

You can also view other aspects of policy management in the dashboard (as well as other views). In addition, the interface can be customized to create user-specific and role-specific layouts that are suited to specific roles or individuals (for example, creating a unique view that reflects the different interests and privileges of the compliance officer).

Examples of compliance policies

The flexibility and value of IT Compliance Analyzer is illustrated using some examples from actual compliance policies. These conditions, which test the configuration data provided by Application Discovery Manager, are defined in plain wording.

Examples of configuration checks include:

- **Check that web servers in the Human Resources and Finance departments that are running Red Hat Linux 3 have had update No. 6 applied**—Validates a configuration.
- **Check that Oracle 10g database servers in New York and Chicago have their shared pool size set to no more than 3,500,000**—Tests an application detail settings, but qualifies that test by narrowing the scope to the two cities.
- **Check that all client connections from the call center to the credit card authorization system use a secure protocol**—Verifies the relationship between an application transaction and the network protocol it uses.

Examples of managing best practices in VMware environments include:

- **Check that all virtual machines are actively managed by VirtualCenter**—Ensures that no “rogue” ESX Servers are on the network.
- **Check that there are no more than 30 virtual machines on a single ESX Server**—Keeps hardware resources from being over-utilized.

- **Check that there are no more than 4 virtual CPUs per VM on one ESX Server**—Complies with proven performance recommendations from VMware.
- **Check that all VMs have VMware Tools installed and running**—Ensures that the latest VM management software is installed and running.

Examples of ensuring minimum standards include:

- **Check that all Oracle DB servers used for the inventory application have two CPUs and at least 4 GB of memory**—Evaluates if a specific type of server has enough resources to support the application’s demands.
- **Check that Windows systems in Memphis have anti-virus software installed**—Looks for specific security elements.

Examples of supporting security policies include:

- **Check that the Oracle servers in Seattle don’t have floppy drives**—Supports security policies by ensuring servers have no removable media.

- **Check that retail web servers and their back-end databases aren’t running on the same host**—Shows how a policy can also reflect performance guidelines by ensuring that two specific software elements are located on separate physical hosts.
- **Check that there are no connections between Apache Web servers in the DMZ and application servers in the Accounting department**—Guarantees that no suspect connections exist from the DMZ to a sensitive internal system.
- **Client connections from the call center to the credit card authorization servers must use a secure protocol**—Ensures that sensitive customer information is protected.

Examples of testing for the absence of conditions include:

- **Check that no more than 100 web-based clients are connected to each web server in the EMEA region**—Ensures that a performance rule has not been exceeded.
- **Check that Windows systems in North America don’t have Kazaa installed**—Tests for the non-existence of certain software.
- **Check that Windows 2003 file servers in Miami have no connections that use ports 80, 443, or 8080**—Tests for potential points of network-based attacks.

The automated IT governance solution for applications

As enterprises and organizations across industries increasingly emphasize the importance of IT compliance and governance policies, you need a solution that can help ensure IT compliance by analyzing application configurations, changes, and dependencies according to your specific IT policies, and alerting you automatically when policy violations occur.

By eliminating the cumbersome, time-consuming, resource-intensive, and error-prone manual methods commonly used to assess compliance and governance, IT Compliance Analyzer—Application Edition ushers in a new era of control over application configurations. With IT Compliance Analyzer—Application Edition, IT operations can now help ensure strong self-governance through policies defined by business-specific requirements, professional best practices, and regulatory directives.

The simple graphical interface in EMC IT Compliance Analyzer—Application Edition’s policy builder allows you to easily create custom policies or modify existing policies or templates to meet specific needs.

About EMC

EMC Corporation is the world's leading developer and provider of information infrastructure technology and solutions that enable organizations of all sizes to transform the way they compete and create value from their information. Information about EMC's products and services can be found at www.EMC.com.



EMC Corporation
Hopkinton
Massachusetts
01748-9103
1-508-435-1000
In North America 1-866-464-7381
www.EMC.com

Take the next step

To learn more about how EMC Ionix IT Compliance Analyzer—Application Edition and other EMC resource management solutions can positively impact your business and IT operations, contact your local EMC representative, call us at 1-866-464-7381 (North America) or visit our website at www.EMC.com.