Tivoli Endpoint Manager for Configuration Management

User's Guide

Note: Before using this information and the product it supports, read the information in Notices.

Contents

Part One 1

Introduction 1

System requirements 1

Installing Configuration Management 1

Part Two 3

Fixlets and Analyses 3

Check Fixlets 3

Modifying check parameters 5

Taking a remediation action 5

Measured Value Analyses 6

Part Three 7

Creating and managing custom checklists 7

Creating Custom Checklists 7

Customizing content 8

Configuration Management Reporting 9

Part Four 11

Support 11

Frequently asked questions 11

Technical support 12

Part Five 13

Notices 13

Part One

Introduction

This guide describes a portfolio of security configuration content called Configuration Management. This content is organized through checklists, which assess and manage the configurations of desktops, laptops, and servers. The Configuration Management solution has achieved Security Content Automation Protocol (SCAP) certification with the National Institute of Standards and Technology (NIST) for both misconfiguration assessment and remediation. By offering an extensive library of technical checks, Configuration Management detects and enforces security configuration policies using industry best practices.

This guide serves as a resource for IT personnel responsible for managing and enforcing corporate system configuration policies on endpoints. The Configuration Management checklists allow security teams to define the security parameters and configurations required by corporate policy. IT managers use the Configuration Management checklists to enforce security policies and document the current state of compliance against corporate policies. Tivoli Endpoint Manager console operators focus on the detailed day-to-day configuration management of all systems to use detailed information for each endpoint. Auditors use Configuration Management checklists to determine the current state of compliance for systems within the entire organization.

System requirements

Configure your Tivoli Endpoint Manager deployment according to the following requirements:

Minimum supported browser versions:

- Internet Explorer 7.0 or later

Minimum Adobe Flash player version:

- Flash Player 9.0 or later

Minimum Tivoli Endpoint Manager component versions:

- Console 8.0 or later
- Windows Client 8.0
- UNIX Client 7.2.5.21

Installing Configuration Management

Each Configuration Management checklist is provided as a single site and represents a single standard and platform. When added to a Tivoli Endpoint Manager deployment, the content is continuously updated and automatically delivered. Computers must be subscribed to the site to collect data from Tivoli Endpoint Manager clients. This data is used for reporting and analysis.

The process of site subscription depends on the version of the Tivoli Endpoint Manager console that you have installed. For more information about site subscription, see the Knowledge Base article **here**.

Alternatively, an air-gap can be used to physically separate the Tivoli Endpoint Manager server from the Internet Fixlet server. For more information, see http://support.bigfix.com/bes/install/airgapnetwork.html.

The Fixlets in this site can be used as-is or customized to meet your own security policies. Compliance calculations are evaluated locally on each endpoint, and the Configuration Management solution is scalable and can accommodate large numbers of computers.

You can choose to copy Configuration Management content to custom sites. This allows you to customize the content.

Part Two

Fixlets and Analyses

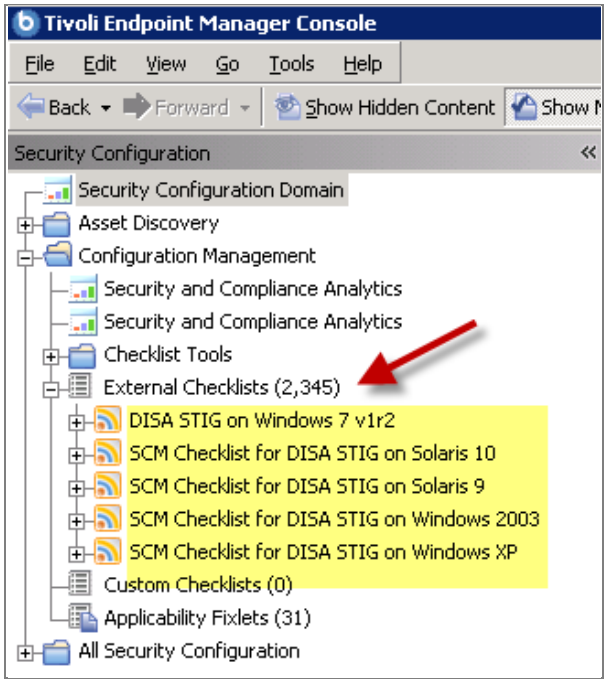
Check Fixlets in Configuration Management checklists assess an endpoint against a configuration standard. Many check Fixlets have a corresponding analysis, sometimes referred to as *measured values*, which report the value of the element that the check Fixlet evaluates.

Check Fixlets

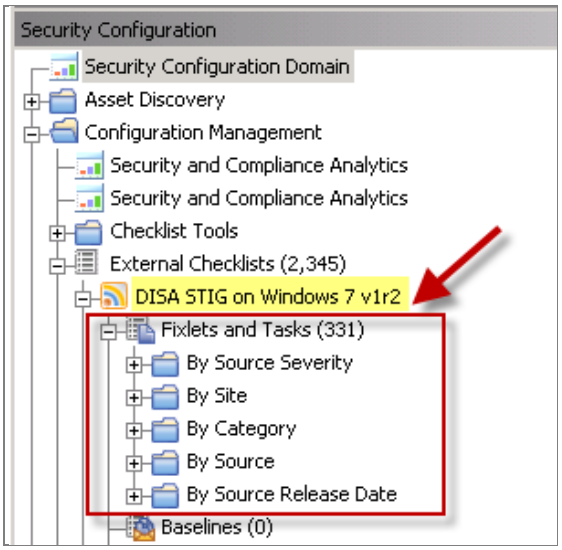
A check Fixlet becomes relevant when a client computer is out of compliance with a configuration standard. By viewing the Configuration Management Fixlets, you can identify non-compliant computers and the corresponding standards.

To start using the Configuration Management checklists, obtain a masthead for the appropriate Configuration Management site and open it within the Tivoli Endpoint Manager console. When the site has been gathered in the console, follow the steps below to view the checks:

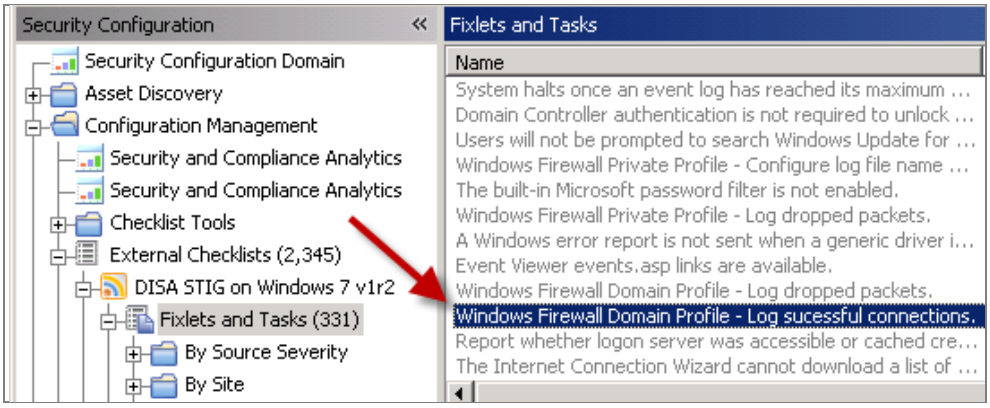
1. Select a Configuration Management checklist from the navigation tree.



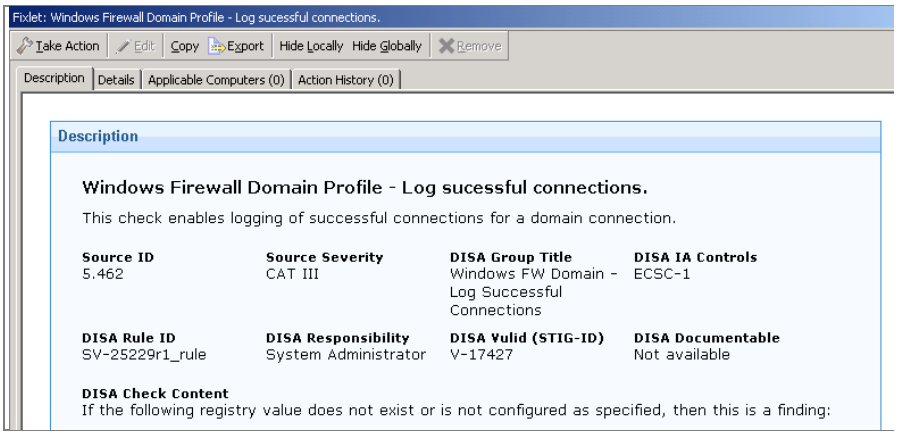
2. Expand a checklist and click *Fixlets and Tasks.*



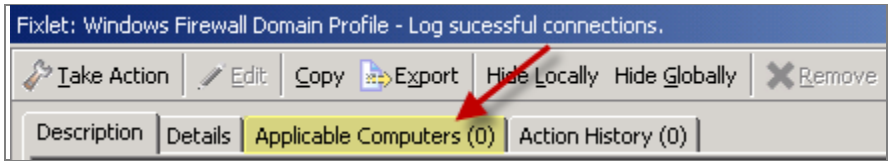
3. Click one of the Fixlets displayed in the list. The Fixlet opens with the following tabs: *Description, Details, Applicable Computers,* and *Action History*. Click the *Description* tab to view the text describing this Fixlet.



The Fixlet window typically contains a description of the check, options to customize the configuration setting, and a related Action to remediate one or more systems to the expected configuration value.



The Fixlet is applicable to a subset of endpoints on your network. The size of that subset is shown in the Applicable Computers tab.



Note: *UNIX controls provide custom parameterization, but through a different mechanism. For more information, see the Configuration Management Checklists Guide for Windows and UNIX.*

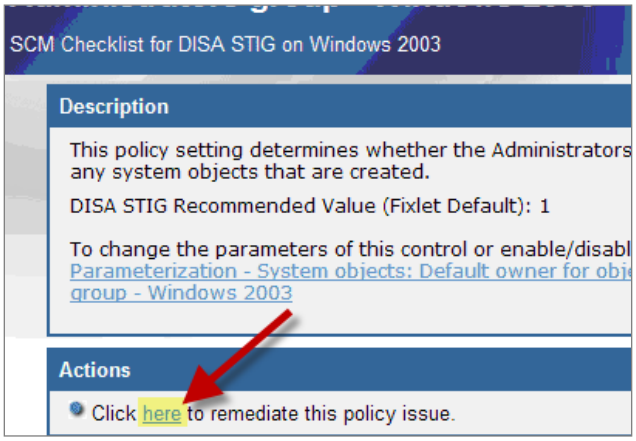
Modifying check parameters

In addition to monitoring compliance status and remediating settings that are out of compliance, you can also modify the parameters used in determining the compliance of the checks. For example, you can set the minimum password length on an endpoint to 14 characters. You can customize the password-length parameter to your specific policy.

For more information about modifying check parameters, see the *Configuration Management Checklists Guide for Windows and UNIX.*

Taking a remediation action

Many Fixlet controls have built-in Actions to remediate an issue. To start the remediation process, click the link in the Actions box.



The Take Action dialog opens, where you can target the computers that you want to remediate. For more information about the Take Action dialog, see the Tivoli Endpoint Manager Console Operator's Guide.

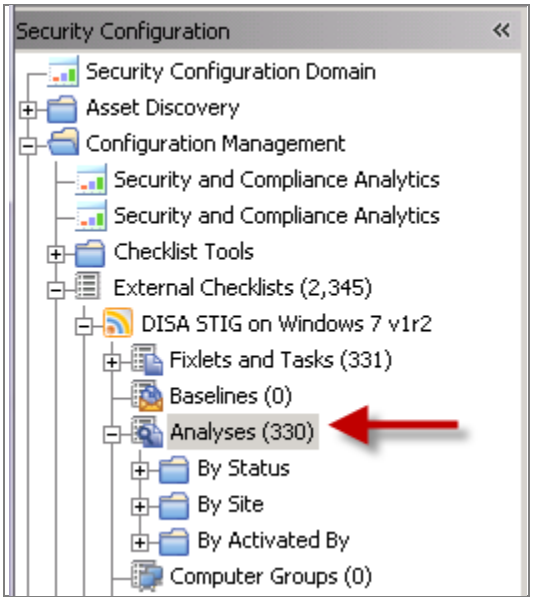
A remediation action typically sets a value in a file or in the Windows registry. Most UNIX remediations run the runme.sh file for the appropriate check. This action applies the recommended value shipped with the product or the customized parameter you set according to your own corporate policy.

After you have targeted a set of endpoints, click *OK* and enter your Private Key Password to send the action to the appropriate endpoints. While the actions are run on the endpoints and the setting is remediated, you can watch the progress of the actions in the console.

When every endpoint in a deployment is brought into compliance, the check Fixlet is no longer relevant and is removed from the list of relevant Fixlets. Although the Fixlets are no longer listed, they continue checking for computers that deviate from the specified level of compliance. To view them, click the "Show Non-Relevant Content" tab at the top of the console window.

Measured Value Analyses

In addition to check Fixlets, some checklists include analyses that provide the actual values of the items being checked. Measured values are retrieved using analysis properties. You can find measured value analyses by clicking the Analyses subnode within any checklist.



Note: *For best performance, only activate the analyses that you need for your deployment. Only activated analyses are visible in SCA.*

Part Three

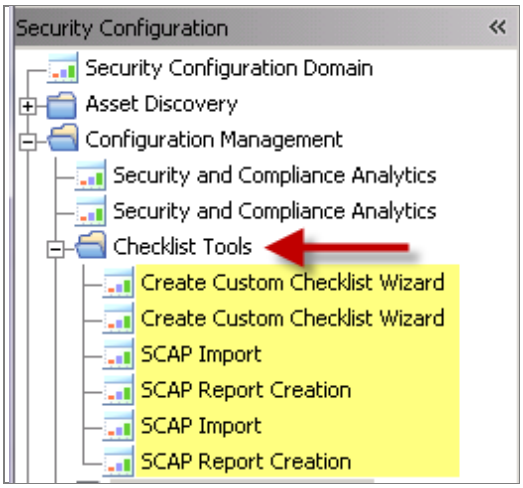
Creating and Managing Custom Checklists

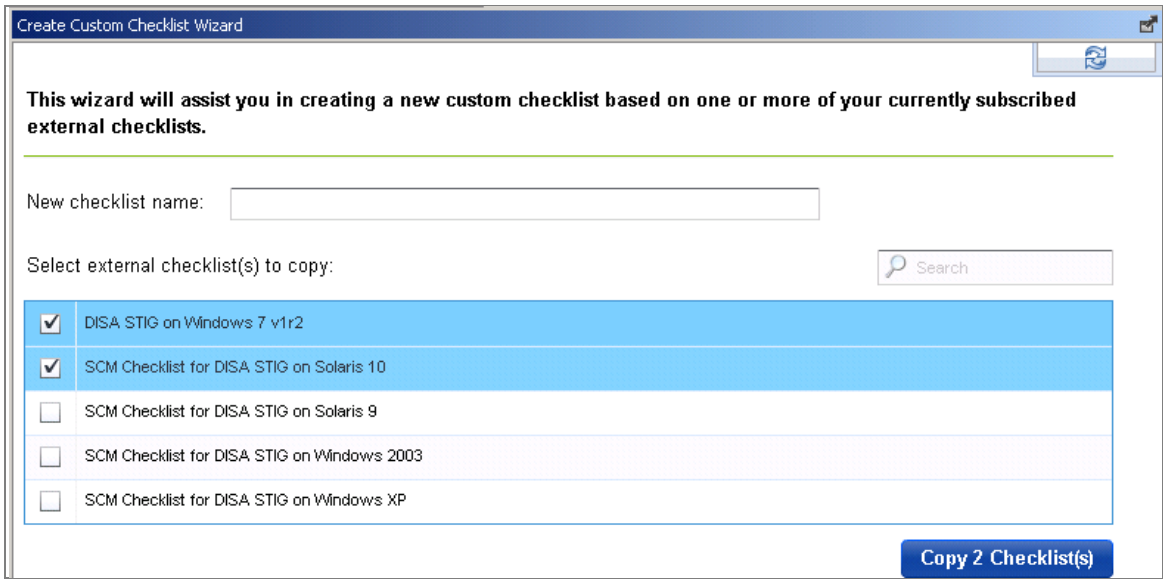
The ability to customize Configuration Management parameters and exclude specific computers from an analysis gives you control over your security status. However, you can also use custom checklists to fine-tune the settings monitored in your deployment. Custom checklists target specific sets of computers with tailored content using the subscription mechanism. This allows statistics to be gathered with finer granularity. To create your own checklist with custom sites, perform the following steps.

Step 1: ***Create*** *a custom checklist from an existing external checklist*
Step 2: ***Customize*** *Fixlets using built-in parameterization*
Step 3: ***Subscribe*** *the proper computers to the custom checklist*

Creating Custom Checklists

Click the *Checklist Tools* folder in the navigation tree to access the Create Custom Checklists wizard.





Before creating a custom checklist, you must be subscribed to the Configuration Management Reporting external site. To create a custom checklist based on existing external checklists, perform the following steps:

1. Open the *Create Custom Checklist* wizard (located in the *Checklist Tools* folder of the main menu).
2. Type in a name for your new custom site in the appropriate text box.
3. Select one or more checklists that you want to copy into your new custom list. If you are subscribed to a large number of checklists, you can use the *Search* box to filter the displayed checklists.
4. Click *Copy # Checklist(s)* at the bottom of the window.
5. Enter your private key password.

The console begins copying the checks in the selected lists into your new custom checklist. Depending on the number and size of the checklists selected, this might take several minutes.

Use care when subscribing computers to custom checklists. Custom checklists do not support site relevance, which protects you from bad subscriptions. For more information about subscribing computers to sites, see the Tivoli Endpoint Manager Console Operator's Guide.

Customizing content

Now that you have a custom checklist populated with content copied from external checklists, you can configure your checklist by any of the following means:

- Configure check parameters to control remediation
- Delete unwanted or unnecessary checks

For more information about these steps, see the Configuration Management Checklists Guide and the Custom Fixlet Authoring documentation.

> **Note:** *In Console versions 8.0 and later, subscribing computers to a custom checklist site is handled in the same way as with External checklist subscriptions (see previous section entitled "Subscribing computers to Configuration Management checklist sites").*

Configuration Management Reporting

In previous releases, the primary reporting tools for the Configuration Management solution included the Configuration Management dashboard, Exception Management dashboard, and Web Reports. These tools, while still accessible for customers with previously-saved reports and exceptions, have now been superseded by the *Security and Compliance Analytics* (SCA) product, which is included in all Configuration Management subscription packages.

For more information about SCA, see the documentation **here**.

Part Four

Support

Frequently asked questions

Can I parameterize all checks?

Not all checks can be parameterized using the Fixlet user interface we provide. In cases where a check can be parameterized, the method depends on the type of content. See the Configuration Management Checklists Guide for more information.

Are remediation actions available for all checks?

Remediation actions are available for a subset of checks.

Where can I find a sample file containing UNIX parameters?

See the Configuration Management Checklists Guide.

Are there compliance evaluation reports/mechanisms that compare a laptop or server against FISMA/NIST/DISA standards?

Configuration Management checks assess servers, laptops, and desktops against a predefined set of configuration guidance such as DISA STIG and FDCC.

Tivoli Endpoint Manager also supports configuration standards from NIST, NSA, and other standards organizations. Regulatory compliance regulations such as FISMA, PCI, and others can easily be supported by customizing the checklists provided by IBM.

What happens if I subscribe sites incorrectly to a system?

Each Configuration Management site applies to a specific operating system or product. It is important that each computer subscribed to each site matches the correct operating system configuration. This ensures the accuracy of the compliance results for each Configuration Management site, and prevents potential performance issues. External sites contain site relevance to ensure that only applicable computers are subscribed. However, custom sites do not support site relevance, so you are responsible for maintaining accurate subscriptions.

When I run a remediation action on a UNIX endpoint, how do I ensure that a system is not remediated more than once?

When a remediation action is run, the remediation action reruns the detection script. When the detection script is run, it provides the validation of whether or not the remediation was successful. If successful, the Fixlet becomes non-relevant. If unsuccessful, the Fixlet remains relevant.

What does the letter designation mean on the end of some of the scripts within the UNIX content?

We used the DISA STIG unique identifiers as part of the naming convention for each DISA STIG control that was built. In the case where we had to separate a single control into multiple scripts, the scripts include a letter designator on the end that provides a unique ID for each control.

What is the security associated with the base parameter file that defines the parameters for the UNIX content?

The standard permissions for this file are 700 (RWE for the owner of the file). In this case, the owner must be root or whichever user is the owner of the BES Client.

Technical support

IBM offers a number of specialized support options to help you learn, understand, and optimize your use of this product:

- Tivoli Endpoint Manager Info Center
- BigFix Support Site
- Documentation
- Knowledge Base
- Forums and Communities

Part Five

Notices

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
1623-14, Shimotsuruma, Yamato-shi
Kanagawa 242-8502 Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
2Z4A/101
11400 Burnet Road
Austin, TX 78758 U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS", without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.

TRADEMARKS:

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both.

If these and other IBM trademarked terms are marked on their first occurrence in this information with a trademark symbol (® or ™), these symbols indicate U.S. registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at http://www.ibm.com/legal/copytrade.shtml.

Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Other company, product, and service names may be trademarks or service marks of others.