

*IBM Endpoint Manager for  
Configuration Management User's  
Guide*

**IBM**



---

# Contents

## Configuration Management User's Guide 1

Setting up Configuration Management. . . . .	1
System requirements. . . . .	2
Using checks and checklists . . . . .	3
Check Fixlets . . . . .	3
Modifying check parameters . . . . .	5
Activating Measured Value Analyses . . . . .	5
Creating and Managing Custom Checklists . . . . .	6
Using the Synchronize Custom Checks wizard . . . . .	7
Taking a remediation action . . . . .	9
Configuring Windows checklists . . . . .	10
Viewing checks . . . . .	11
Activating prerequisite Fixlet tasks. . . . .	11
Modifying Windows check parameters . . . . .	11
Remediation of Windows configuration settings . . . . .	12
Configuring UNIX checklists . . . . .	12
Configuring checklists. . . . .	13
Analyses . . . . .	22

Using the Create Custom Relevance SCM content wizard . . . . .	22
Creating custom UNIX Security Configuration Management content . . . . .	23
Importing SCAP content . . . . .	24
Learning about SCAP . . . . .	24
SCAP Checklists. . . . .	27
Using the Import Windows SCAP Wizard . . . . .	27
Using the Report Creation wizard . . . . .	29
Using OVALDI . . . . .	29
Configuration Management Reporting . . . . .	30
Frequently asked questions . . . . .	30
Glossary . . . . .	31
Support . . . . .	35
Notices. . . . .	35
Programming interface information . . . . .	38
Trademarks . . . . .	38
Terms and conditions for product documentation . . . . .	38



---

# Configuration Management User's Guide

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) validation 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.

---

## Setting up Configuration Management

Follow these steps to set up your Configuration Management deployment.

Follow these steps to set up Configuration Management

1. Plan your Configuration Management deployment.
2. Subscribe to the external SCM sites.
3. Create custom sites or custom checklists.

### Planning your Configuration Management deployment

Keep in mind the following steps as you plan your configuration management deployment.

1. Identify which computers will run the Configuration Management content.
2. Group the computers by operating system.
3. Create subgroups within each operating system that must comply with the different standards.

### Subscribing to sites

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

The process of site subscription depends on the version of the Endpoint Manager console that you installed. For more information, see the Administrator's User Guide.

Alternatively, an air-gap can be used to physically separate the Endpoint Manager server from the Internet Fixlet server. For more information, see [Installing in an Air-Gapped Network](#).

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 so you can customize the content.

## Creating custom sites

As each Configuration Management checklist is provided as a single site, when you create a custom site, you are in effect, creating a custom checklist.

Use custom checklists to fine-tune the settings that are monitored in your deployment. You can customize Configuration Management parameters and exclude specific computers from an analysis. Custom checklists target specific sets of computers with tailored content with the use of the subscription mechanism.

Creating custom checklists involves the following steps

1. Create a custom checklist from an existing external checklist.
2. Customize Fixlets using built-in parameterization.
3. Subscribe the correct computers to the custom checklist.

You can use the Create Custom Checklist wizard to create new custom checklists that are based on your currently subscribed external checklists. For more information, see [Creating custom checklists](#).

## System requirements

Set up your deployment according to the system requirements to successfully deploy Configuration Management.

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

*Table 1. Supported components and system requirements to deploy Configuration Management*

Components	Requirements
Supported browser versions	Internet Explorer 7.0 or later
Adobe Flash player version	Flash Player 9.0 or later
IBM Endpoint Manager component versions	<ul style="list-style-type: none"> <li>• Console 8.0 or later</li> <li>• Windows Client 8.0</li> <li>• UNIX Client:               <ul style="list-style-type: none"> <li>– Superseded version: IBM Endpoint Manager UNIX Client 7.2</li> <li>– Non-superseded version: IBM Endpoint Manager UNIX Client version 8.1.551.0</li> </ul> </li> </ul>

## Using checks and checklists

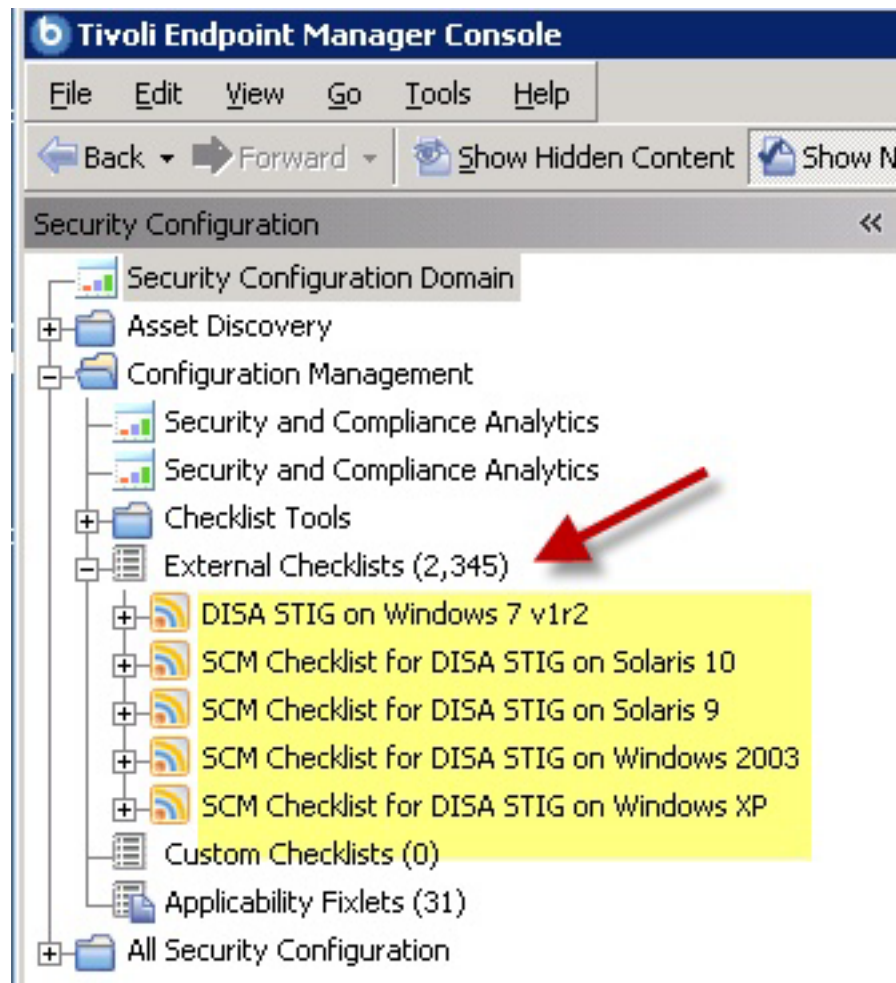
Check Fixlets in Configuration Management checklists assess an endpoint against a configuration standard. Many check Fixlets have a corresponding analysis, sometimes referred to as *measured values*, which report the value of the element that the check Fixlet evaluates.

### Check Fixlets

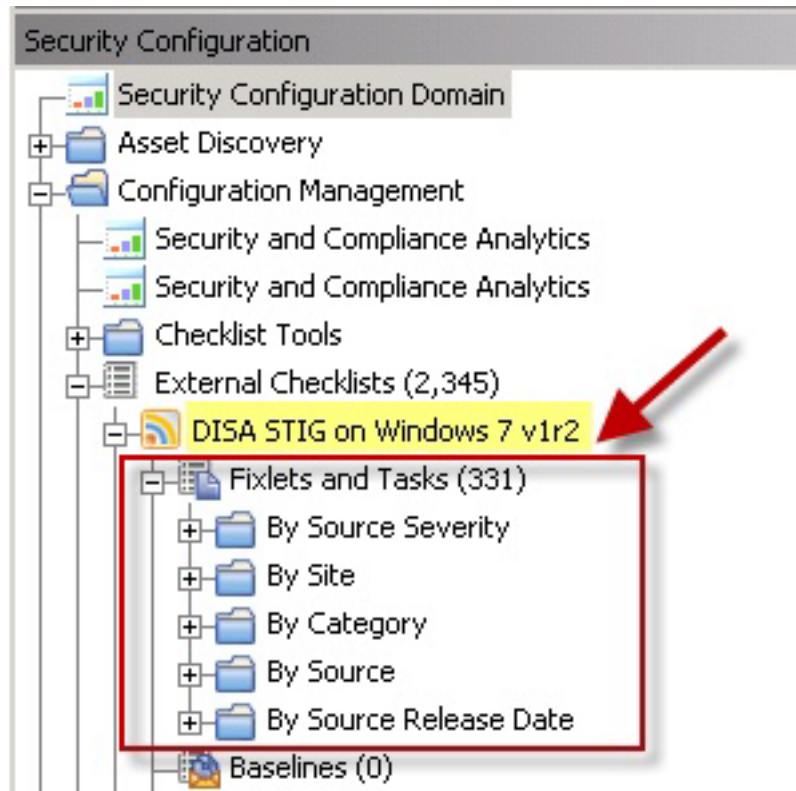
A check Fixlet becomes relevant when a client computer is out of compliance with a configuration standard. By viewing the Configuration Management Fixlets, you can identify non-compliant computers and the corresponding standards.

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:

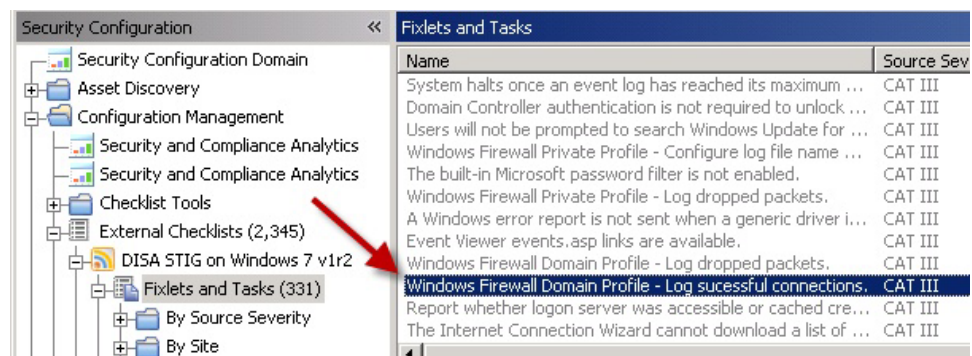
1. Select a Configuration Management checklist from the navigation tree.



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

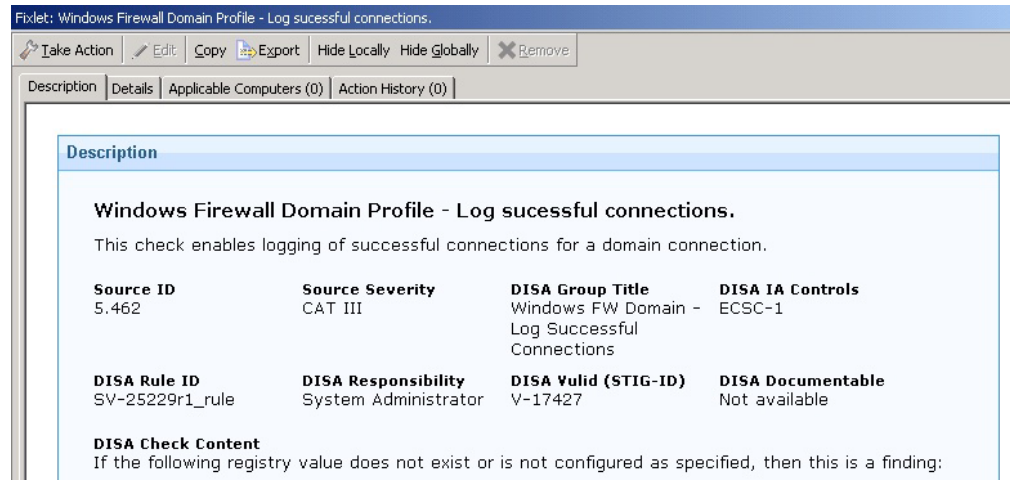


3. Click one of the Fixlets displayed in the list. The Fixlet opens with the following tabs: *Description*, *Details*, *Applicable Computers*, and *Action History*. Click the *Description* tab to view the text describing this Fixlet.

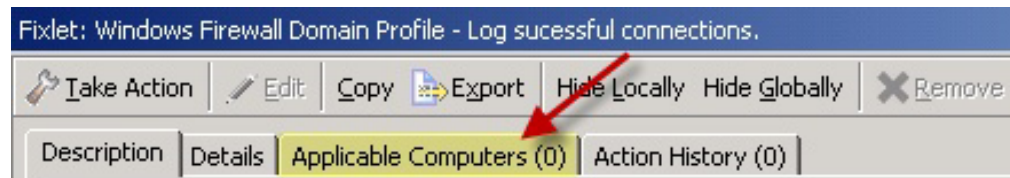


The Fixlet window typically contains a description of the check, options to customize the configuration setting, and a related Action to remediate one or more systems to the expected configuration value.





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

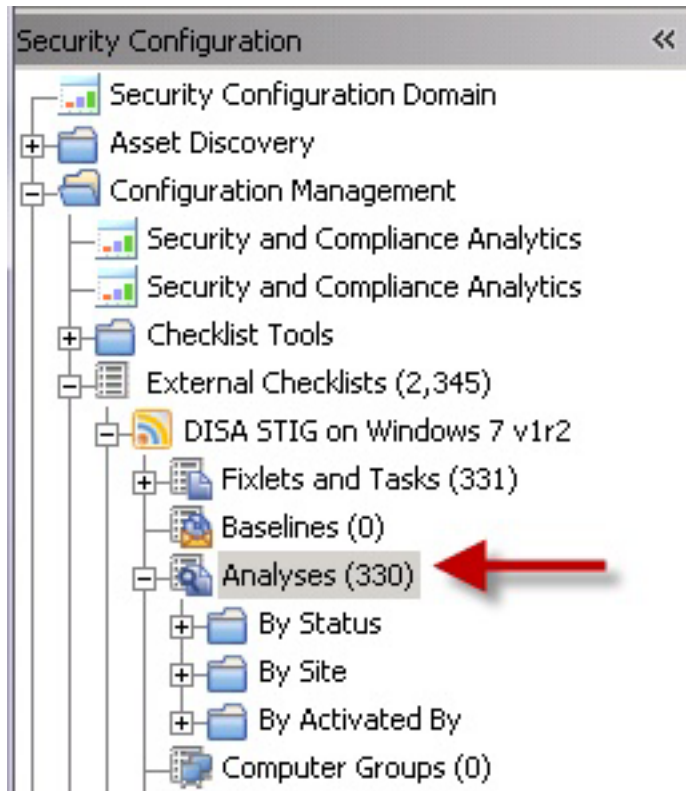
In addition to monitoring compliance status and remediating settings that are out of compliance, you can also modify the parameters used in determining the compliance of the checks. For example, you can set the minimum password length on an endpoint to 14 characters. You can customize the password-length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

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

## Activating Measured Value Analyses

Click the Analyses subnode within a checklist to find 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.

## 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.

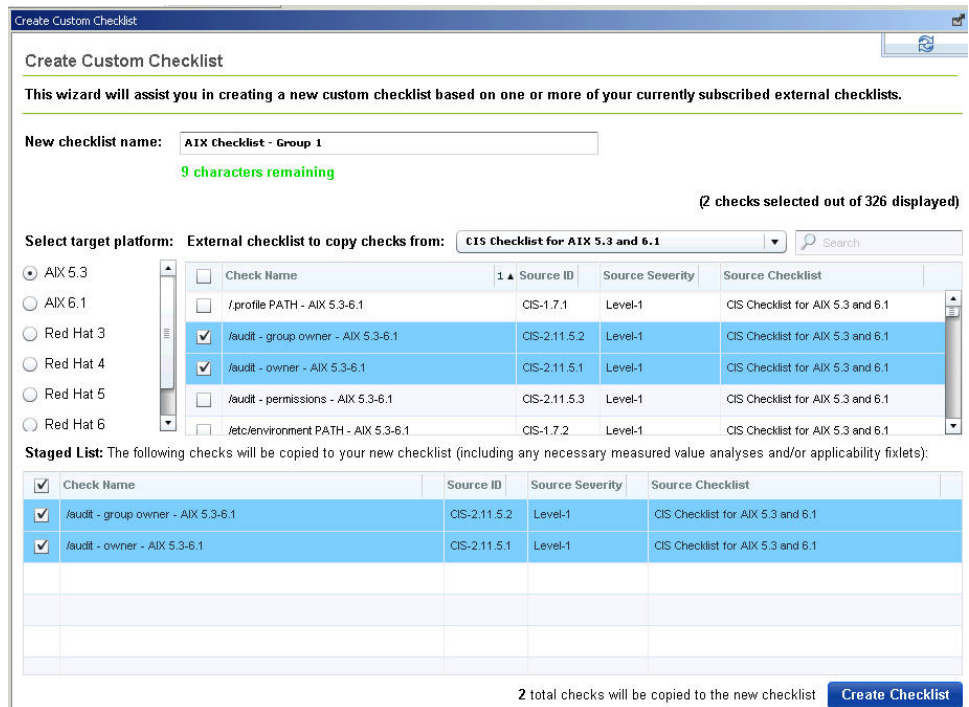
- Step 1: Create a custom checklist from an existing external checklist
- Step 2: Customize Fixlets using built-in parameterization
- Step 3: Subscribe the proper computers to the custom checklist

### Creating custom checklists

Use this wizard to create custom checklists.

You must be subscribed to the SCM Reporting external site.

1. From the **Security Configuration Domain**, go to **Configuration Management > Checklist Tools > Create Custom Checklist**.



2. Enter the name of the new checklist.
3. Select the target platform.
4. Click the drop-down menu to select which external checklist you will copy the checks from. As you select the checks, they are shown in the staged list at the lower part of the window.
5. Click **Create Checklist**.

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

**Note:** Use care when you subscribe computers to custom checklists. Custom checklists do not support site relevance, which protects you from bad subscriptions.

## 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

**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.

## Using the Synchronize Custom Checks wizard

Use the SCM Synchronize Custom Checks wizard to update any custom checks in your deployment whose external sources have since been updated by IBM. You

can use any additional functionality or bug fixes that may have been provided by IBM (in the form of external site updates) since the custom copies were made.

To synchronize a custom checklist, you must have the latest version of the Create Custom Checklist wizard (SCM Reporting version 36 or later). The latest version of the wizard adds required metadata to the copied checks that allows the sync wizard to determine whether the current external source has been modified since the copy was made.

- First time SCM user

If your Endpoint Manager deployment does not have any custom checklists that were created prior to the release of the sync wizard, any custom checklists you create from now on will be compatible with the Synchronize Custom Checks wizard.

- Existing SCM user and you used the previous version of the Create Custom Checklist wizard

If you already have one or more custom checklists created with an older version of the Create Custom Checklist wizard, you will have to first recreate these and any other custom checklists that you wish to have synchronizing abilities using the latest version of the Create Custom Checklist wizard.

## Scanning for out-of-date checks

You can make basic global scans or detailed targeted scans for out-of-date checks.

The custom checklist that you will synchronize must be created with the latest version of the Create Custom Checklist wizard (SCM Reporting version 36 or later).

This wizard scans all SCM custom checklists for external updates, and displays the checklists that need an update or synchronization in the table. Please note that this scan will not detect checks that have been added to or removed from an external site.

The detailed targeted scan requires the user to select a source checklist (external) and a destination checklist (custom) before performing the scan. This scan does a limited scan that performs a comparison of the source and destination checklists to determine whether or not there are any: out of date custom checks, newly added external checks, or recently removed external checks.

This scan is designed for use only in cases where the user intends to maintain an up-to-date copy of an entire external checklist. If the destination was not originally created as a copy of the source, the results of this scan may be confusing and/or misleading; however, there are no hard restrictions to this end, and the user may perform a detailed targeted scan comparison between any external and custom checklist pair.

1. Select the appropriate tab.
  - Basic Global Scan
  - Detailed Targeted Scan
    - a. Select the source from the external checklists.
    - b. Select the destination of the custom checklist.
    - c. Option: Click the **Only show** drop-down menu to select from the filter choices.
2. Click **Scan** to scan for out-of-sync checks.

## Synchronizing out-of-date checks

Custom parameterizations will be automatically preserved.

1. From the Out of Sync Checks window, select the checkboxes in the left-most column.
2. Click **Synchronize** in upper left corner. A progress indicator box displays the percentage complete and an estimated remaining time to complete the synchronization operation. You can also cancel the operation at any time from this window.

**Note:** The synchronization process can take a number of seconds per check. Keep in mind when synchronizing large sets of checks at a time.

## Preserving custom remediation actions

Follow these steps to preserve manually edited remediation action scripts for checks in your custom checklists.

Normally, synchronizing a custom check overwrites the existing remediation action, if there are any, with the latest from the external source. However, if you manually edited the remediation action script for checks in your custom checklists, you can preserve this custom action after synchronizing.

**Note:** Preserving a custom action in this way prohibits this check from receiving updates and bug fixes to the remediation action portion of the check. This option is only suggested for cases in which the user is sure that the action of the source check is either missing or incorrect, or if your security policy calls for remediating the check in a custom manner.

1. From the **Synchronize Custom Checks** wizard, click the name of the custom check. The corresponding Fixlet opens.
2. Click **Edit** at the upper part of the Fixlet window. In the window that opens, click the **Actions** tab.
3. Select the wanted action in the first list. In most cases, there is only one.
4. Add / SCMSyncManager: NO\_SYNC to the first line of the **Action Script** text box.

## 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.

## System objects: Default owner for object Administrators group - Windows 2003

SCM Checklist for DISA STIG on Windows 2003

### Description


This policy setting determines whether the Administrators group is the default owner for any system objects that are created.

DISA STIG Recommended Value (Fixlet Default): 1

To change the parameters of this control or enable/disable it, see [Parameterization - System objects: Default owner for object Administrators group - Windows 2003](#)

### Actions

Click [here](#) to remediate this policy issue.



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.

---

## Configuring Windows checklists

The Configuration Management checklists for Windows systems are delivered as a set of Fixlets and tasks that can help you find the information you need to manage your deployment.

## Viewing checks

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 noncompliant computers and the corresponding standards.

You need a masthead for the appropriate Configuration Management site. For a list of SCM Checklists, see the SCM Checklists wiki. From the Endpoint Manager console, gather the site and do the following steps to view the checks.

1. Select a Configuration Management checklist from the navigation tree.
2. Expand a checklist.
3. Click **Fixlets and Tasks**. The **Fixlets and Tasks** section opens on the right.
4. Click one of the Fixlets that is displayed in the list. The Fixlet opens with the following tabs: Description, Details, Applicable Computers, and Action History.
5. Click the **Description** tab to view the text that describes the Fixlet. The Fixlet window typically the following details: 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.

## Activating prerequisite Fixlet tasks

Some Fixlets require you to activate tasks before you can use the Fixlets.

Some Fixlets require that you activate a task before you can use the Fixlet. You can identify these tasks by the word 'Task' that appends the Fixlet name. For example, if the Fixlet name is Accounts: Rename Administrator Account, the task that is associated with that Fixlet is called Task - Accounts: Rename Administrator Account.

1. From the Security Configuration domain, go to **All Security Configuration > Sites**.
2. Select the site.
3. Select the task. The word Task appends tasks that are associated to Fixlets that require prerequisite tasks before use.
4. You can do any of the following steps:
  - Click **Take Action**.
  - From the **Description** tab, go to **Actions** and click the appropriate Action link.
5. Click **OK**.

Apply the Fixlet that initially required the task to be activated.

## Modifying Windows check parameters

Modify check parameters by changing the desired value in the check description.

You can modify only parameters of checks in custom sites.

**Note:** Not all checks in custom sites can be parameterized.

In some cases, you can modify the parameters used in determining the compliance of checks. For example, you can set the minimum password length on an endpoint to be 14 characters. You can customize the password-length parameter to your specific policy.

Not all checks can be parameterized. Only copies of checks located in custom sites can be parameterized.

1. Open the check and click the **Description** tab.
2. Scroll down to the **Desired value for this parameter:** field and enter the value.
3. Click **Save**.

## Remediation of Windows configuration settings

Follow these steps to remediate configuration settings.

You can audit, assess, and remediate configuration settings using Tivoli Endpoint Manager Configuration Management. For Fixlet checks that can be automatically remediated, you receive an action displayed in the relevant Fixlet. Not all Fixlets have a remediation action.

1. From the **Security Configuration Domain**, go to **All Security Configuration > Fixlets and Tasks**.
2. Expand the sub-folders to search for the Fixlet you want to enable.
3. In the Fixlet window, click the **Description** tab and scroll down to the Actions box.
4. Click in the Actions box link to remediate the specified policy issue.
5. Set your parameters in the Take Action dialog and click **OK**.

---

## Configuring UNIX checklists

You can configure checklists for the superseded and non-superseded UNIX content.

### Differences between superseded and non-superseded UNIX content

The Configuration Management UNIX content has superseded and non-superseded versions for every site. In the License Overview dashboard, superseded content have 'Superseded' appended to the site name. For example, the site name for the earlier content for the DISA STIG for Red Hat Enterprise Linux 6 is 'SCM Checklist for DISA STIG on RHEL 6 (superseded)'.

The superseded or earlier content uses client settings for parameter values so you could set different values on different endpoints. The non-superseded or later content has the parameter values scoped to the site's subscription so all endpoints subscribed to that site must use the same parameter values.

*Table 2. Comparison between superseded and non-superseded UNIX content*

	<b>Superseded or earlier content</b>	<b>Non-superseded or newer content</b>
Setting parameters	Sets different values on different endpoints	Stores parameters on a per-Fixlet basis



Table 2. Comparison between superseded and non-superseded UNIX content (continued)

	Superseded or earlier content	Non-superseded or newer content
	Requires applicability Fixlets which are in the SCM Reporting site. All endpoints must subscribe to the SCM Reporting site.	Requires an applicability Fixlet in the custom site to work with SCA.
Content	Downloads the related scripts	Each Fixlet contains the related shell script Placed in different directories
Synchronization	Synchronized in the same way as other sites such as Patch Management sites or the BES Support site	Runs from a custom site and uses the Synchronization wizard

## Configuring checklists

Use IBM Endpoint Manager for Configuration Management to configure your checklists by using the -F option in the action scripts or by parametrizing checks from the console or at the system level.

### Select checks via task

Follow these steps to run subsets of the checks on your own schedule.

The default behavior for UNIX Configuration Management deployment is to run the scripts as a single batch. However, you can also run any subset of the checks on your own defined schedule. Each time you do this, the batch that you deploy overwrites any previous batch commands. The `runme.sh` master script provides a '-F' option, which takes a file name as its argument. It has the following form:

```
./runme.sh -F <FILE>
```

This command causes `runme.sh` to perform *only* the set of checks specified in <FILE>. This is a 7-bit ASCII file with UNIX newlines containing a list of the specific checks you want to run, of the form:

```
GEN000020
GEN000480
GEN000560
```

This function allows you to run only the scripts you need when you need them. To enable this function, create a custom action. This action creates the file containing the list of checks and then deploys it to your chosen Endpoint Manager clients. This action is similar to creating a custom parameter file.

1. In the Endpoint Manager console, go to **Tools > Take Custom Action**. The Take Action dialog opens.
2. Click the **Target** tab and select the endpoints on which you want to create checks.
3. Click the **Applicability** tab and click the second button to run this action on computers with a custom relevance clause.
4. In the text box, enter a relevance clause to identify a subset of computers you want to target. For example, to restrict the action to Solaris 10 systems, enter the following expression:

```
name of operating system = "SunOS 5.10" (not exists last
active time of it or (now - last active time of it) > (15
*minute)) of action
```

5. Click the **Action Script** tab to create a script that copies your file onto the target computers. Click the second button and then enter a script. The script creates the target directory with the file containing the checks to run and then moves the file into the appropriate directory. The following sample script, which you can copy and paste, specifies three checks, GEN000020, GEN000480, and GEN000560.

```
// create a script that will create the necessary directory
delete __appendfile
appendfile #!/bin/sh
appendfile mkdir -p ../../scm_preserve/SunOS/5.10
delete createdir.sh
move __appendfile createdir.sh
wait /bin/sh ./createdir.sh
```

```
// create the file containing the checks that you wish to run
delete __appendfile
appendfile GEN000020
appendfile GEN000480
appendfile GEN000560
delete ../../scm_preserve/SunOS/5.10/daily.txt
move __appendfile ../../scm_preserve/SunOS/5.10/daily.txt
```

## Parametizing checks of UNIX content

Use the task that is associated with a particular Fixlet to modify parameters for content from the console.

You can customize security policies and change the values for defined configuration settings to meet specific corporate policies. Use Endpoint Manager to customize the content in the default Fixlet site by special targeting, customizing parameters, and disabling checks. Custom sites offer greater flexibility.

Fixlet checks can be parameterized to suit each individual situation. Because parameters are stored as site settings, you can parameterize the same check differently for each site containing a copy of the check.

1. To open a task, click the **Check Parameterization** link under the **Description** tab.
2. Go to the Actions box and see the two actions that are associated with the task. Use the first action to toggle the evaluation and the second action to modify the parameter that is associated with the check.
3. Click the second link to configure the parameter for the check. The recommended parameter is the default value or the last value that you entered if you previously customized the parameter. Enter a new value or click **OK** to accept the existing value.
4. Select the parameters of your action in the Take Action dialog and click **OK**.

You have now set a parameter for the specified Fixlet, which propagates to the targeted computers to align them with your corporate policy.

## Running checklists

When you run the Deploy and Run Security Checklist, the Master Run script `runme.sh` runs all the Endpoint Manager check scripts. When you run the Deploy and Run Security Checklist task, the Master Run script runs the individual check scripts located on the UNIX system.

You can modify the this behavior using the `-F` option to schedule specific checks. Use `-G` to run global checks. The Master Run script also creates a file named `/var/opt/BESClient/SCM/mytmp/results/master.results` which contains the overall results of running the various OS-specific scripts.

### Understanding the output:

With UNIX content, endpoint scans are accomplished by a series of UNIX Bourne shell scripts that provide greater accessibility to UNIX system administrators.

With most Endpoint Manager content, Fixlets constantly evaluate conditions on each endpoint. The console shows the results when the relevance clause of the Fixlet evaluates to true.

With UNIX content, a task initiates a scan of the endpoints, which can be run on an ad hoc basis each time a scan is required. It can also be run as a recurring policy from the console.

The endpoint scan is accomplished by a series of UNIX Bourne shell scripts. While each script runs, it detects a setting or condition. The script writes the information to an output file that is made available to the corresponding Fixlet check for evaluation. When the log files are written to disk, the Fixlets read each log file and show the results in the console. Although the result is similar, this method of detection provides greater accessibility to UNIX system administrators.

After you run the Deploy and Run Security Checklist task, the scripts are in a directory under `/var/opt/BESClient/SCM`.

The following image is a graphical representation of the directory structure.

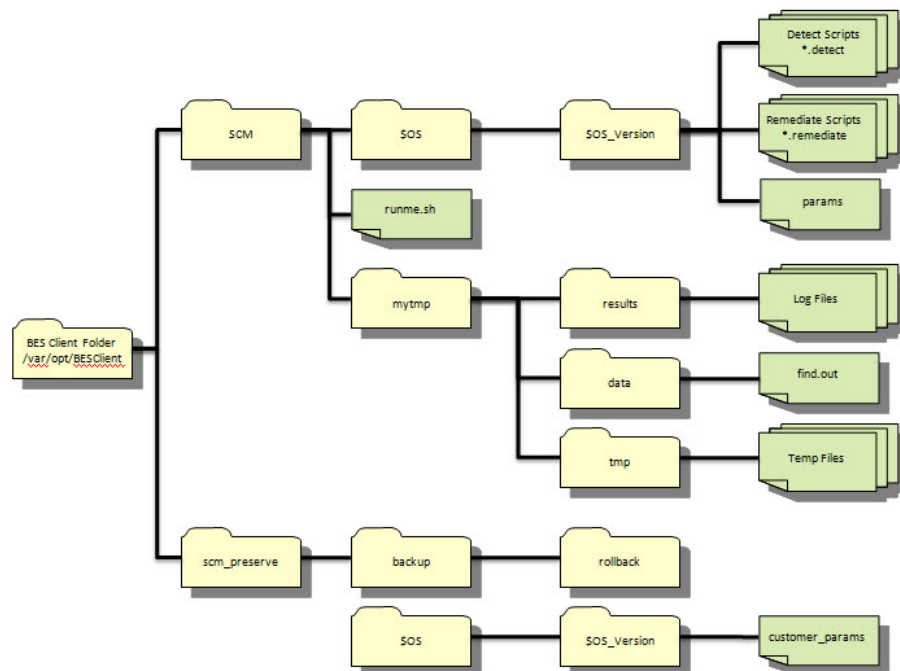


Table 3. Description of directories, subdirectories, and files

Directory/Script	Description
<BES Client Folder> / SCM	This directory is the base directory for the OS-specific check scripts and the master script (runme.sh). The contents of this directory are overwritten each time the 'Deploy and Run Security Checklist' task is run from the Endpoint Manager console.
../SCM/util	A subdirectory of the BES Client Folder / SCM directory, this subdirectory contains utility scripts that are used by the master script and in the individual detection and remediation scripts. The primary utility that is found in this directory is the 'globalfind' script.
../SCM/\$OS/\$OS_version	This directory is specific to the platform on which it runs, as specified by \$OS and \$OS version. For example, the Red Hat Enterprise Linux 4 shows as (../SCM/Linux/4). This directory path contains the specific detection scripts, remediation scripts, and the base parameter file that is used by the scripts. Each check script is named with the corresponding control ID that is used to describe the check. Each corresponding Fixlet also references the check ID.
../SCM/runme.sh	This script is the master script that is called by the Deploy and Run Security Checklist task within the Endpoint Manager console. This script runs the 'globalfind' script and the individual check scripts.
../SCM/mytmp/results	This folder is where the OS-specific detection scripts write their log files. These logs are examined by Fixlets and used to determine if a check is compliant or non-compliant. Each log file corresponds to the check ID for the given check.
../SCM/mytmp/data	This folder contains the <b>find.out</b> file. This file is generated by the <b>globalfind</b> script and contains a directory listing of all local file systems and other information. This file is used by many of the OS-specific scripts and is updated only when the <b>globalfind</b> script is run.
<BES Client Folder>/scm_preserve	This directory is the base directory that is used to retain the rollback scripts, custom checks, parameters, and other information that is not intended to be overwritten each time the 'Deploy and Run Security Checklist' task is run.
../scm_preserve/backup/rollback	Each time a remediation script is run, a corresponding rollback script is created. This script allows the administrator to roll back to the previous setting associated with the specific check.

Table 3. Description of directories, subdirectories, and files (continued)

Directory/Script	Description
<code>../scm_preserve/\$OS/\$OS_version</code>	This directory might contain custom scripts that are produced by the administrator and not provided by Endpoint Manager. Scripts that are in this directory must conform to the input or output specifications are run with out-of-the-box checks when running the 'Deploy and Run Security Checklist' task.
<code>../scm_preserve/\$OS/\$OS_version</code> <code>/customer_params</code>	This file is used to store any custom parameters that are defined by the administrator. Any parameters defined in this file override the default parameters specified in the <code>params</code> file stored in <code>&lt;BES Client Folder&gt;/SCM/\$OS/\$OS_version/params</code> .

Each operating system-specific script writes two files in `/var/opt/BESClient/mytmp/results`. The filenames correspond to the name of the OS-specific script. For example `GEN000020.detect` writes two files `GEN000020.detect.log` and `GEN000020.results`.

The file with the `.log` extension contains the `STDOUT` and `STDERR` of the operating system-specific script. Under normal conditions, this file is empty. When `runme.sh` is run with the `-t` option, this file contains the trace output of the operating system-specific script.

When created, the files with the `.results` extension are read by a Fixlet and the result becomes available through the Endpoint Manager console. The Fixlets examine the `[STATUS]` section to determine relevance.

The following is an example of a results file:

```
[RUN_DATE]
01 Apr 2008
[RUN_DATE_EOF]
[DESCRIPTION]
The UNIX host is configured to require a password for access to single-user
and maintenance modes
[DESCRIPTION_EOF]
[FIXLET_DESCRIPTION]
This UNIX host is not configured to require a password for access to single-user
and maintenance modes
[FIXLET_DESCRIPTION_EOF]
[CHECK_COVERAGE]
DISA-STIG-GEN000020
[CHECK_COVERAGE_EOF]
[STATUS]
PASS
[STATUS_EOF]
[PARAMETERS]
CONFIG_FILE=/etc/default/sulogin;SETTING=PASSREQ;OP='';VALUE=NO
[PARAMETERS_EOF]
[TIMETAKEN]
0
[TIMETAKEN_EOF]
```

[REASON]  
 The /etc/default/sulogin file does not exist, the system will default to requiring a password for single-user and maintenance modes  
 [REASON\_EOF]

Each of the sections found within the log file output are described in the following table:

*Table 4. Descriptions of sections found within the log file output*

Section Name	Description
[RUN_DATE]	Contains the date that the script was run.
[DESCRIPTION] and [FIXLET_DESCRIPTION] Deprecated	No longer used – deprecated file
[CHECK_COVERAGE]	Contains the names of the regulations to which this Fixlet applies. (No longer used – deprecated files)
[STATUS]	Used by the associated Fixlet to determine relevance. It contains one of the following strings: PASS, FAIL, or NA. If this section contains the string FAIL, then the associated Fixlet becomes relevant.
[PARAMETERS]	Contains the parameters associated with the script. Spaces display as a semicolon. On output into this file, spaces are converted to semicolons for display purposes. This is not representative of how the parameters are set.
[TIMETAKEN]	Contains the number of seconds of wall-clock time that the script took to run.
[REASON]	Contains a description of why the script passed or failed. This section provides information needed to construct analysis properties and return specific information to the Endpoint Manager Console.

The **runme.sh** script also creates a file containing the overall results of running the various OS-specific scripts.

This file, named `/var/opt/BESClient/SCM/mytmp/results/master.results`, displays as follows:

```
TOTAL_SCRIPTLETS_RUN:69
TOTAL_SCRIPTLETS_PASS:33
TOTAL_SCRIPTLETS_FAIL:36
TOTAL_SCRIPTLETS_NA:0
TOTAL_SCRIPTLETS_ERR:0
TOTAL_TIME_TAKEN:1367
```

### Modifying global scan options:

You can control the behavior of the global scan through the Configure Filesystems Scan Options task.

UNIX content includes a global scan script that is used to do a full system scan. The results of this scan are used in a number of scripts. This script eliminates the need to run a full system scan multiple times when you are evaluating a set of

checks on a single system. This feature allows Endpoint Manager to be more efficient and causes less impact on the system during a configuration scan.

The global scan script runs by default when you are using the Endpoint Manager Deploy and Run Security Checklist task. It is used by the Master Run script with the use of the `-g` option. The behavior of the global scan script can be controlled through the Configure Filesystems Scan Options task.

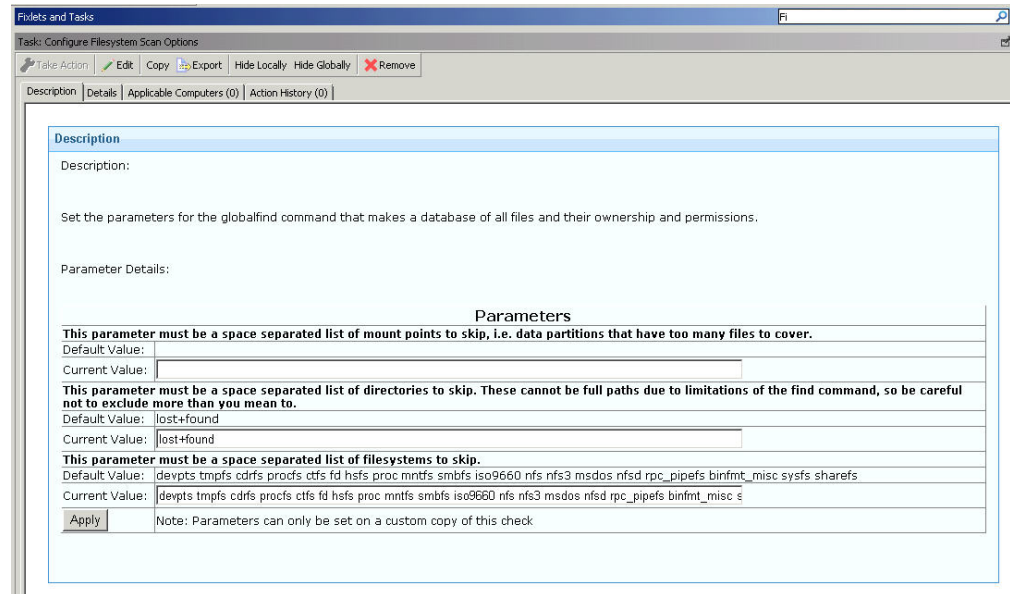


Table 5. Parameters and their descriptions

Parameter	Description
EXCLUDEFS	<p>A list of specific file systems to exclude from scanning. This list must be a space-separated list of all the file system types to exclude from the search.</p> <p>By default, the global find script excludes the following file system types from its search:</p> <ul style="list-style-type: none"> <li>• cdrfs</li> <li>• procs</li> <li>• ctf</li> <li>• fd</li> <li>• hfs</li> <li>• proc</li> <li>• mntfs</li> <li>• smbfs</li> <li>• iso9660</li> <li>• nfs</li> <li>• msdos</li> </ul>

Table 5. Parameters and their descriptions (continued)

Parameter	Description
EXCLUDEMOUNTS	<p>A list of specific mount points to exclude from scanning. This parameter must be defined as a space-separated list of all the file system mounts to exclude from the search. This prevents the shared file system from being scanned from multiple systems.</p> <p>For example, if several systems mount a shared directory on a Storage Area Network named /san, you might want to exclude them with a parameter such as: EXCLUDEMOUNTS="/san"</p> <p>By default, this parameter is not used and is represented as an empty value.</p>
EXCLUDEDIRS	<p>List of directories to exclude from scanning. Any directory names specified in EXCLUDEDIRS are omitted from the directory listing.</p> <p>By default, this parameter excludes the lost+found directory.</p>

**Note:** When you exclude a directory, you also exclude all similarly-named directories. For example, if you specify EXCLUDEDIRS="/foo/", you also exclude /foo/usr/foo and /usr/local/foo.

#### Scheduling specific checks:

You can create a custom action to run a subset of checks on your own schedule.

The default behavior for a UNIX deployment is to run the scripts as a single batch. However, you can also run any subset of the checks on your own defined schedule. Each time that you do, the batch that you deploy overwrites any previous batch commands. The runme.sh master script provides a '-F' option, which takes a file name as its argument. It has the following form:

```
./runme.sh -F <FILE>
```

This command causes runme.sh to run *only* the set of checks that are specified in <FILE>. This file is a 7-bit ASCII file with UNIX newlines that contains a list of the specific checks you want to run, as follows:

```
GEN000020
GEN000480
GEN000560
```

To select a specific script and run schedule, create a custom action. This action creates the file that contains the list of checks and deploys it to Endpoint Manager clients. This action is similar to the creation of a custom parameter file.

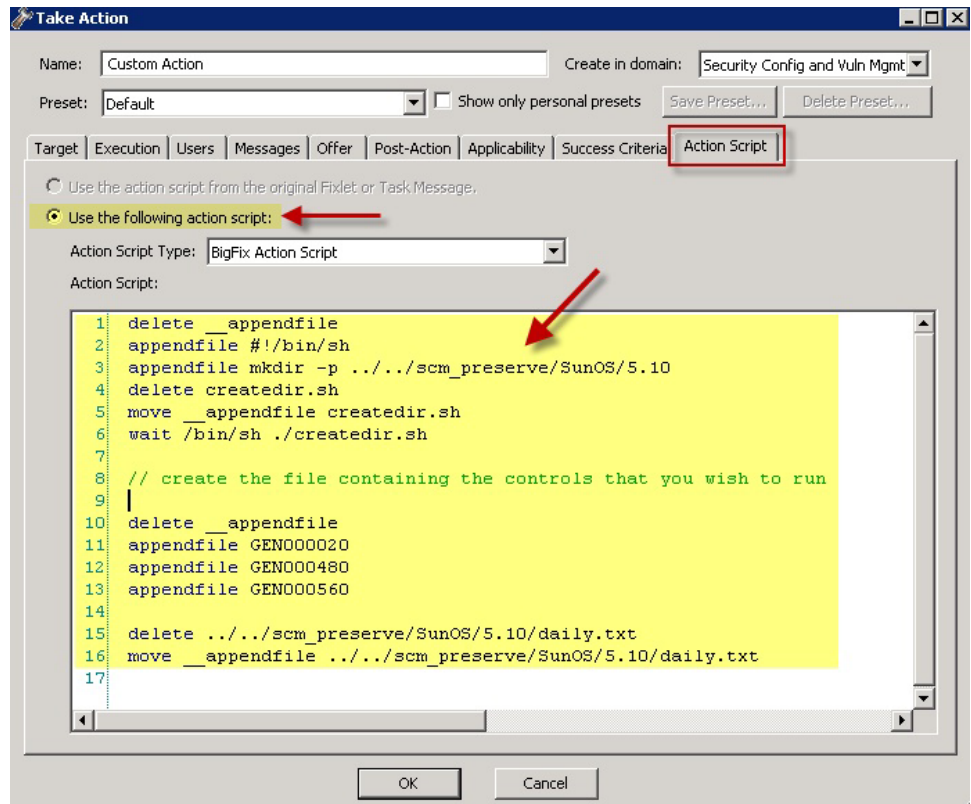
1. In the console, go to **Tools > Take Custom Action** to access the Take Action dialog.
2. To run the action on computers with a custom relevance clause, click the **Applicability** tab and select **...the following relevance clause evaluates to true..**



- In the text box, enter a relevance clause to identify the subset of computers you want to target. For example, to restrict the action to Solaris 10 systems, enter the following expression:

```
name of operating system = "SunOS 5.10" (not exists
last active time of it or (now - last active time of
it) > (15 *minute)) of action
```

- Click the **Action Script** tab to create a script that copies your file onto target computers. Click the second button and enter a script like the one in the following screen capture.

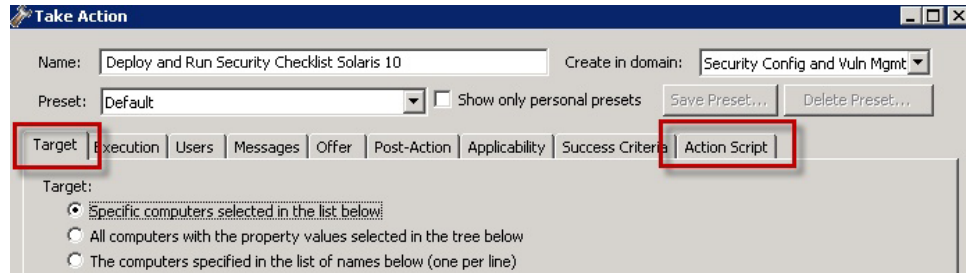


- This script creates the target directory with the file that contains the checks that you want to run and moves the file into the appropriate directory. You can copy and paste the following sample script that specifies three checks, GEN000020, GEN000480, and GEN000560.

```
// create a script that will create the necessary directory
delete __appendfile
appendfile #!/bin/sh
appendfile mkdir -p ../../scm_preserve/SunOS/5.10
delete createdir.sh
move __appendfile createdir.sh
wait /bin/sh ./createdir.sh
```

```
// create the file containing the checks that you wish to run
delete __appendfile
appendfile GEN000020
appendfile GEN000480
appendfile GEN000560
delete ../../scm_preserve/SunOS/5.10/daily.txt
move __appendfile ../../scm_preserve/SunOS/5.10/daily.txt
```

- Run the runme.sh script with the `-F` option. Modify the Deploy and Run Security Checklist task to run the script.



- a. Find and select the Deploy and Run Security Checklist task.
  - b. Click **Take Action**
  - c. In the **Target** tab, then select the endpoints.
7. Click the **Action Script** tab. Modify the Action Script to make runme.sh use the -F option and point to the file that contains the check list. The file in the example is named daily.txt.
  8. You can copy, paste, and modify the following sample script.

```

prefetch DISA.zip sha1:99c90759cc496c506222db55bd864eba4063b955 size:108089
http://software.bigfix.com/download/SCM/SunOS-20080417.zip
delete __appendfile
delete run_SCM.sh
appendfile #!/bin/sh
if {exists folder ((pathname of parent folder of parent folder of folder
(pathname of client folder of current site)) & "/SCM")}
  appendfile rm -rf {{{pathname of parent folder of parent folder of folder
(pathname of client folder of current site)) & "/SCM"}}
endif
appendfile mv __Download/DISA.zip {{{pathname of parent folder of parent
folder of folder (pathname of client folder of current site)}}}
appendfile cd {{{pathname of parent folder of parent folder of folder
(pathname of client folder of current site)}}}
appendfile gzip -dvS .zip DISA.zip
appendfile FILE=`ls -l DISA* | grep -v zip`
appendfile tar xf $FILE
appendfile rm -rf $FILE
appendfile cd {{{pathname of parent folder of parent folder of folder
(pathname of client folder of current site)) & "/SCM"}}
appendfile ./runme.sh -F ../scm_preserve/SunOS/5.10/daily.txt
move __appendfile run_SCM.sh
wait sh ./run_SCM.sh

```

## Analyses

Each check Fixlet in the DISA UNIX content has an associated analysis. Check Fixlets display the compliance state, and analyses display the state of each configuration item.

These analyses are provided to enable the display of Measured Values in IBM Endpoint Manager Security and Compliance Analytics. If you are using only a subset of the available check Fixlets for your implementation, activate only the analyses that are associated with the check Fixlets you are using.

## Using the Create Custom Relevance SCM content wizard

Follow these steps to incorporate custom checks into an existing SCM custom site.

- You must have a custom site that is created through the **Create Custom Checklist** wizard in the SCM Reporting site.

- Check that the custom checks are up to date and that bug fixes are installed with the **Synchronize Custom Checks** wizard.

Use this dashboard to incorporate custom checks into an existing SCM Custom site.

1. In the **Security Configuration Domain**, go to **All Security Configuration > Wizards > Create Custom Relevance SCM Content**. The **Create Custom Relevance SCM checks** wizard opens
2. Enter the following required information:
  - Site
  - Applicability Fixlet
  - Fixlet title
  - SourceID
  - Source
  - Source Release Date
  - Category
  - Severity
3. Enter the Fixlet description. You can use simple HTML format to create your description.
4. Enter the Compliance Relevance.
5. Enter the Analysis Relevance.
  - a. Optional: Select the box if you want to include the desired value.
  - b. Enter the title of the desired value.
  - c. Enter the desired value.
6. Enter the Remediation Action Script.
7. Click **Create Fixlet**.

## Creating custom UNIX Security Configuration Management content

Follow these steps to create custom check for UNIX Security Configuration Management.

- You must have a custom site that is created through the **Create Custom Checklist** wizard in the SCM Reporting site.
- Check that the custom checks are up to date and that bug fixes are installed with the **Synchronize Custom Checks** wizard.

Use this dashboard to incorporate custom checks into an existing SCM Custom site based on an arbitrary bourne shell script.

1. Go to **Wizards > Create Custom Unix SCM Content**. The **Create custom Unix SCM checks** dashboard opens.
2. Enter the following required information:
  - Site
  - Applicability Fixlet
  - Fixlet title
  - SourceID
  - Source
  - Source Release Date
  - Category

- Severity

Create Custom Unix SCM Content

### Create custom Unix SCM checks

---

**This allows you to create a custom Unix SCM check based on an arbitrary bourne shell script.**

The purpose of this tool is to allow you to incorporate custom checks into an existing SCM Custom site. Before running this tool create a custom SCM site using the Create Custom Checklist Wizard in the SCM Reporting site.

**Required Information**

Site	<input type="text" value="AIX Custom List 1"/>
Applicability Fixlet	<input type="text" value="Applicability Fixlet - IBM AIX 5.3 or IBM AIX 6.1"/>
Fixlet title	<input type="text"/>
SourceID	<input type="text"/>
Source	<input type="text"/>
Source Release Date	<input type="text"/>
Category	<input type="text"/>
Severity	<input type="text"/>

3. Enter the Fixlet description. You can use simple HTML format to create your description.
4. Enter the Compliance Relevance.
5. Enter the Analysis Relevance.
  - a. Optional: Select the box if you want to include the desired value.
  - b. Enter the title of the desired value.
  - c. Enter the desired value.
6. Enter the Remediation Action Script.
7. Click **Create Fixlet**.

Once the scan is complete, customers can start an import to the Security Compliance Analysis.

## Importing SCAP content

### Learning about SCAP

#### Information Security Automation Program (ISAP)

The Information Security Automation Program (ISAP) automates and standardizes technical security operations. Primarily focused on government, ISAP offers security checking, remediation, and automation of technical compliance activities to such regulations as FISMA and the FDCC.

ISAP objectives include enabling standards-based communication of vulnerability data, customizing and managing configuration baselines for various IT products, assessing information systems and reporting compliance status, using standard metrics to weight and aggregate potential vulnerability impact, and remediating identified vulnerabilities.

#### SCAP standards

##### Common Vulnerabilities and Exposures (CVE)

The SCAP CVE standard is a dictionary of publicly known information security vulnerabilities that enable data exchanges between security products and provide a baseline index point for evaluating coverage of tools and services.

Tivoli Endpoint Manager has actively supported CVE for several versions of the product and maintains a mature product integration with CVE content. Any security patch or vulnerability that has an associated CVE ID and is available as either a SCAP data stream or available through other Tivoli Endpoint Manager developed processes will display the relevant CVE ID within the Tivoli Endpoint Manager console.

You can find this ID associated with a given security patch or vulnerability by opening the Tivoli Endpoint Manager console and navigating to a patch or vulnerability Fixlet site, double-clicking a relevant Fixlet, selecting the Details tab and viewing the CVE ID. The CVE ID is also accessible from other views and can be used as part of the reporting criteria for detailed and summary reports on individual end-point systems or for a large group of systems reported on in the aggregate.

### **Common Configuration Enumeration (CCE™)**

The SCAP CCE standard provides unique identifiers to system configuration issues to facilitate fast and accurate correlation of configuration data across multiple information sources and tools. For example, CCE Identifiers can associate checks in configuration assessment tools with statements in configuration best practice documents. The Tivoli Endpoint Manager platform includes the ability to assess workstations, laptops, servers, and mobile computing devices against common configuration settings to identify misconfiguration states in a diverse computing environment. Tivoli Endpoint Manager fully supports CCE and displays the CCE ID for each misconfiguration for which there is a CCE ID within the Tivoli Endpoint Manager console. In the case where a misconfiguration is associated with multiple CCE IDs, all IDs are cross-referenced and displayed.

To find the CCE ID associated with a configuration setting, open the Tivoli Endpoint Manager console and navigate to a configuration setting used by a SCAP data stream. Click on a Fixlet that represents a configuration setting and view the Source ID column. The Source ID displays the CCE ID. The CCE ID is also accessible from other views and can be used as part of the reporting criteria for detailed reports and summary reports on individual end-point systems or for a large group of systems reported on in the aggregate.

### **Common Platform Enumeration (CPE™)**

The SCAP CPE standard is a structured naming scheme for information technology systems, platforms, and packages. Based on the generic syntax for Uniform Resource Identifiers (URI), CPE includes a formal name format, a language for describing complex platforms, a method for checking names against a system, and a description format for binding text and tests to a name. Tivoli Endpoint Manager uses CPE to ensure that configuration settings are assessed on the correct system. Regardless of the operating system, the CPE ID can identify a platform and ensure that an assessment is performed.

You can assess and remediate system configurations by targeting systems by platform in addition to other targeting mechanisms. By targeting a particular platform, you can ensure that system scans are done properly

and are weighed against applicable configuration checks. Checks are assessed in real-time based on the platform and policies can be enforced, giving administrators current visibility and control over platforms in a distributed or non-distributed computing environment.

### **Common Vulnerability Scoring System (CVSS)**

The SCAP CVSS standard provides an open framework for communicating the characteristics of IT vulnerabilities. Its quantitative model ensures repeatable, accurate measurement while displaying vulnerability characteristics used to generate the scores. Thus, CVSS is well suited as a standard measurement system for industries, organizations, and agencies that need accurate and consistent vulnerability impact scores.

Tivoli Endpoint Manager assesses and reports on vulnerabilities and quantifies the impact for multiple computing platforms. Tivoli Endpoint Manager fully supports the CVSS standard and displays both the CVSS base score for each applicable vulnerability and the CVSS Base Score Vector used to produce the score.

Tivoli Endpoint Manager administrators can access the CVSS score and the associated vector string from within the Tivoli Endpoint Manager console. For additional details, administrators can navigate to the a vulnerability definition from within the Fixlets. Tivoli Endpoint Manager provides a link for administrators to connect to the CVSS definition located on the NVD website. Tivoli Endpoint Manager enhances the value of CVSS by displaying this common metric for detailed reports on individual end-point systems and for large groups of systems reported on in the aggregate.

### **Extensible Configuration Checklist Description Format (XCCDF)**

The SCAP XCCDF standard is a specification language for writing security checklists, benchmarks, and related documents. An XCCDF document represents a structured collection of security configuration rules for some sets of target systems and is the core element of the SCAP data stream. The specification also defines a data model and format for storing results of checklist compliance testing.

SCAP data streams use the XCCDF format to translate underlying configuration checks that are defined in Tivoli Endpoint Manager Fixlets. When created, these SCAP-based configuration Fixlets allow administrators to assess their computing assets against the SCAP-defined configuration rules in real-time and on a global scale.

When the SCAP configuration rules are imported into Tivoli Endpoint Manager, any system can immediately assess against the defined configuration rules. The results of those configuration checks are relayed to the Tivoli Endpoint Manager console, where administrators can view results and generate detailed reports on an individual system or on large groups of systems.

IBM Endpoint Manager also exports the results of the configuration checks into the defined XCCDF report format so that the organization can store, send, or import those reports into another tool.

### **Open Vulnerability and Assessment Language (OVAL™)**

The SCAP OVAL standard is an international, information security community standard that promotes security content and standardizes the transfer of this information across an entire spectrum of security tools and services. The OVAL language is a collection of XML schema for

representing system information, expressing specific machine states, and reporting the results of an assessment.

Through a repository of vulnerability assessment policies, Tivoli Endpoint Manager assesses managed computers against OVAL vulnerability definitions using real-time data tracking based on the data elements of each definition. These policies are automatically retrieved by the Tivoli Endpoint Manager product within an organization's network. When validated for authenticity, the policies are made available to the Tivoli Endpoint Manager client installed on each managed computer and added to their local library of configuration policies. The agent continuously evaluates the state of the machine against each policy so that any instance of non-compliance can be reported to the Tivoli Endpoint Manager Server for administrator review. If pre-authorized by an administrator, the appropriate corrective action is applied to the computer immediately upon misconfiguration detection, even to remote or mobile users not connected to the organization's network.

## SCAP Checklists

IBM Endpoint Manager has taken the SCAP checklist XML, generated Endpoint Manager content from it, and made it available through subscription. Customers load the external site mastheads for each of the available SCAP checklists in the Endpoint Manager console, and the Endpoint Manager server downloads the content and makes it available to the Endpoint Manager administrator to begin evaluating on systems.

Endpoint Manager currently provides out-of-the-box content for the Federal Desktop Core Configuration (FDCC) SCAP checklists. As new checklists are made available by NIST, IBM Endpoint Manager might include those sites as part of the subscription service.

In addition to the Fixlet sites, Endpoint Manager includes a reporting dashboard that provides visibility into the results of the system evaluations and a reporting dashboard for generating Endpoint Manager content from an SCAP checklist. These dashboards are found in the **SCM Reporting** site.

The following out-of-the-box SCAP checklists are currently available as part of this product:

- *FDCC on Windows XP*
- *FDCC on Windows XP Firewall*
- *FDCC on Windows Vista*
- *FDCC on Windows Vista Firewall*
- *FDCC on Internet Explorer 7*
- *USGCB on Windows 7 Firewall*
- *USGCB on Windows 7 Energy*
- *USGCB on Internet Explorer 8*
- *USGCB on Windows 7*

## Using the Import Windows SCAP Wizard

You must create a custom site that will contain the resulting checklist.

The Import Windows SCAP Content wizard generates IBM Endpoint Manager content from a set of SCAP XML input files into a custom site. The content that is generated includes a Fixlet for each check found in the SCAP checklist.

To find SCAP checklists, see the National Checklist Program Repository. The SCAP Import wizard has been validated for checklists at Tier IV in this repository. The wizard supports checklists designed for the Windows platform.

**Note:** The Import Windows SCAP Content wizard is the latest version of the import wizard but it has not received SCAP certification. Click the link in the wizard to access the earlier, certified version.

1. From the **Security Configuration Domain**, go to **All Security Configuration > Wizards > Import Windows SCAP Content**.

The screenshot shows the 'Import Windows SCAP Content' wizard. At the top, there is a title bar and a header. Below the header, a paragraph explains the wizard's purpose: 'Use this wizard to import a Windows SCAP checklist into a custom site. This will make it possible to assess the compliance of the endpoints in a deployment against technical security standards provided by USGCB, DISA, FDCC and others. Importing UNIX SCAP content is not currently supported.' Below this is a text input field containing a file path: 'r\U\_AIX\_6.1\_v1r2\_stig\_20130426\U\_AIX\_6.1-V1R2\_STIG\_Manual\U\_AIX\_6.1-V1R2\_STIG\_Manual-xccdf.xml', followed by a 'Select' button. A section titled 'Select a profile from the following choices:' contains a dropdown menu with 'I - Mission Critical Classified' selected. Below the dropdown, the 'Name:' is 'I - Mission Critical Classified', 'Source id:' is 'MAC-1\_Classified', and 'Description:' is '<ProfileDescription></ProfileDescription>'. A section titled 'How strictly should issues and errors in the source XML be handled?' has three radio buttons: 'Strict', 'Lenient (ignore minor issues)' (which is selected), and 'Lax (make a best effort to import the content)'. To the right, there are four checkboxes: 'Include OVAL checklists?', 'Skip OVAL validation?', 'Skip XML validation?', and 'Allow unescaped HTML in check descriptions? (may contain script tags - use with caution)'. At the bottom of this section is an 'Import' button. A footer note states: 'This is the most up to date version of the import wizard, but it has not received SCAP certification. Click [here](#) for an older, certified version.'

2. Click **Select** and choose the XCCDF file that will be imported.
3. Click the dropdown menu to select from the following profiles:
  - I - Mission Critical Classified
  - I - Mission Critical Public
  - I - Mission Critical Sensitive
  - II - Mission Support Classified
  - II - Mission Support Public
  - II - Mission Support Sensitive
  - III - Administrative Classified
  - III - Administrative Sensitive
4. Identify how the issues and errors should be handled. Click to select from the following choices:
  - Strict
  - Lenient (ignore minor issues)
  - Lax (make a best effort to import the content)
5. Optional: You can choose to apply the following conditions to the Windows checklist that will be imported.
  - Include OVAL checklists - Select this box to process XCCDF rules that reference an entire OVAL file.



- Skip OVAL validation
  - Skip XML validation
  - Allow unescaped HTML in check description - Use with caution. This option may contain script tags.
6. Click **Import**.
  7. Select the custom site from the menu.
  8. Click **OK**.

## Using the Report Creation wizard

1. Click SCAP Report Creation.
2. Select report parameters.
  - a. Specify a SCAP checklist from the menu.
  - b. To specify an output folder, click the top *Browse* button.
  - c. Optional: To specify an XCCDF schema to validate the results file, click the lower *Browse* button.
3. Target computers.
 

You can target computers by name, property, or computer group. You can also manually enter a list of computers in the designated field. Click the *View Targeted Computers* button to check your selection.

4. Select Additional Report Properties.
 

Use the scroll bar to view a list of available report properties. Check any applicable boxes and view each selection in the corresponding *Included in Report* box on the right.
5. Click *Create Report*.
 

Allocate adequate time for the creation of these reports. The amount of time to generate a report depends on the size of your deployment. For example, creating a report for a deployment of 5000 computers can take 15 minutes on a properly-sized console computer.

## Using OVALDI

Security Configuration Management uses Oval Interpreter (OVALDI), an open-source reference implementation that uses OVAL to scan computer vulnerabilities and generate OVAL full results.

The Oval Interpreter (OVALDI) is a freely available reference implementation that demonstrates the evaluation of OVAL definitions. Using command line interface, OVALDI collects and evaluates system information to generate an OVAL Results file based on a set of Definitions. OVALDI is under BSD license. For more information about OVALDI, see Fixlet 9 in the SCM Reporting site.

---

## 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 Security and Compliance Analytics, which is included in all Configuration Management subscription packages.

For more information about Security and Compliance Analytics, see the Security and Compliance Analysis User Guide.

---

## 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.

---

## Glossary

### **Action Password**

See signing password.

### **Action Scripting Language**

The language used for crafting action scripts. Action can be crafted in different scripting languages, including AppleScript and Unix shells.

### **Ambiguous software**

A software is considered “ambiguous” when it a) has an executable that looks like another executable, or b) when it exists in more than one place in the catalog (Microsoft Word as a standalone product or bundled with Microsoft Office).

### **BigFix Enterprise Suite (BES)**

The previous name for IBM Endpoint Manager.

**Client** Software installed on each networked computer to be managed under the IBM Endpoint Manager. The Client accesses a pool of Fixlet messages, checks the computer it is installed on for vulnerabilities, and sends the Server a message when such a condition occurs. Previously known as the BES Client, it is now known as the IBM Endpoint Manager Client, or simply Client.

### **Console**

A management program that provides an overview of the status of all the computers with the Client installed in the network, identifying which might be vulnerable and offering corrective actions. Previously known as the BES Console, it is now known as the IBM Endpoint Manager Console, or simply Console.

### **CO2 Emissions**

CO2 is one of the primary greenhouse gases and power generation is one of the largest sources of CO2 emissions. The amount of CO2 emitted per kWh generated varies significantly based on how the electricity is

generated. For example, hydroelectric and nuclear power plants do not emit CO<sub>2</sub>, but coal-fired power plants emit significant CO<sub>2</sub>.

**Custom Site**

You can create your own custom content and host it in a custom site. This can only be done by a Master Operator that has been granted the rights to create custom content (use the Admin program to allocate these users).

**Data stream**

A string of information that serves as a source of package data.

**Definitive package**

A string of data that identifies the presence of software and serves as the primary method for identifying the presence of software on a computer.

**DSA** Distributed Server Architecture. Multiple Servers are linked to provide full redundancy in case of failure.

**Fixlet message**

A mechanism for targeting and describing a problematic situation on a computer and providing an automatic fix for it.

**Fixlet servers**

Web servers offering Fixlet site subscriptions. They can be either internal to the enterprise network or external to the network (if direct external web access is allowed).

**Fixlet site**

A trusted source from which the Client obtains Fixlet messages.

**Generator Install folder**

The directory on the installation computer where the Generator places the installation files for the IBM Endpoint Manager system.

**IBM Endpoint Manager**

A preventive maintenance tool for enterprise environments that monitors computers across networks to find and correct vulnerabilities with a few simple mouse-clicks.

**IBM Endpoint Manager database**

A component of the system that stores data about individual computers and Fixlet messages. The IBM Endpoint Manager Server's interactions primarily affect this database, which runs on SQL Server.

**Installation Computer**

A secure computer (separate from the IBM Endpoint Manager Server computer) that hosts and runs the Installation Generator.

**Installation Generator**

An application that creates installers for the core IBM Endpoint Manager system components.

**Management Rights**

Ordinary Console Operators can be limited to a specified group of computers. These limits represent the management rights for that user. Only a Site Administrator or a Master Operator can assign management rights.

**Master Operator**

A Console Operator with administrative rights. A Master Operator can do almost everything a Site Administrator can do, with the exception of creating new operators.

**Masthead**

Files containing the parameters of the IBM Endpoint Manager process, including URLs that point to where trusted Fixlet content is available. The IBM Endpoint Manager Client brings content into the enterprise based on subscribed mastheads.

**Mirror server**

A server required in the IBM Endpoint Manager system if the enterprise does not allow direct web access but instead uses a proxy server that requires password-level authentication.

**Operator**

A person who operates the IBM Endpoint Manager Console. Ordinary operators can deploy Fixlet actions and edit certain computer settings. Master Operators have extra privileges, among them the ability to assign management rights to other operators.

**Package**

A secondary artifact collected from computers, which is an identification string pulled from the Windows registry.

**Package data**

A type of data used in the Software Catalog to help distinguish between two similar executables – includes “regular” and “definitive” packages.

**Power States**

System Power States define the overall power consumption of a system. IBM Endpoint Manager Power Management tracks four main power states – Active, Idle, Standby or Hibernation, and Power Off. For detailed information about power states, see the related Knowledge Base Article from the IBM Endpoint Manager support website.

**Note:** On Mac systems, Power State Tracking is limited to Active and Power Off.

**Price per kWh**

This is the amount you pay for electricity. One kWh is equal to 1,000 watts used for one hour. As a reference point, a standard desktop and monitor runs for approximately six hours on one kWh of electricity. A typical cost for a kWh is \$0.10 in many regions of North America. However, electricity costs vary significantly depending on region and power provider, and different computer models vary power usage.

**Relay**

This is a Client that is running special server software. Relays spare your server and the network by minimizing direct server-client downloads and by compressing upstream data. Relays are automatically discovered by Clients, which dynamically choose the best Relay to connect to. Previously known as the BES Relay, it is now known as the IBM Endpoint Manager Relay, or simply Relay.

**Relevance Language**

The language in which relevance clauses are written.

**Root Server**

Refers to the HTTP or HTTPS services offered by the main Server as an alternative to IIS. The IBM Endpoint Manager Root Server is specially tuned to Fixlet traffic and is more efficient than IIS for this application. Previously known as the BES Root Server, it is now known as the IBM Endpoint Manager Root Server, or simply Root Server.

**SCAP Check**

A specific configuration check within a SCAP checklist. Checks are written in XCCDF and are required to include SCAP enumerations and mappings per the SCAP template.

**SCAP Checklists**

SCAP checklists are configuration checklists written in a machine readable language (XCCDF). SCAP checklists, also referred to as “checklists” or “baselines”, have been submitted to and accepted by the NIST National Checklist Program. They also conform to a SCAP template to ensure compatibility with SCAP products and services. The SCAP template discusses requirements for including SCAP enumerations and mappings within the checklist.

**SCAP Content**

Consists of security checklist data represented in automated XML formats, vulnerability and product name related enumerations, and mappings between the enumerations.

**SCAP Enumerations**

Include a list of all known security related software flaws (CVE), a list of known software configuration issues (CCE), and a list of standard vendor and product names (CPE).

**SCAP Mappings**

Interrelate the enumerations and provide standards-based impact measurements for software flaws and configuration issues. Thus, for any given software flaw (CVE), one can determine the affected standard product names (CPE). For any given standard product name (CPE), one can determine the configuration issues that affect that product (CCE). For any given software flaw (CVE) or configuration issue (CCE), one can determine the standard impact score (CVSS).

**SCAP Reports**

SCAP reports are required to include SCAP enumerations and mappings per the SCAP template.

**SCAP Test Procedures**

SCAP checklists reference “SCAP test procedures” for machine readable information on performing low level checks of machine state (OVAL). SCAP test procedures are used in conjunction with SCAP checklists.

**Server** A collection of interacting applications (web server, CGI-BIN, and database server) that coordinates the relay of information to and from individual computers in the IBM Endpoint Manager system. The server processes may be hosted by a single server computer or segmented to run on separate server computers or replicated on redundant servers. Previously known as the BES Server, it is now known as the IBM Endpoint Manager Server, or simply Server.

**Signing password**

The password (specified when the IBM Endpoint Manager system was installed) used by a Console operator to sign an action for deployment. It is called the *action* password in the Console interface.

**Site Administrator**

The person in charge of installing IBM Endpoint Manager, authorizing and creating new Console operators.

**SQL server**

A full-scale database engine from Microsoft that can be acquired and

installed into the IBM Endpoint Manager system to satisfy more than the basic reporting and data storage needs. A step up from SQLite

**Standard deployment**

A deployment of the IBM Endpoint Manager that applies to workgroups and to enterprises with a single administrative domain. It is intended for a setting in which all Client computers have direct access to a single internal server.

**System install folder**

The directory on the IBM Endpoint Manager Server where the Server software and related files (including Console and Client installers) will be installed.

**VPN** Virtual Private Network. An encrypted channel (or tunnel) that allows companies to extend their local-area networks across the world by using an inexpensive Internet connection.

**Wake-from-Standby**

Windows and other operating systems allow applications to wake a computer from standby at pre-defined times. Using Wake-from-Standby, a computer wakes itself without the need for Wake-on-LAN.

**Wake-on-LAN**

Wake-on-LAN (WoL) is a standard mechanism for waking computers by sending them a specific network packet (known as the magic packet). Wake-on-LAN is difficult in many network environments because of network restrictions regarding broadcasts from other subnets. IBM Endpoint Manager Power Management handles these complexities by sending WoL packets from nearby agents in the same subnet.

**WAN** Wide-area network. Many offices are connected by WAN. The bandwidth of your WAN determines the placement of Relays in your deployment, with thin WANs requiring more relays to aggregate downloads and reduce overhead.

---

## Support

For more information about this product, see the following resources:

- [http://pic.dhe.ibm.com/infocenter/tivihelp/v26r1/topic/com.ibm.tem.doc\\_9.1/welcome/welcome.html](http://pic.dhe.ibm.com/infocenter/tivihelp/v26r1/topic/com.ibm.tem.doc_9.1/welcome/welcome.html)
- IBM Endpoint Manager Support site
- IBM Endpoint Manager wiki
- Knowledge Base
- Forums and Communities

---

## Notices

This information was developed for products and services that are offered in the USA.

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, MD-NC119  
Armonk, NY 10504-1785  
United States of America*

For license inquiries regarding double-byte character set (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.  
19-21, Nihonbashi-Hakozakicho, Chuo-ku  
Tokyo 103-8510, 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 websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this IBM product and use of those websites 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.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

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.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

All IBM prices shown are IBM's suggested retail prices, are current and are subject to change without notice. Dealer prices may vary.

This information is for planning purposes only. The information herein is subject to change before the products described become available.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

#### 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.

Each copy or any portion of these sample programs or any derivative work, must include a copyright notice as follows:

Portions of this code are derived from IBM Corp. Sample Programs.

## Programming interface information

### Trademarks

IBM, the IBM logo, and [ibm.com](http://ibm.com) are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at [www.ibm.com/legal/copytrade.shtml](http://www.ibm.com/legal/copytrade.shtml).

Adobe, Acrobat, PostScript and all Adobe-based trademarks are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, other countries, or both.

IT Infrastructure Library is a registered trademark of the Central Computer and Telecommunications Agency which is now part of the Office of Government Commerce.

Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

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

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

ITIL is a registered trademark, and a registered community trademark of The Minister for the Cabinet Office, and is registered in the U.S. Patent and Trademark Office.

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

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

Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc. in the United States, other countries, or both and is used under license therefrom.

Linear Tape-Open, LTO, the LTO Logo, Ultrium, and the Ultrium logo are trademarks of HP, IBM® Corp. and Quantum in the U.S. and other countries.

## Terms and conditions for product documentation

Permissions for the use of these publications are granted subject to the following terms and conditions.

### Applicability

These terms and conditions are in addition to any terms of use for the IBM website.

## **Personal use**

You may reproduce these publications for your personal, noncommercial use provided that all proprietary notices are preserved. You may not distribute, display or make derivative work of these publications, or any portion thereof, without the express consent of IBM.

## **Commercial use**

You may reproduce, distribute and display these publications solely within your enterprise provided that all proprietary notices are preserved. You may not make derivative works of these publications, or reproduce, distribute or display these publications or any portion thereof outside your enterprise, without the express consent of IBM.

## **Rights**

Except as expressly granted in this permission, no other permissions, licenses or rights are granted, either express or implied, to the publications or any information, data, software or other intellectual property contained therein.

IBM reserves the right to withdraw the permissions granted herein whenever, in its discretion, the use of the publications is detrimental to its interest or, as determined by IBM, the above instructions are not being properly followed.

You may not download, export or re-export this information except in full compliance with all applicable laws and regulations, including all United States export laws and regulations.

IBM MAKES NO GUARANTEE ABOUT THE CONTENT OF THESE PUBLICATIONS. THE PUBLICATIONS ARE PROVIDED "AS-IS" AND WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE.