

TCK User's Guide for Technology Implementors

Table of Contents

Eclipse Foundation	1
Preface	2
Who Should Use This Book	2
Before You Read This Book	2
Typographic Conventions	2
Shell Prompts in Command Examples	3
1 Introduction	4
1.1 Compatibility Testing	4
1.2 About the TCK	6
1.3 Getting Started With the TCK	9
2 Procedure for Certification	10
2.1 Certification Overview	10
2.2 Compatibility Requirements	10
2.3 Test Appeals Process	15
2.4 Specifications for Jakarta Security	17
2.5 Libraries for Jakarta Security	17
3 Installation	18
3.1 Obtaining a Compatible Implementation	18
3.2 Installing the Software	18
4 Setup and Configuration	20
4.1 Configuring Your Environment to Run the TCK Against the Compatible Implementation	20
4.2 Configuring Your Environment to Repackage and Run the TCK Against the Vendor Implementation	22
4.4 Custom Configuration Handlers	22
4.5 Custom Deployment Handlers	23
4.6 Using the JavaTest Harness Software	24
5 Executing Tests	25
5.1 Starting All Tests	25
5.2 Running a Subset of the Tests	26
5.3 Running the TCK Against another CI	27
5.4 Running the TCK Against a Vendor's Implementation	27
5.5 Test Reports	27
6 Debugging Test Problems	29
6.1 Overview	29
6.2 Report Files	30
6.3 Configuration Failures	30

A Frequently Asked Questions.....	31
A.1 Where do I start to debug a test failure?.....	31
A.2 How do I restart a crashed test run?	31
A.3 What would cause tests be added to the exclude list?	31

Eclipse Foundation

Technology Compatibility Kit User's Guide for Jakarta Security

Release 3.0 for Jakarta EE

May 2022

Technology Compatibility Kit User's Guide for Jakarta Security, Release 3.0 for Jakarta EE

Copyright © 2017, 2022 Oracle and/or its affiliates. All rights reserved.

This program and the accompanying materials are made available under the terms of the Eclipse Public License v. 2.0, which is available at <http://www.eclipse.org/legal/epl-2.0>.

SPDX-License-Identifier: EPL-2.0

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

References in this document to Java EE Security refer to the Jakarta Security unless otherwise noted.

Preface

This guide describes how to install, configure, and run the Technology Compatibility Kit (TCK) that is used to test the Jakarta Security (Security 3.0) technology.

The Security TCK is a portable, configurable automated test suite for verifying the compatibility of a vendor's implementation of the Security 3.0 Specification (hereafter referred to as the vendor implementation or VI). The Security TCK uses the JavaTest harness version 5.0 to run the test suite



Note All references to specific Web URLs are given for the sake of your convenience in locating the resources quickly. These references are always subject to changes that are in many cases beyond the control of the authors of this guide.

Jakarta EE is a community sponsored and community run program. Organizations contribute, along side individual contributors who use, evolve and assist others. Commercial support is not available through the Eclipse Foundation resources. Please refer to the Eclipse EE4J project site (<https://projects.eclipse.org/projects/ee4j>). There, you will find additional details as well as a list of all the associated sub-projects (Implementations and APIs), that make up Jakarta EE and define these specifications. If you have questions about this Specification you may send inquiries to es-dev@eclipse.org. If you have questions about this TCK, you may send inquiries to es-dev@eclipse.org.

Who Should Use This Book

This guide is for vendors that implement the Security 3.0 technology to assist them in running the test suite that verifies compatibility of their implementation of the Security 3.0 Specification.

Before You Read This Book

You should be familiar with the Security 3.0, version 3.0 Specification, which can be found at <https://jakarta.ee/specifications/security/3.0/>.

Before running the tests in the Security TCK, you should familiarize yourself with the JavaTest documentation which can be accessed at the [JT Harness web site](#).

Typographic Conventions

The following table describes the typographic conventions that are used in this book.

Convention	Meaning	Example
Boldface	Boldface type indicates graphical user interface elements associated with an action, terms defined in text, or what you type, contrasted with onscreen computer output.	From the File menu, select Open Project . A cache is a copy that is stored locally. <code>machine_name% *su*</code> <code>Password:</code>
Monospace	Monospace type indicates the names of files and directories, commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.	Edit your <code>.login</code> file. Use <code>ls -a</code> to list all files. <code>machine_name% you have mail.</code>
<i>Italic</i>	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.	Read Chapter 6 in the <i>User's Guide</i> . Do <i>not</i> save the file. The command to remove a file is <code>rm filename</code> .

Shell Prompts in Command Examples

The following table shows the default UNIX system prompt and superuser prompt for the C shell, Bourne shell, and Korn shell.

Shell	Prompt
C shell	<code>machine_name%</code>
C shell for superuser	<code>machine_name#</code>
Bourne shell and Korn shell	<code>\$</code>
Bourne shell and Korn shell for superuser	<code>#</code>
Bash shell	<code>shell_name-shell_version\$</code>
Bash shell for superuser	<code>shell_name-shell_version#</code>

1 Introduction

This chapter provides an overview of the principles that apply generally to all Technology Compatibility Kits (TCKs) and describes the Jakarta Security TCK (Security 3.0 TCK). It also includes a high level listing of what is needed to get up and running with the Security TCK.

This chapter includes the following topics:

- [Compatibility Testing](#)
- [About the TCK](#)
- [Getting Started With the TCK](#)

1.1 Compatibility Testing

Compatibility testing differs from traditional product testing in a number of ways. The focus of compatibility testing is to test those features and areas of an implementation that are likely to differ across other implementations, such as those features that:

- Rely on hardware or operating system-specific behavior
- Are difficult to port
- Mask or abstract hardware or operating system behavior

Compatibility test development for a given feature relies on a complete specification and compatible implementation (CI) for that feature. Compatibility testing is not primarily concerned with robustness, performance, nor ease of use.

1.1.1 Why Compatibility Testing is Important

Jakarta platform compatibility is important to different groups involved with Jakarta technologies for different reasons:

- Compatibility testing ensures that the Jakarta platform does not become fragmented as it is ported to different operating systems and hardware environments.
- Compatibility testing benefits developers working in the Jakarta programming language, allowing them to write applications once and then to deploy them across heterogeneous computing environments without porting.
- Compatibility testing allows application users to obtain applications from disparate sources and deploy them with confidence.
- Conformance testing benefits Jakarta platform implementors by ensuring a level playing field for

all Jakarta platform ports.

1.1.2 TCK Compatibility Rules

Compatibility criteria for all technology implementations are embodied in the TCK Compatibility Rules that apply to a specified technology. Each TCK tests for adherence to these Rules as described in [Chapter 2, "Procedure for Certification."](#)

1.1.3 TCK Overview

A TCK is a set of tools and tests used to verify that a vendor's compatible implementation of a Jakarta EE technology conforms to the applicable specification. All tests in the TCK are based on the written specifications for the Jakarta EE platform. A TCK tests compatibility of a vendor's compatible implementation of the technology to the applicable specification of the technology. Compatibility testing is a means of ensuring correctness, completeness, and consistency across all implementations developed by technology licensees.

The set of tests included with each TCK is called the test suite. Most tests in a TCK's test suite are self-checking, but some tests may require tester interaction. Most tests return either a Pass or Fail status. For a given platform to be certified, all of the required tests must pass. The definition of required tests may change from platform to platform.

The definition of required tests will change over time. Before your final certification test pass, be sure to download the latest version of this TCK.

1.1.4 Jakarta EE Specification Process (JESP) Program and Compatibility Testing

The Jakarta EE Specification Process (JESP) program is the formalization of the open process that has been used since 2019 to develop and revise Jakarta EE technology specifications in cooperation with the international Jakarta EE community. The JESP program specifies that the following three major components must be included as deliverables in a final Jakarta EE technology release under the direction of the responsible Expert Group:

- Technology Specification
- Compatible Implementation (CI)
- Technology Compatibility Kit (TCK)

For further information about the JESP program, go to Jakarta EE Specification Process community page <https://jakarta.ee/specifications>.

1.2 About the TCK

The Security TCK 3.0 is designed as a portable, configurable, automated test suite for verifying the compatibility of a vendor's implementation of the Security 3.0 Specification.

1.2.1 TCK Specifications and Requirements

This section lists the applicable requirements and specifications.

- **Specification Requirements:** Software requirements for a Security implementation are described in detail in the Security 3.0 Specification. Links to the Security specification and other product information can be found at <https://jakarta.ee/specifications/security/3.0/>.
- **Security Version:** The Security 3.0 TCK is based on the Security Specification, Version 3.0.
- **Compatible Implementation:** One Security 3.0 Compatible Implementation, Eclipse Soteria 3.0 is available from the Eclipse EE4J project (<https://projects.eclipse.org/projects/ee4j>). See the CI documentation page at <https://projects.eclipse.org/projects/ee4j.soteria> for more information.

See the Security TCK Release Notes for more specific information about Java SE version requirements, supported platforms, restrictions, and so on.

1.2.2 TCK Components

The Security TCK 3.0 includes the following components:

- JavaTest harness version 5.0 and related documentation. See [JT Harness web site](#) for additional information.
- Security TCK signature tests; check that all public APIs are supported and/or defined as specified in the Security Version 3.0 implementation under test.
- If applicable, an exclude list, which provides a list of tests that your implementation is not required to pass.
- API tests for all of the Security API in all related packages:
 - `jakarta.security.enterprise`
 - `jakarta.security.enterprise.authentication.mechanism.http`
 - `jakarta.security.enterprise.credential`
 - `jakarta.security.enterprise.identitystore`

The Security TCK tests run on the following platforms:

- CentOS Linux 7

1.2.3 JavaTest Harness

The JavaTest harness version 5.0 is a set of tools designed to run and manage test suites on different Java platforms. To JavaTest, Jakarta EE can be considered another platform. The JavaTest harness can be described as both a Java application and a set of compatibility testing tools. It can run tests on different kinds of Java platforms and it allows the results to be browsed online within the JavaTest GUI, or offline in the HTML reports that the JavaTest harness generates.

The JavaTest harness includes the applications and tools that are used for test execution and test suite management. It supports the following features:

- Sequencing of tests, allowing them to be loaded and executed automatically
- Automated reporting capability to minimize manual errors
- Failure analysis
- Test result auditing and auditable test specification framework
- Distributed testing environment support

To run tests using the JavaTest harness, you specify which tests in the test suite to run, how to run them, and where to put the results as described in [Chapter 4, "Setup and Configuration."](#)

1.2.4 TCK Compatibility Test Suite

The test suite is the collection of tests used by the JavaTest harness to test a particular technology implementation. In this case, it is the collection of tests used by the Security TCK 3.0 to test a Security 3.0 implementation. The tests are designed to verify that a vendor's runtime implementation of the technology complies with the appropriate specification. The individual tests correspond to assertions of the specification.

The tests that make up the TCK compatibility test suite are precompiled and indexed within the TCK test directory structure. When a test run is started, the JavaTest harness scans through the set of tests that are located under the directories that have been selected. While scanning, the JavaTest harness selects the appropriate tests according to any matches with the filters you are using and queues them up for execution.

1.2.5 Exclude Lists

Each version of a TCK includes an Exclude List contained in a `.jtx` file. This is a list of test file URLs that identify tests which do not have to be run for the specific version of the TCK being used. Whenever tests are run, the JavaTest harness automatically excludes any test on the Exclude List from being executed.

A vendor's compatible implementation is not required to pass or run any test on the Exclude List. The Exclude List file, `<TS_HOME>/bin/ts.jtx`, is included in the Security TCK.



From time to time, updates to the Exclude List are made available. The exclude list is included in the Jakarta TCK ZIP archive. Each time an update is approved and released, the version number will be incremented. You should always make sure you are using an up-to-date copy of the Exclude List before running the Security TCK to verify your implementation.

A test might be in the Exclude List for reasons such as:

- An error in an underlying implementation API has been discovered which does not allow the test to execute properly.
- An error in the specification that was used as the basis of the test has been discovered.
- An error in the test itself has been discovered.
- The test fails due to a bug in the tools (such as the JavaTest harness, for example).

In addition, all tests are run against the compatible implementations. Any tests that fail when run on a compatible Jakarta platform are put on the Exclude List. Any test that is not specification-based, or for which the specification is vague, may be excluded. Any test that is found to be implementation dependent (based on a particular thread scheduling model, based on a particular file system behavior, and so on) may be excluded.



Vendors are not permitted to alter or modify Exclude Lists. Changes to an Exclude List can only be made by using the procedure described in [Section 2.3.1, "TCK Test Appeals Steps."](#)

1.2.6 TCK Configuration

You need to set several variables in your test environment, modify properties in the `<TS_HOME>/bin/ts.jte` file, and then use the JavaTest harness to configure and run the Security tests, as described in [Chapter 4, "Setup and Configuration."](#)



The Jakarta EE Specification Process support multiple compatible implementations. These instructions explain how to get started with the Eclipse Soteria 3.0 CI. If you are using another compatible implementation, refer to material provided by that implementation for specific instructions and procedures.

1.3 Getting Started With the TCK

This section provides an general overview of what needs to be done to install, set up, test, and use the Security TCK. These steps are explained in more detail in subsequent chapters of this guide.

1. Make sure that the following software has been correctly installed on the system hosting the JavaTest harness:
 - A Jakarta EE 10.0 CI (for example Eclipse Soteria 3.0) or, at a minimum, a Web server with a Servlet container
 - A suitable database for your CI. Eclipse Soteria 3.0 is preconfigured to use Apache Derby.
 - Java SE 11
 - Apache Ant 1.10.0+
 - Apache Maven 3.6.3+
 - A CI for Security 3.0. One example is Eclipse Soteria 3.0.
 - Security TCK version 3.0, which includes:
 - The Security 3.0 Vendor Implementation (VI)

See the documentation for each of these software applications for installation instructions. See [Chapter 3, "Installation,"](#) for instructions on installing the Security TCK.

 1. Set up the Security TCK software.

See [Chapter 4, "Setup and Configuration,"](#) for details about the following steps.

 1. Set up your shell environment.
 2. Modify the required properties in the `<TS_HOME>/bin/ts.jte` file.
 3. Configure the JavaTest harness.
 2. Test the Security 3.0 implementation.

Test the Security implementation installation by running the test suite. See [Chapter 5, "Executing Tests."](#)

2 Procedure for Certification

This chapter describes the compatibility testing procedure and compatibility requirements for Jakarta Security. This chapter contains the following sections:

- [Certification Overview](#)
- [Compatibility Requirements](#)
- [Test Appeals Process](#)
- [Specifications for Jakarta Security](#)
- [Libraries for Jakarta Security](#)

2.1 Certification Overview

The certification process for Security 3.0 consists of the following activities:

- Install the appropriate version of the Technology Compatibility Kit (TCK) and execute it in accordance with the instructions in this User's Guide.
- Ensure that you meet the requirements outlined in [Compatibility Requirements](#) below.
- Certify to the Eclipse Foundation that you have finished testing and that you meet all of the compatibility requirements, as required by the Eclipse Foundation TCK License.

2.2 Compatibility Requirements

The compatibility requirements for Security 3.0 consist of meeting the requirements set forth by the rules and associated definitions contained in this section.

2.2.1 Definitions

These definitions are for use only with these compatibility requirements and are not intended for any other purpose.

Table 2-1 Definitions

Term	Definition
API Definition Product	A Product for which the only Java class files contained in the product are those corresponding to the application programming interfaces defined by the Specifications, and which is intended only as a means for formally specifying the application programming interfaces defined by the Specifications.
Computational Resource	<p>A piece of hardware or software that may vary in quantity, existence, or version, which may be required to exist in a minimum quantity and/or at a specific or minimum revision level so as to satisfy the requirements of the Test Suite.</p> <p>Examples of computational resources that may vary in quantity are RAM and file descriptors.</p> <p>Examples of computational resources that may vary in existence (that is, may or may not exist) are graphics cards and device drivers.</p> <p>Examples of computational resources that may vary in version are operating systems and device drivers.</p>
Configuration Descriptor	Any file whose format is well defined by a specification and which contains configuration information for a set of Java classes, archive, or other feature defined in the specification.
Conformance Tests	All tests in the Test Suite for an indicated Technology Under Test, as released and distributed by the Eclipse Foundation, excluding those tests on the published Exclude List for the Technology Under Test.
Container	An implementation of the associated Libraries, as specified in the Specifications, and a version of a Java Platform, Standard Edition Runtime Product, as specified in the Specifications, or a later version of a Java Platform, Standard Edition Runtime Product that also meets these compatibility requirements.
Documented	Made technically accessible and made known to users, typically by means such as marketing materials, product documentation, usage messages, or developer support programs.
Exclude List	The most current list of tests, released and distributed by the Eclipse Foundation, that are not required to be passed to certify conformance. The Jakarta EE Specification Committee may add to the Exclude List for that Test Suite as needed at any time, in which case the updated TCK version supplants any previous Exclude Lists for that Test Suite.

Term	Definition
Libraries	<p>The class libraries, as specified through the Jakarta EE Specification Process (JESP), for the Technology Under Test.</p> <p>The Libraries for Jakarta Security are listed at the end of this chapter.</p>
Location Resource	<p>A location of classes or native libraries that are components of the test tools or tests, such that these classes or libraries may be required to exist in a certain location in order to satisfy the requirements of the test suite.</p> <p>For example, classes may be required to exist in directories named in a CLASSPATH variable, or native libraries may be required to exist in directories named in a PATH variable.</p>
Maintenance Lead	<p>The corresponding Jakarta EE Specification Project is responsible for maintaining the Specification, and the TCK for the Technology. The Specification Project Team will propose revisions and updates to the Jakarta EE Specification Committee which will approve and release new versions of the specification and TCK.</p>
Operating Mode	<p>Any Documented option of a Product that can be changed by a user in order to modify the behavior of the Product.</p> <p>For example, an Operating Mode can be binary (enable/disable optimization), an enumeration (select from a list of protocols), or a range (set the maximum number of active threads).</p> <p>Note that an Operating Mode may be selected by a command line switch, an environment variable, a GUI user interface element, a configuration or control file, etc.</p>
Product	<p>A vendor's product in which the Technology Under Test is implemented or incorporated, and that is subject to compatibility testing.</p>
Product Configuration	<p>A specific setting or instantiation of an Operating Mode.</p> <p>For example, a Product supporting an Operating Mode that permits user selection of an external encryption package may have a Product Configuration that links the Product to that encryption package.</p>
Rebuildable Tests	<p>Tests that must be built using an implementation-specific mechanism. This mechanism must produce specification-defined artifacts. Rebuilding and running these tests against a known compatible implementation verifies that the mechanism generates compatible artifacts.</p>
Resource	<p>A Computational Resource, a Location Resource, or a Security Resource.</p>

Term	Definition
Rules	These definitions and rules in this Compatibility Requirements section of this User's Guide.
Runtime	The Containers specified in the Specifications.
Security Resource	<p>A security privilege or policy necessary for the proper execution of the Test Suite.</p> <p>For example, the user executing the Test Suite will need the privilege to access the files and network resources necessary for use of the Product.</p>
Specifications	<p>The documents produced through the Jakarta EE Specification Process (JESP) that define a particular Version of a Technology.</p> <p>The Specifications for the Technology Under Test are referenced later in this chapter.</p>
Technology	Specifications and one or more compatible implementations produced through the Jakarta EE Specification Process (JESP).
Technology Under Test	Specifications and a compatible implementation for Jakarta Security Version 3.0.
Test Suite	The requirements, tests, and testing tools distributed by the Maintenance Lead as applicable to a given Version of the Technology.
Version	A release of the Technology, as produced through the Jakarta EE Specification Process (JESP).

2.2.2 Rules for Jakarta Security Products

The following rules apply for each version of an operating system, software component, and hardware platform Documented as supporting the Product:

Security1 The Product must be able to satisfy all applicable compatibility requirements, including passing all Conformance Tests, in every Product Configuration and in every combination of Product Configurations, except only as specifically exempted by these Rules.

For example, if a Product provides distinct Operating Modes to optimize performance, then that Product must satisfy all applicable compatibility requirements for a Product in each Product Configuration, and combination of Product Configurations, of those Operating Modes.

Security1.1 If an Operating Mode controls a Resource necessary for the basic execution of the Test Suite, testing may always use a Product Configuration of that Operating Mode providing that Resource, even if other Product Configurations do not provide that Resource. Notwithstanding such exceptions,

each Product must have at least one set of Product Configurations of such Operating Modes that is able to pass all the Conformance Tests.

For example, a Product with an Operating Mode that controls a security policy (i.e., Security Resource) which has one or more Product Configurations that cause Conformance Tests to fail may be tested using a Product Configuration that allows all Conformance Tests to pass.

Security1.2 A Product Configuration of an Operating Mode that causes the Product to report only version, usage, or diagnostic information is exempted from these compatibility rules.

Security1.3 An API Definition Product is exempt from all functional testing requirements defined here, except the signature tests.

Security2 Some Conformance Tests may have properties that may be changed. Properties that can be changed are identified in the configuration interview. Properties that can be changed are identified in the JavaTest Environment (.jte) files in the Test Suite installation. Apart from changing such properties and other allowed modifications described in this User's Guide (if any), no source or binary code for a Conformance Test may be altered in any way without prior written permission. Any such allowed alterations to the Conformance Tests will be provided via the Jakarta EE Specification Project website and apply to all vendor compatible implementations.

Security3 The testing tools supplied as part of the Test Suite or as updated by the Maintenance Lead must be used to certify compliance.

Security4 The Exclude List associated with the Test Suite cannot be modified.

Security5 The Maintenance Lead can define exceptions to these Rules. Such exceptions would be made available as above, and will apply to all vendor implementations.

Security6 All hardware and software component additions, deletions, and modifications to a Documented supporting hardware/software platform, that are not part of the Product but required for the Product to satisfy the compatibility requirements, must be Documented and available to users of the Product.

For example, if a patch to a particular version of a supporting operating system is required for the Product to pass the Conformance Tests, that patch must be Documented and available to users of the Product.

Security7 The Product must contain the full set of public and protected classes and interfaces for all the Libraries. Those classes and interfaces must contain exactly the set of public and protected methods, constructors, and fields defined by the Specifications for those Libraries. No subsetting, supersetting, or modifications of the public and protected API of the Libraries are allowed except only as specifically exempted by these Rules.

Security7.1 If a Product includes Technologies in addition to the Technology Under Test, then it must contain the full set of combined public and protected classes and interfaces. The API of the Product must contain the union of the included Technologies. No further modifications to the APIs of the

included Technologies are allowed.

Security8 Except for tests specifically required by this TCK to be rebuilt (if any), the binary Conformance Tests supplied as part of the Test Suite or as updated by the Maintenance Lead must be used to certify compliance.

Security9 The functional programmatic behavior of any binary class or interface must be that defined by the Specifications.

Security10 The Runtime must report an error when processing a Configuration Descriptor that does not conform to the Specifications.

Security11 The presence of an XML comment in a Configuration Descriptor, when processed by the Runtime, must not cause the functional programmatic behavior of the Runtime to vary from the functional programmatic behavior of the Runtime in the absence of that comment.

Security12 The presence of an XML comment in a Configuration Descriptor, when processed by a Deployment Tool, must not cause the functional programmatic behavior of the Deployment Tool to vary from the functional programmatic behavior of the Deployment Tool in the absence of that comment.

2.3 Test Appeals Process

Jakarta has a well established process for managing challenges to its TCKs. Any implementor may submit a challenge to one or more tests in the Security TCK as it relates to their implementation. Implementor means the entity as a whole in charge of producing the final certified release. **Challenges filed should represent the consensus of that entity.**

2.3.1 Valid Challenges

Any test case (e.g., test class, @Test method), test case configuration (e.g., deployment descriptor), test beans, annotations, and other resources considered part of the TCK may be challenged.

The following scenarios are considered in scope for test challenges:

- Claims that a test assertion conflicts with the specification.
- Claims that a test asserts requirements over and above that of the specification.
- Claims that an assertion of the specification is not sufficiently implementable.
- Claims that a test is not portable or depends on a particular implementation.

2.3.2 Invalid Challenges

The following scenarios are considered out of scope for test challenges and will be immediately closed

if filed:

- Challenging an implementation's claim of passing a test. Certification is an honor system and these issues must be raised directly with the implementation.
- Challenging the usefulness of a specification requirement. The challenge process cannot be used to bypass the specification process and raise in question the need or relevance of a specification requirement.
- Claims the TCK is inadequate or missing assertions required by the specification. See the Improvement section, which is outside the scope of test challenges.
- Challenges that do not represent a consensus of the implementing community will be closed until such time that the community does agree or agreement cannot be made. The test challenge process is not the place for implementations to initiate their own internal discussions.
- Challenges to tests that are already excluded for any reason.
- Challenges that an excluded test should not have been excluded and should be re-added should be opened as a new enhancement request

Test challenges must be made in writing via the Security specification project issue tracker as described in [Section 2.3.3, "TCK Test Appeals Steps."](#)

All tests found to be invalid will be placed on the Exclude List for that version of the Security TCK.

2.3.3 TCK Test Appeals Steps

1. Challenges should be filed via the Jakarta Security specification project's issue tracker using the label **challenge** and include the following information:
 - The relevant specification version and section number(s)
 - The coordinates of the challenged test(s)
 - The exact TCK and exclude list versions
 - The implementation being tested, including name and company
 - The full test name
 - A full description of why the test is invalid and what the correct behavior is believed to be
 - Any supporting material; debug logs, test output, test logs, run scripts, etc.

2. Specification project evaluates the challenge.

Challenges can be resolved by a specification project lead, or a project challenge triage team, after a consensus of the specification project committers is reached or attempts to gain consensus fails. Specification projects may exercise lazy consensus, voting or any practice that follows the principles of Eclipse Foundation Development Process. The expected timeframe for a response is two weeks or less. If consensus cannot be reached by the specification project for a prolonged period of time, the default recommendation is to exclude the tests and address the dispute in a

future revision of the specification.

3. Accepted Challenges.

A consensus that a test produces invalid results will result in the exclusion of that test from certification requirements, and an immediate update and release of an official distribution of the TCK including the new exclude list. The associated **challenge** issue must be closed with an **accepted** label to indicate it has been resolved.

4. Rejected Challenges and Remedy.

When a `challenge` issue is rejected, it must be closed with a label of **invalid** to indicate it has been rejected. There appeal process for challenges rejected on technical terms is outlined in Escalation Appeal. If, however, an implementer feels the TCK challenge process was not followed, an appeal issue should be filed with specification project's TCK issue tracker using the label **challenge-appeal**. A project lead should escalate the issue with the Jakarta EE Specification Committee via email (jakarta.ee-spec@eclipse.org). The committee will evaluate the matter purely in terms of due process. If the appeal is accepted, the original TCK challenge issue will be reopened and a label of **appealed-challenge** added, along with a discussion of the appeal decision, and the **challenge-appeal** issue will be closed. If the appeal is rejected, the **challenge-appeal** issue should be closed with a label of **invalid**.

5. Escalation Appeal.

If there is a concern that a TCK process issue has not been resolved satisfactorily, the [Eclipse Development Process Grievance Handling](#) procedure should be followed to escalate the resolution. Note that this is not a mechanism to attempt to handle implementation specific issues.

2.4 Specifications for Jakarta Security

The Jakarta Security specification is available from the specification project web-site: <https://jakarta.ee/specifications/security/3.0/>.

2.5 Libraries for Jakarta Security

The following is a list of the packages comprising the required class libraries for Security 3.0:

- **jakarta.security.enterprise**
- **jakarta.security.enterprise.authentication.mechanism.http**
- **jakarta.security.enterprise.credential**
- **jakarta.security.enterprise.identitystore**

For the latest list of packages, also see:

<https://jakarta.ee/specifications/security/3.0/>

3 Installation

This chapter explains how to install the Jakarta Security TCK software.

After installing the software according to the instructions in this chapter, proceed to [Chapter 4, "Setup and Configuration,"](#) for instructions on configuring your test environment.

3.1 Obtaining a Compatible Implementation

Each compatible implementation (CI) will provide instructions for obtaining their implementation. Eclipse Soteria 3.0 is a compatible implementation which may be obtained from <https://projects.eclipse.org/projects/ee4j.soteria>

3.2 Installing the Software

Before you can run the Security TCK tests, you must install and set up the following software components:

- A Jakarta EE 10.0 CI (for example Eclipse Soteria 3.0) or, at a minimum, a Web server with a Servlet container
- A suitable database for your CI. Eclipse Soteria 3.0 is preconfigured to use Apache Derby.
- Java SE 11
- Apache Ant 1.10.0+
- Apache Maven 3.6.3+
- A CI for Security 3.0, one example is Eclipse Soteria 3.0
- Security TCK version 3.0, which includes:
- The Security 3.0 Vendor Implementation (VI)

Follow these steps:

1. Install the Java SE 11 software, if it is not already installed.
Download and install the Java SE 11 software from <http://www.oracle.com/technetwork/java/javase/downloads/index.html>. Refer to the installation instructions that accompany the software for additional information.
2. Install the Apache Ant 1.10.0+ software, if it is not already installed.
Download and install Apache Ant 1.10.0+ software from Apache Ant Project. For complete information about Ant, refer to the extensive documentation on the Apache Project site. The Apache Ant Manual is available at <http://ant.apache.org/manual/index.html>. Apache Ant is

protected under the Apache Software, License 2.0, which is available on the Apache Ant Project license page at <http://ant.apache.org/license.html>.

3. Install the Apache Maven 1.10.0+ software, if it is not already installed.
Download and install Apache Maven 1.10.0+ software from Apache Maven Project.
4. Install the Security TCK 3.0 software.
 1. Copy or download the Security TCK software to your local system.
You can obtain the Security TCK software from the Jakarta EE site <https://jakarta.ee/specifications/security/3.0/>.
 2. Use the `unzip` command to extract the bundle in the directory of your choice:
`unzip jakarta-security-tck-3.0.0.zip`
This creates the TCK directory. The TCK is the test suite home, `<TS_HOME>`.
5. Install the Jakarta EE 10.0 CI software (the servlet Web container used for running the Security TCK with the Security 3.0 CI), if it is not already installed.
Download and install the Servlet Web container with the Security 3.0 CI used for running the Security TCK 3.0, represented by the Jakarta EE 10.0 CI. If you intend to use Eclipse Soteria 3.0, you may obtain this software via the downloads tab from the project website: <https://projects.eclipse.org/projects/ee4j.soteria>. You may also use Eclipse GlassFish 7.0 as your CI. You can obtain that from <https://projects.eclipse.org/projects/ee4j.glassfish>
6. Install a Security 3.0 Compatible Implementation.
A Compatible Implementation is used to validate your initial configuration and setup of the Security TCK 3.0 tests, which are explained further in [Chapter 4, "Setup and Configuration."](#)
The Compatible Implementations for Security are listed on the Jakarta EE Specifications web site: <https://jakarta.ee/specifications/security/3.0/>.
7. Install a Web server on which the Security TCK test applications can be published for testing the VI.
8. Install the Security VI to be tested.
Follow the installation instructions for the particular VI under test.

4 Setup and Configuration



The Jakarta EE Specification process provides for any number of compatible implementations. As additional implementations become available, refer to project or product documentation from those vendors for specific TCK setup and operational guidance.

This chapter describes how to set up the Security TCK. Before proceeding with the instructions in this chapter, be sure to install all required software, as described in [Chapter 3, "Installation."](#)

After completing the instructions in this chapter, proceed to [Chapter 5, "Executing Tests,"](#) for instructions on running the Security TCK.

4.1 Configuring Your Environment to Run the TCK Against the Compatible Implementation

After configuring your environment as described in this section, continue with the instructions in [Section 4.6, "Using the JavaTest Harness Software."](#)



In these instructions, variables in angle brackets need to be expanded for each platform. For example, `<TS_HOME>` becomes `$TS_HOME` on Solaris/Linux and `%TS_HOME%` on Windows. In addition, the forward slashes (/) used in all of the examples need to be replaced with backslashes (\) for Windows. Finally, be sure to use the appropriate separator for your operating system when specifying multiple path entries (; on Windows, : on UNIX/Linux).

On Windows, you must escape any backslashes with an extra backslash in path separators used in any of the following properties, or use forward slashes as a path separator instead.

1. Set the following environment variables in your shell environment:
 1. `JAVA_HOME` to the directory in which Java SE 11 is installed
 2. `TS_HOME` to the directory in which the Security TCK 3.0 software is installed
 3. `PATH` to include the following directories: `JAVA_HOME/bin`, `SOTERIA_HOME/bin`, `ANT_HOME/bin` and `M2_HOME/bin`
2. Copy `<TS_HOME>/bin/ts.jte.standalone` as `<TS_HOME>/bin/ts.jte` if TCK is run in standalone mode. Edit your `<TS_HOME>/bin/ts.jte` file and set the following environment variables:
 1. Set `securityapi.classes` to include all necessary JAR files that pertain to your implementation.
 2. Set `web.home` to the location where the securityapi is implemented. For example, If you are using

Eclipse GlassFish 7.0 as your CI, set `web.home=<GLASSFISH_HOME_FOLDER>`.

3. Set `jdbc.lib.class.path` to the location where the JDBC drivers are installed.
4. Set `jdbc.db` to the name of the database under test. Valid values include:

```
derby
mysql
oracle
```

5. Set `sigTestClasspath` to include any additional classes not specified with the `securityapi.classes` property.
6. Set `work.dir` to the default directory in which JavaTest writes temporary files that are created during test execution. The default location is `<TS_HOME>/tmp/JTwork`. This property is required for the TCK Ant targets.
7. Set `report.dir` to the default directory in which JavaTest creates a test report for the most recent test run. The default location is `<TS_HOME>/tmp/JTreport`. This property is a required property for the TCK Ant targets; it must be set. To disable reporting, set the `report.dir` property to `"none"`.

8. If you are testing against the default UnboundID LDAP server that is bundled with the TCK (recommended), make sure the following properties are set:

```
ldap.server=unboundid
ldap.install.server=true
ldap.ldif.file=${ts.home}/bin/ldap.ldif
```

If you are testing against a different LDAP server, then set the following property:

```
ldap.install.server=false
```

For a non-default LDAP, you must manually install the server on the local machine, and configure it to listen on port 11389. You will also need to load the test data by importing the file `<TS_HOME>/bin/ldap.ldif`.

3. Start the database under test.
4. Ensure that no process is using port 11389. If you are not using the default LDAP server, start the LDAP server under test.
5. Initialize the Vendor Implementation (server, database, and LDAP).
Change to the `<TS_HOME>/bin` directory and execute the following command.

```
ant config.vi
ant init.ldap
```

6. Deploy all the server packages for testing. To do so, execute the following command:

```
ant deploy.all
```


4.2 Configuring Your Environment to Repackage and Run the TCK Against the Vendor Implementation

After configuring your environment as described in this section, continue with the instructions in [Section 4.4, "Using the JavaTest Harness Software."](#)



In these instructions, variables in angle brackets need to be expanded for each platform. For example, `<JAVA_HOME>` becomes `$JAVA_HOME` on Solaris/Linux and `%JAVA_HOME%` on Windows. In addition, the forward slashes (/) used in all of the examples need to be replaced with backslashes (\) for Windows. Finally, be sure to use the appropriate separator for your operating system when specifying multiple path entries (; on Windows, : on UNIX/Linux).

On Windows, you must escape any backslashes with an extra backslash in path separators used in any of the following properties, or use forward slashes as a path separator instead.

Before You Begin

Decide against which Security implementation the tests will be run and determine to which Servlet-compliant Web server the Security TCK applications will be published.

Adapt the above instructions for the vendor implementation.

4.4 Custom Configuration Handlers

Configuration handlers are used to configure and unconfigure a Security 3.0 implementation during the certification process. These are similar to deployment handlers but used for configuration. A configuration handler is an Ant build file that contains at least the required targets listed below:

- `config.vi` - to configure the vendor implementation
- `clean.vi` - to unconfigure the vendor implementation

These targets are called from the `<TS_HOME>/bin/build.xml` file and call down into the implementation-specific configuration handlers.

To provide your own configuration handler, create a `config.vi.xml` file with the necessary configuration steps for your implementation and place the file under the `<TS_HOME>/bin/xml/impl/<your_impl>` directory.

For more information, you may wish to view `<TS_HOME>/bin/xml/impl/glassfish/config.vi.xml`, the configuration file for Jakarta EE 10.0 Compatible Implementation, Eclipse GlassFish.

4.5 Custom Deployment Handlers

Deployment handlers are used to deploy and undeploy the WAR files that contain the tests to be run during the certification process. A deployment handler is an Ant build file that contains at least the required targets listed in the table below.

The Security TCK provides these deployment handlers:

- `<TS_HOME>/bin/xml/impl/none/deploy.xml`
- `<TS_HOME>/bin/xml/impl/glassfish/deploy.xml`
- `<TS_HOME>/bin/xml/impl/tomcat/deploy.xml`

The `deploy.xml` files in each of these directories are used to control deployment to a specific container (no deployment, deployment to the Eclipse GlassFish Web container, deployment to the Tomcat Web container) denoted by the name of the directory in which each `deploy.xml` file resides. The primary `build.xml` file in the `<TS_HOME>/bin` directory has a target to invoke any of the required targets (`-deploy`, `-undeploy`, `-deploy.all`, `-undeploy.all`).

4.5.1 To Create a Custom Deployment Handler

To deploy tests to another Security implementation, you must create a custom handler.

1. Create a new directory in the `<TS_HOME>/bin/xml/impl` directory tree. For example, create the `<TS_HOME>/bin/xml/impl/my_deployment_handler` directory. Replace `my_deployment_handler` with the value of the `impl.vi` property that you set in Step 5 of the configuration procedure described in Section 4.2, "Configuring Your Environment to Repackage and Run the TCK Against the Vendor Implementation".
2. Copy the `deploy.xml` file from the `<TS_HOME>/bin/xml/impl/none` directory to the directory that you created.
3. Modify the required targets in the `deploy.xml` file. This is what the `deploy.xml` file for the "none" deployment handler looks like.

```

<project name="No-op Deployment" default="deploy">
  <!-- No-op deployment target -->
  <target name="-deploy">
    <echo message="No deploy target implemented for this deliverable"/>
  </target>
  <target name="-undeploy">
    <echo message="No undeploy target implemented for this deliverable"/>
  </target>
  <target name="-deploy.all">
    <echo message="No deploy target implemented for this deliverable"/>
  </target>
  <target name="-undeploy.all">
    <echo message="No undeploy target implemented for this deliverable"/>
  </target>
</project>

```

Although this example just echoes messages, it does include the four required Ant targets (`-deploy`, `-undeploy`, `-deploy.all`, `-undeploy.all`) that your custom `deploy.xml` file must contain. With this as your starting point, look at the required targets in the `deploy.xml` files in the Tomcat and Eclipse Glassfish directories for guidance as you create the same targets for the Web container in which you will run your implementation of Security.

The following Ant targets can be called from anywhere under the `<TS_HOME>/src` directory:

- `deploy`
- `undeploy`
- `deploy.all`
- `undeploy.all`

The `deploy.all` and `undeploy.all` targets can also be called from the `<TS_HOME>/bin` directory.



The targets in the `deploy.xml` file are never called directly. They are called indirectly by the targets listed above.

4.6 Using the JavaTest Harness Software

It is recommended to run the Security TCK test suite using the JavaTest harness software in JavaTest batch mode, from the command line in your shell environment; if using this method, please proceed directly to [Chapter 5, "Executing Tests."](#)

5 Executing Tests

The Security TCK uses the JavaTest harness to execute a set of tests in the test suite. For detailed instructions that explain how to run and use JavaTest, see the JavaTest User's Guide and Reference in the documentation bundle.

This chapter includes the following topics:

- [Starting JavaTest](#)
- [Running a Subset of the Tests](#)
- [Running the TCK Against your selected CI](#)
- [Running the TCK Against a Vendor's Implementation](#)
- [Test Reports](#)



The instructions in this chapter assume that you have installed and configured your test environment as described in [Chapter 3, "Installation,"](#) and [Chapter 4, "Setup and Configuration,"](#) respectively.

5.1 Starting All Tests

It is recommended to run the Security TCK from the command line in your shell environment



The `mvn` command referenced in the following two procedures and elsewhere in this guide is the Apache Maven build tool, which will need to be downloaded separately. The `build.xml` file in `<TS_HOME>/bin` contains the various Ant targets for the Security TCK test suite. Ant commands can be run via maven using maven-antrun-plugin.

5.1.1 To Start All tests in Command-Line Mode

1. Start the tests using the following command:

```
mvn clean verify
```

Example 5-1 Security TCK Signature Tests

To run the Security TCK signature tests, enter the following commands:

```
cd tck/signaturetest/  
mvn clean verify
```

Example 5-2 Start JavaTests in jakarta-security-tck/security-tck

To run the Javatests:

```
cd tck/security-tck/  
mvn clean verify
```

Example 5-3 Subset of Test Directories

To run a subset of test directories, enter the following commands:

```
cd tck/app-custom-identity-store-handler/  
mvn clean verify
```

5.2 Running a Subset of the Tests

Use the following modes to run a subset of the tests:

- [Section 5.2.1, "To Run a Subset of Tests in Command-Line Mode"](#)

5.2.1 To Run a Subset of Tests in Command-Line Mode

1. Change to the directory containing the tests you want to run.
2. Start the test run by executing the following command:

```
mvn verify
```

The tests in the directory and its subdirectories are run.

5.3 Running the TCK Against another CI

Some test scenarios are designed to ensure that the configuration and deployment of all the prebuilt Security TCK tests against one Compatible Implementation are successful operating with other compatible implementations, and that the TCK is ready for compatibility testing against the Vendor and Compatible Implementations.

1. Verify that you have followed the configuration instructions in [Section 4.1, "Configuring Your Environment to Run the TCK Against the Compatible Implementation."](#)
2. If required, verify that you have completed the steps in [Section 4.3.2, "Deploying the Prebuilt Archives."](#)
3. Run the tests, as described in [Section 5.1, "Starting JavaTest,"](#) and, if desired, [Section 5.2, "Running a Subset of the Tests."](#)

5.4 Running the TCK Against a Vendor's Implementation

This test scenario is one of the compatibility test phases that all Vendors must pass.

1. Verify that you have followed the configuration instructions in [Section 4.2, "Configuring Your Environment to Repackage and Run the TCK Against the Vendor Implementation."](#)
2. If required, verify that you have completed the steps in [Section 4.3.3, "Deploying the Test Applications Against the Vendor Implementation."](#)
3. Run the tests, as described in [Section 5.1, "Starting JavaTest,"](#) and, if desired, [Section 5.2, "Running a Subset of the Tests."](#)

5.5 Test Reports

A set of report files is created for every test run. These report files can be found in the report directory you specify. After a test run is completed, the JavaTest harness writes HTML reports for the test run. You can view these files in the JavaTest ReportBrowser when running in GUI mode, or in the web browser of your choice outside the JavaTest interface.

To see all of the HTML report files, enter the URL of the `report.html` file. This file is the root file that links to all of the other HTML reports.

The JavaTest harness also creates a `summary.txt` file in the report directory that you can open in any text editor. The `summary.txt` file contains a list of all tests that were run, their test results, and their status messages.

5.5.1 Creating Test Reports

Use the following modes to create test reports:

- [Section 5.5.1.1, "To Create a Test Report in Command-Line Mode"](#)

5.5.1.1 To Create a Test Report in Command-Line Mode

1. Specify where you want to create the test report.
 1. To specify the report directory from the command line at runtime, use:

```
ant -Dreport.dir="report_dir"
```

Reports are written for the last test run to the directory you specify.

2. To specify the default report directory, set the `report.dir` property in `<TS_HOME>/bin/ts.jte`.
For example:

```
report.dir="/home/josephine/reports"
```

3. To disable reporting, set the `report.dir` property to `"none"`, either on the command line or in `<TS_HOME>/bin/ts.jte`.
For example:

```
ant -Dreport.dir="none"
```

5.5.2 Viewing an Existing Test Report

Use the following modes to view an existing test report:

- [Section 5.5.2.1, "To View an Existing Report in Command-Line Mode"](#)

5.5.2.2 To View an Existing Report in Command-Line Mode

Use the Web browser of your choice to view the `report.html` file in the report directory you specified from the command line or in `<TS_HOME>/bin/ts.jte`.

6 Debugging Test Problems

There are a number of reasons that tests can fail to execute properly. This chapter provides some approaches for dealing with these failures. Please note that most of these suggestions are only relevant when running the test harness in GUI mode.

This chapter includes the following topics:

- [Overview](#)
- [Report Files](#)
- [Configuration Failures](#)

6.1 Overview

The goal of a test run is for all tests in the test suite that are not filtered out to have passing results. If the root test suite folder contains tests with errors or failing results, you must troubleshoot and correct the cause to satisfactorily complete the test run.

- **Errors:** Tests with errors could not be executed by the JavaTest harness. These errors usually occur because the test environment is not properly configured.
- **Failures:** Tests that fail were executed but had failing results.

The Test Manager GUI provides you with a number of tools for effectively troubleshooting a test run. See the JavaTest User's Guide and JavaTest online help for detailed descriptions of the tools described in this chapter. Ant test execution tasks provide command-line users with immediate test execution feedback to the display. Available JTR report files and log files can also help command-line users troubleshoot test run problems.

For every test run, the JavaTest harness creates a set of report files in the reports directory, which you specified by setting the `report.dir` property in the `<TS_HOME>/bin/ts.jte` file. The report files contain information about the test description, environment, messages, properties used by the test, status of the test, and test result. After a test run is completed, the JavaTest harness writes HTML reports for the test run. You can view these files in the JavaTest ReportBrowser when running in GUI mode, or in the Web browser of your choice outside the JavaTest interface. To see all of the HTML report files, enter the URL of the `report.html` file. This file is the root file that links to all of the other HTML reports.

The JavaTest harness also creates a `summary.txt` file in the report directory that you can open in any text editor. The `summary.txt` file contains a list of all tests that were run, their test results, and their status messages.

The work directory, which you specified by setting the `work.dir` property in the `<TS_HOME>/bin/ts.jte` file, contains several files that were deposited there during test execution: `harness.trace`, `log.txt`,

`lastRun.txt`, and `testsuite`. Most of these files provide information about the harness and environment in which the tests were executed.



You can set `harness.log.traceflag=true` in `<TS_HOME>/bin/ts.jte` to get more debugging information.

6.2 Report Files

Report files are another good source of troubleshooting information. You may view the individual test results of a batch run in the JavaTest Summary window, but there are also a wide range of HTML report files that you can view in the JavaTest ReportBrowser or in the external browser or your choice following a test run. See [Section 5.5, "Test Reports,"](#) for more information.

6.3 Configuration Failures

Configuration failures are easily recognized because many tests fail the same way. When all your tests begin to fail, you may want to stop the run immediately and start viewing individual test output. However, in the case of full-scale launching problems where no tests are actually processed, report files are usually not created (though sometimes a small `harness.trace` file in the report directory is written).

A Frequently Asked Questions

This appendix contains the following questions.

- [Where do I start to debug a test failure?](#)
- [How do I restart a crashed test run?](#)
- [What would cause tests be added to the exclude list?](#)

A.1 Where do I start to debug a test failure?

From the JavaTest GUI, you can view recently run tests using the Test Results Summary, by selecting the red Failed tab or the blue Error tab. See [Chapter 6, "Debugging Test Problems,"](#) for more information.

A.2 How do I restart a crashed test run?

If you need to restart a test run, you can figure out which test crashed the test suite by looking at the `harness.trace` file. The `harness.trace` file is in the report directory that you supplied to the JavaTest GUI or parameter file. Examine this trace file, then change the JavaTest GUI initial files to that location or to a directory location below that file, and restart. This will overwrite only `.jtr` files that you rerun. As long as you do not change the value of the GUI work directory, you can continue testing and then later compile a complete report to include results from all such partial runs.

A.3 What would cause tests be added to the exclude list?

The JavaTest exclude file (`<TS_HOME>/bin/ts.jtx`) contains all tests that are not required to be run. The following is a list of reasons for a test to be included in the Exclude List:

- An error in a Compatible Implementation that does not allow the test to execute properly has been discovered.
- An error in the specification that was used as the basis of the test has been discovered.
- An error in the test has been discovered.

Appendix B is not used for the Security TCK.