

CIS IBM CICS Transaction Server 6.1 Benchmark

v1.0.0 - 06-17-2022

Terms of Use

Please see the below link for our current terms of use:

<https://www.cisecurity.org/cis-securesuite/cis-securesuite-membership-terms-of-use/>

Table of Contents

Terms of Use	1
Table of Contents	2
Overview	4
Intended Audience.....	4
Consensus Guidance	5
Typographical Conventions.....	6
Recommendation Definitions.....	7
Title	7
Assessment Status.....	7
Automated	7
Manual.....	7
Profile	7
Description.....	7
Rationale Statement	7
Impact Statement.....	8
Audit Procedure.....	8
Remediation Procedure.....	8
Default Value.....	8
References	8
CIS Critical Security Controls® (CIS Controls®).....	8
Additional Information.....	8
Profile Definitions	9
Acknowledgements	10
Recommendations	11
1 Authorization and Access Control Management	11
1.1 RACF Options	12
1.1.1 Ensure that RACF changes are accepted immediately (Manual).....	13
1.2 Resource Protection.....	15
1.2.1 Ensure that only authorized users can run transactions (Manual)	16
1.2.2 Ensure that only authorized users can access resources (Manual)	20
1.3 System Settings	25
1.3.1 Ensure that SIT parameter SEC=YES is set in all regions (Manual)	26
1.4 User Privilege	28
1.4.1 Ensure that only authorized users can issue SPI commands (Manual)	29
1.4.2 Ensure that a user requires authorization to start work under a different userid (Manual)	33
2 Logging and Auditing.....	36

2.1 System Settings	37
2.1.1 Ensure that passwords are redacted in line traces (Manual)	38
3 Confidentiality.....	40
3.1 Network Traffic.....	41
3.1.1 Ensure that no unencrypted IP connections use BASICAUTH (Manual)	42
<i>Appendix: Summary Table</i>	<i>44</i>
<i>Appendix: Change History</i>	<i>46</i>

Overview

All CIS Benchmarks focus on technical configuration settings used to maintain and/or increase the security of the addressed technology, and they should be used in **conjunction** with other essential cyber hygiene tasks like:

- Monitoring the base operating system for vulnerabilities and quickly updating with the latest security patches
- Monitoring applications and libraries for vulnerabilities and quickly updating with the latest security patches

In the end, the CIS Benchmarks are designed as a key **component** of a comprehensive cybersecurity program.

This document provides prescriptive guidance for establishing a secure configuration posture for IBM® CICS Transaction Server for z/OS®. Refer to <https://www.ibm.com/legal/copytrade> for listing of United States trademarks owned by IBM and related information. To obtain the latest version of this guide, please visit <http://workbench.cisecurity.org>. If you have questions, comments, or have identified ways to improve this guide, please write us at feedback@cisecurity.org.

Intended Audience

This benchmark is intended for CICS Transaction Server for z/OS system and application administrators, security specialists, and auditors who plan to develop, deploy, assess, or secure solutions that incorporate IBM CICS Transaction Server for z/OS

Consensus Guidance

This CIS Benchmark was created using a consensus review process comprised of a global community of subject matter experts. The process combines real world experience with data-based information to create technology specific guidance to assist users to secure their environments. Consensus participants provide perspective from a diverse set of backgrounds including consulting, software development, audit and compliance, security research, operations, government, and legal.

Each CIS Benchmark undergoes two phases of consensus review. The first phase occurs during initial Benchmark development. During this phase, subject matter experts convene to discuss, create, and test working drafts of the Benchmark. This discussion occurs until consensus has been reached on Benchmark recommendations. The second phase begins after the Benchmark has been published. During this phase, all feedback provided by the Internet community is reviewed by the consensus team for incorporation in the Benchmark. If you are interested in participating in the consensus process, please visit <https://workbench.cisecurity.org/>.

Typographical Conventions

The following typographical conventions are used throughout this guide:

Convention	Meaning
<code>Stylized Monospace font</code>	Used for blocks of code, command, and script examples. Text should be interpreted exactly as presented.
<code>Monospace font</code>	Used for inline code, commands, or examples. Text should be interpreted exactly as presented.
<i><italic font in brackets></i>	Italic texts set in angle brackets denote a variable requiring substitution for a real value.
<i>Italic font</i>	Used to denote the title of a book, article, or other publication.
Note	Additional information or caveats

Recommendation Definitions

The following defines the various components included in a CIS recommendation as applicable. If any of the components are not applicable it will be noted or the component will not be included in the recommendation.

Title

Concise description for the recommendation's intended configuration.

Assessment Status

An assessment status is included for every recommendation. The assessment status indicates whether the given recommendation can be automated or requires manual steps to implement. Both statuses are equally important and are determined and supported as defined below:

Automated

Represents recommendations for which assessment of a technical control can be fully automated and validated to a pass/fail state. Recommendations will include the necessary information to implement automation.

Manual

Represents recommendations for which assessment of a technical control cannot be fully automated and requires all or some manual steps to validate that the configured state is set as expected. The expected state can vary depending on the environment.

Profile

A collection of recommendations for securing a technology or a supporting platform. Most benchmarks include at least a Level 1 and Level 2 Profile. Level 2 extends Level 1 recommendations and is not a standalone profile. The Profile Definitions section in the benchmark provides the definitions as they pertain to the recommendations included for the technology.

Description

Detailed information pertaining to the setting with which the recommendation is concerned. In some cases, the description will include the recommended value.

Rationale Statement

Detailed reasoning for the recommendation to provide the user a clear and concise understanding on the importance of the recommendation.

Impact Statement

Any security, functionality, or operational consequences that can result from following the recommendation.

Audit Procedure

Systematic instructions for determining if the target system complies with the recommendation

Remediation Procedure

Systematic instructions for applying recommendations to the target system to bring it into compliance according to the recommendation.

Default Value

Default value for the given setting in this recommendation, if known. If not known, either not configured or not defined will be applied.

References

Additional documentation relative to the recommendation.

CIS Critical Security Controls® (CIS Controls®)

The mapping between a recommendation and the CIS Controls is organized by CIS Controls version, Safeguard, and Implementation Group (IG). The Benchmark in its entirety addresses the CIS Controls safeguards of (v7) "5.1 - Establish Secure Configurations" and (v8) "4.1 - Establish and Maintain a Secure Configuration Process" so individual recommendations will not be mapped to these safeguards.

Additional Information

Supplementary information that does not correspond to any other field but may be useful to the user.

Profile Definitions

The following configuration profiles are defined by this Benchmark:

- **Level 1**

Items in this profile intend to:

- be practical and prudent;
- provide a clear security benefit; and
- not inhibit the utility of the technology beyond acceptable means.

- **Level 2**

This profile extends the "Level 1 - Server" profile. Items in this profile exhibit one or more of the following characteristics:

- are intended for environments or use cases where security is paramount.
- acts as defense in depth measure.
- may negatively inhibit the utility or performance of the technology.

Acknowledgements

This Benchmark exemplifies the great things a community of users, vendors, and subject matter experts can accomplish through consensus collaboration. The CIS community thanks the entire consensus team with special recognition to the following individuals who contributed greatly to the creation of this guide:

Contributor

Colin Penfold

Editor

Shaun Kelley

Eric Pinnell

Recommendations

1 Authorization and Access Control Management

CICS can be configured to protect resources using RACF profiles in various classes. Authorization is based on user IDs that represent end users or systems. These user IDs are either trusted or previously authenticated.

1.1 RACF Options

1.1.1 Ensure that RACF changes are accepted immediately (Manual)

Profile Applicability:

- Level 1

Description:

RACF sends a type 71 ENF signal to listening CICS regions when a RACF CONNECT or REMOVE command changes a user's resource authorization level. It also sends a type 71 ENF signal when a user ID is revoked. This can occur when a RACF REVOKE command is issued or when a user ID is revoked automatically as a result of too many failed password attempts.

When CICS receives a type 71 ENF event for a user ID, all cached user tokens for the user ID are invalidated. Subsequent requests from that user ID result in a refresh of the user's authorization level.

The CICS SIT option RACFSYNC can be set to the following

- YES - CICS listens for type 71 ENF events.
- NO - CICS does not listen for type 71 ENF events.

RACFSYNC=YES should be specified.

Rationale:

If RACFSYNC=NO a user who has been revoked or has had their privileges change will continue to use their previous level of privilege on any CICS regions that they have previously used. The cache is only deleted when a user ID has not been used on a CICS region for the amount of time specified in the USRDELAY SIT parameter.

Impact:

This option can have a performance impact if you have a very large number of CICS regions. To minimize the impact you normally only configure this option on production regions. In addition RACF commands to add or remove users from groups should not be issued in large numbers at the same time.

Audit:

Issue the z/OSMF Compliance data collection REST API to drive collection of compliance evidence in the SMF 1154 record.

```
https://{host}:{port}/zosmf/compliance/rest/v1/facts
```

1. Wait for the data to be collected; this may take up to a minute in some regions.
2. Customize and run the DFH\$54P sample JCL to create a spreadsheet containing data for all of the CICS TS regions.
3. Open the spreadsheet and review the settings of the RACFSYNC column. They should all be set to YES.

Remediation:

1. Set RACFSYNC=YES
2. Restart CICS






Default Value:

RACFSYNC=YES

References:

1. [SIT option RACFSYNC](<https://www.ibm.com/docs/en/cics-ts/6.1?topic=summary-racfsync>)
2. [Compliance data collection](<https://www.ibm.com/docs/en/cics-ts/6.1?topic=audit-compliance-data-collection.html>)
3. [z/OSMF Compliance data collection REST API](<https://www.ibm.com/docs/en/zos/2.5.0?topic=facility-zos-management-programming-guide>)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.2 Establish an Access Revoking Process Establish and follow a process, preferably automated, for revoking access to enterprise assets, through disabling accounts immediately upon termination, rights revocation, or role change of a user. Disabling accounts, instead of deleting accounts, may be necessary to preserve audit trails.			
v7	16.7 Establish Process for Revoking Access Establish and follow an automated process for revoking system access by disabling accounts immediately upon termination or change of responsibilities of an employee or contractor . Disabling these accounts, instead of deleting accounts, allows preservation of audit trails.			

1.2 Resource Protection

1.2.1 Ensure that only authorized users can run transactions (Manual)

Profile Applicability:

- Level 1

Description:

The authority to run CICS transactions is determined by a pair of RACF classes specified by the XTRAN SIT option. This option can have the following values

- YES - The resource class name is TCICSTRN and the grouping class name is GCICSTRN.
- *name* - The resource class name is Tname and the grouping class name is Gname.
- NO - CICS does not perform any transaction security checks, allowing any user to run any transaction.

XTRAN must be set to YES or a *name*.

The profiles in these classes are used to define which users or groups of users have authority to run transactions.

There are two special categories of CICS supplied transactions which are not defined in the RACF class.

CAT1 transactions

These are part of the CICS system code. In releases prior to CICS TS 6.1 these had to be defined to RACF to prevent users running these transactions. From CICS TS 6.1 this is no longer necessary. Users cannot run these transactions. Any attempt to do so will result in a transaction abend.

CAT3 transactions

These are transactions which are not subject to security, such as the transactions which allow a user to sign on to CICS.

Rationale:

Transaction security ensures that users that attempt to run a transaction are entitled to do so. Transaction security is the most fundamental form of security checking that is required to secure a CICS region and its applications.

Impact:

None.

Audit:

Issue the z/OSMF Compliance data collection REST API to drive collection of compliance evidence in the SMF 1154 record.

```
https://{host}:{port}/zosmf/compliance/rest/v1/facts
```

1. Wait for the data to be collected; this may take up to a minute in some regions.
2. Customize and run the DFH\$54P sample JCL to create a spreadsheet containing data for all of the CICS TS regions.
3. Open the spreadsheet and review the settings of the XTRAN column.
4. They should all be set to the suffix of the transaction class name. The classes are prefixed by G and T.

In the following the default transaction class names will be used.

It is assumed that you have AUDITOR authority, so that you can issue RACF commands and see all of the output.

List the profiles in the CICS classes by issuing the RACF commands

```
RLIST GCICSTRN ALL  
RLIST TCICSTRN
```

Verify that the classes used contain profiles which identify the transactions used either generically in TCICSTRN, or by name in GCICSTRN.

Follow these guidelines:

- If any profiles have a universal access other than NONE, the transactions which they apply to must access any sensitive data or resources.
- The users given access to generic transactions (in TCICSTRN) or groups of transactions (in GCICSTRN) should be defined in groups.
- The groups should match the roles of users allowed access to the transactions.
- The CICS CAT2 transactions are CICS supplied transactions. These should be defined in GCICSTRN with appropriate roles accessing these transactions.
- If a RACF database is used by both production and test systems, these systems must have separate profiles. This can be done either by using separate classes or by using profile prefixing using SECPRFX.

Remediation:

Categorize the transactions on the system according to who should have access to them.

Define profiles for these transactions either generically or in groups in the classes TCICSTRN or GCICSTRN (or the class names used if the default classes aren't used).

Give READ access to the appropriate groups for these profiles.

An example of this is as follows

```
RDEFINE GCICSTRN memname OWNER(admin) AUDIT(ALL(READ)) UACC(NONE)
RALTER GCICSTRN memname ADDMEM(tran1 tran2 tran3)

PERMIT memname CLASS(GICICSTRN) ID(group) ACCESS(READ)
SETROPTS RACLIST(TCICSTRN) REFRESH
```

1. Set XTRAN=YES or *name*.
2. Restart CICS

Default Value:

XTRAN=YES

References:







1. STIG UCF V-224493
2. [transaction security](<https://www.ibm.com/docs/en/cics-ts/6.1?topic=cics-transaction-security>)
3. [Compliance data collection](<https://www.ibm.com/docs/en/cics-ts/6.1?topic=audit-compliance-data-collection.html>)
4. [z/OSMF Compliance data collection REST API](<https://www.ibm.com/docs/en/zos/2.5.0?topic=facility-zos-management-programming-guide>)

Additional Information:

If the profiles contain a “.”, they contain a prefix and a transaction name (prefix.transid). The prefix is used to defined the same transaction name with a different profile on different CICS regions. You will need to look at the SECPRFX SIT parameter to understand which profiles apply to which regions. A common pattern is to use a prefix of PROD for production regions and TEST for test regions.

- Transaction security: <https://www.ibm.com/docs/en/cics-ts/6.1?topic=cics-transaction-security>
- List of CICS transactions: <https://www.ibm.com/docs/en/cics-ts/6.1?topic=descriptions-list-cics-transactions>
- Simplifying Category 1 transaction security: https://www.ibm.com/docs/en/cics-ts/6.1?topic=whats-new#intro_simplify-category1-security
- Compliance data collection: <https://www.ibm.com/docs/en/cics-ts/6.1?topic=audit-compliance-data-collection.html>
- z/OSMF Compliance data collection REST API
<https://www.ibm.com/docs/en/zos/2.5.0?topic=facility-zos-management-programming-guide>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.			

1.2.2 Ensure that only authorized users can access resources (Manual)

Profile Applicability:

- Level 1

Description:

The authority to access CICS resources is determined by a pair of RACF classes for each resource. This is specified in the Xnnn SIT options (where nnn is the type of resource).

The types of resource, and their resource classes are listed below

SIT	Generic classes	Group classes	Description
XPCT	ACICSPCT	BCICSPCT	started transactions and SPI command access to transactions
XDCT	DCICSDCT	ECICSDCT	transient data queues
XFCT	FCICSFCT	HCICSFCT	Files
XJCT	JCICSJCT	KCICSJCT	journals
XPPT	MCICSPPT	NCICSPPT	programs
XPSB	PCICSPSB	QCICSPSB	PSBs
XRES	RCICSRES	WCICSRES	miscellaneous resources
XTST	SCICSTST	UCICSTST	temporary storage queues
XDB2	ZCICSDB2	XCICSDB2	DB2ENTRYs

These options can have the following values

- YES - Use the default resource class name and the default grouping class name.
- *name* - Use user supplied resource class names with the same 1 character suffix name as the default names (e.g. Aname and Bname for started transactions).
- NO - CICS does not perform any resource security checks, allowing any user full access to the resource.

Xnnn should be set to YES or a *name*. The profiles in these classes are then used to define which users or groups of users have authority to access the resource.

In addition CICS transaction definitions can disable resource security checking. The transaction definition option is RESSEC. This option can have the following values:

- YES - Resource security is checked
- NO - Resource security is not checked

The RESSEC transaction option can be overridden by the RESSEC SIT options. This option can have the following values:

- ASIS - The RESSEC value on the transaction definitions is honored
- ALWAYS - Resource security is checked regardless of the transaction definition

Disabling resource security in a transaction is not generally recommended.

Rationale:

Resource security ensures that users can only READ or UPDATE data or use resources for which they should have access.

Impact:

Introducing resource security will require significant planning to identify which RACF groups should have access to each resource. It would also increase the number of security checks so there will be an increase in CPU.

Audit:

Issue the z/OSMF Compliance data collection REST API to drive collection of compliance evidence in the SMF 1154 record.

```
https://{host}:{port}/zosmf/compliance/rest/v1/facts
```

1. Wait for the data to be collected; this may take up to a minute in some regions.
2. Customize and run the DFH\$54P sample JCL to create a spreadsheet containing data for all of the CICS TS regions. Open the spreadsheet and review the settings each of the Xnnn columns for the regions being audited.
3. Xnnn They should all be set to the suffix of the class name such as CICSnnn.

In the following the file classes using the default class names will be used as an example.

It is assumed that you have AUDITOR authority, so that you can issue RACF commands and see all of the output.

List the profiles in the CICS classes by issuing the RACF commands

```
RLIST HCICSFCT ALL  
RLIST FCICSFCT.
```

Verify that the classes used contain profiles which identify the transactions used either generically in FCICSFCT, or by name in HCICSFCT.

1. Use the CICS Explorer to display all the regions being audited.
2. Check the SIT parameter RESSEC. If this is set to ALWAYS the following steps can be skipped
3. Use the CICS Explorer to display the list of transactions in the regions being audited.
4. Verify that all user transactions (ignore CICS transactions) have RESSEC(YES)

Follow these guidelines:

- If any of the Xnnn SIT parms are set to NO (blank in the spreadsheet) then either that resource type must not be used or must not contain any sensitive data.
- If any profile have a universal access other than NONE, that these resources must not contain any sensitive data.
- The users given access to generic transactions (in FCICSFCT) or groups of transactions (in HCICSFCT) should be defined in groups.
- The groups should match the roles of user allowed access to the transactions.
- For each region check the SIT parameter RESSEC. If this is set to ASIS then check the RESSEC value on the transaction definitions in the region. This should be YES.

Remediation:

Categorize the resources on the system according to who should have access to them. In the following the file classes will be used as an example
Define profiles for these resources either generically or in groups in the classes FCICSFCT or HCICSFCT (or the class names used if the default classes aren't used).

- Give READ or UPDATE access to the appropriate groups for these profiles.

An example of this is as follows

```
RDEFINE HCICSFCT memname OWNER(admin) AUDIT(ALL(READ)) UACC(NONE)
RALTER HCICSFCT memname ADDMEM(file1 file2 file3)

PERMIT memname CLASS(HCICSFCT) ID(group) ACCESS(READ)
SETROPTS RACLIST(FCICSFCT) REFRESH
```

- Set XFCT=YES or *name*
- Change any transaction definitions with RESSEC(NO) to RESSEC(YES)
- Restart CICS

Default Value:

Xnnn=YES

References:

1. [Resource security](<https://www.ibm.com/docs/en/cics-ts/6.1?topic=cics-resource-security>)
2. [Compliance data collection](<https://www.ibm.com/docs/en/cics-ts/6.1?topic=audit-compliance-data-collection.html>)
3. [z/OSMF Compliance data collection REST API](<https://www.ibm.com/docs/en/zos/2.5.0?topic=facility-zos-management-programming-guide>)







Additional Information:

If the profiles contain a “.”, they contain a prefix and a name (e.g prefix.name). The prefix is used to defined the same name with a different profile on different CICS regions. You will need to look at the SECPRFX SIT parameter on each region to understand which profiles apply to which regions. A common pattern is to use a prefix of PROD for production regions and TEST for test regions.

The general resource class is used for a series of resources. The profiles have a prefix before the resource name for these resource types (e.g. BUNDLE.name or secprefix.BUNDLE.name).

Some resources may be omitted and have Xnnn=NO if the region doesn't use these resources for customer data. However alternative processes must be in place to ensure that this is the case.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v7	14.6 <u>Protect Information through Access Control Lists</u> Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.			

1.3 System Settings

1.3.1 Ensure that SIT parameter SEC=YES is set in all regions (Manual)

Profile Applicability:

- Level 1

Description:

The CICS SIT option SEC determines if security is enabled in CICS.

It can be set to the following

- YES - Security is enabled
- NO - Security is disabled

Rationale:

This is the most basic security parameter. It must always be set to YES, with the exception of sandbox regions in LPARs which are totally isolated.

Impact:

None.

Audit:

Issue the z/OSMF Compliance data collection REST API to drive collection of compliance evidence in the SMF 1154 record.

```
https://{host}:{port}/zosmf/compliance/rest/v1/facts
```

1. Customize and run the DFH\$54P sample JCL to create a spreadsheet containing data for all of the CICS TS regions.
2. Open the spreadsheet and review the settings of the SEC column. They must all be set to YES.

Remediation:

- Set SEC=YES
- Restart CICS







Default Value:

SEC=YES

References:

1. [SIT option SEC](<https://www.ibm.com/docs/en/cics-ts/6.1?topic=summary-sec>)
2. [Compliance data collection](<https://www.ibm.com/docs/en/cics-ts/6.1?topic=audit-compliance-data-collection.html>)
3. [z/OSMF Compliance data collection REST API](<https://www.ibm.com/docs/en/zos/2.5.0?topic=facility-zos-management-programming-guide>)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v7	14.6 <u>Protect Information through Access Control Lists</u> Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.			

1.4 User Privilege

1.4.1 Ensure that only authorized users can issue SPI commands (Manual)

Profile Applicability:

- Level 1

Description:

SPI commands in CICS can be used to inquire upon or change the state of resources. They are typically used by operators to monitor CICS and system administrators to make changes. Automation tasks will also need access. They are not normally available to general users.

The authority to issue SPI commands is determined by a pair of RACF classes specified in the XCMD SIT option. This option can have the following values

- YES - The resource class name is CCICSCMD and the grouping class name is VCICSCMD.
- *name* - The resource class name is Cname and the grouping class name is Vname.
- NO - CICS does not perform any command security checks, allowing any user to issue any SPI command.

XCMD must be set to YES or *name*. In addition CICS transaction definitions can disable command security checking. The transaction definition option is CMDSEC. This option can have the following values:

- YES - Command security is checked
- NO - Command security is not checked

The CMDSEC transaction option can be overridden by the CMDSEC SIT option. This option can have the following values:

- ASIS - The CMDSEC value on the transaction definitions is honored
- ALWAYS - Commands security is checked regardless of the transaction definition

Disabling command security in a transaction is not generally recommended.

Rationale:

Changing the state of a resource can have an impact on the health of a CICS region, for example disabling a resource would break applications that use that resource. Being able to inquire on resources may give someone information that they could make use of in an attack, for example what files are there.

Impact:

Introducing command security may require planning to identify which RACF groups should have access to each command.

Audit:

Issue the z/OSMF Compliance data collection REST API to drive collection of compliance evidence in the SMF 1154 record.

```
https://{host}:{port}/zosmf/compliance/rest/v1/facts
```

1. Wait for the data to be collected; this may take up to a minute in some regions.
2. Customize and run the DFH\$54P sample JCL to create a spreadsheet containing data for all of the CICS TS regions.
3. Open the spreadsheet and review the settings of the XCMD column. They should all be set to the suffix of the transaction class name. The classes are prefixed by C and V.

In the following the default class names will be used as an example.

It is assumed that you have AUDITOR authority, so that you can issue RACF commands and see all of the output.

List the profiles in the CICS classes by issuing the RACF commands

```
RLIST CCICSCMD ALL  
RLIST VCICSCMD.
```

Verify that the classes used contain profiles which identify the transactions used either generically in CCICSCMD, or by name in VCICSCMD.

Follow these guidelines:

- Profiles should be defined with UACC(NONE).
- The users given access to commands (in CCICSCMD) or groups of commands (in VCICSCMD) should be defined in groups.
- The groups should match the roles of users allowed access to these commands.
- For each region check the SIT parameter CMDSEC. If this is set to ASIS then check the CMDSEC value on the transaction definitions in the region. This should be YES.

The CICS Explorer can be used to display SIT parameters and transaction definitions for all connected regions.

Remediation:

Categorize the transactions on the system according to who should have access to them, and what level of access should be given, for example READ or UPDATE. Define profiles for these commands either generically or in groups in the classes CCICSCMD or VCICSCMD (or the class names used if the default classes aren't used). Give READ access to the appropriate groups for these profiles. An example of this is as follows:

```
RDEFINE VCICSCMD memname OWNER(admin) AUDIT(ALL(READ)) UACC(NONE)
RALTER VCICSCMD memname ADDMEM(cmd1 cmd2 cmd3)

PERMIT memname CLASS(VCICSCMD) ID(group) ACCESS(READ)
SETROPTS RACLIST(CCICSCMD) REFRESH
```

- Change any transactions definitions which specify CMDSEC(NO) to CMDSEC(YES)
- Set XCMD=YES or *name*
- Restart CICS

Default Value:

XCMD=YES







References:

1. [Commands security](<https://www.ibm.com/docs/en/cics-ts/6.1?topic=cics-command-security>)
2. [Compliance data collection](<https://www.ibm.com/docs/en/cics-ts/6.1?topic=audit-compliance-data-collection.html>)
3. [z/OSMF Compliance data collection REST API](<https://www.ibm.com/docs/en/zos/2.5.0?topic=facility-zos-management-programming-guide>)

Additional Information:

If the profiles contain a “.”, they contain a prefix and a transaction name (prefix.command). The prefix is used to defined the same transaction name with a different profile on different CICS regions. You will need to look at the SECPRFX SIT parameter to understand which profiles apply to which regions. A common pattern is to use a prefix of PROD for production regions and TEST for test regions.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v7	14.6 <u>Protect Information through Access Control Lists</u> Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.			

1.4.2 Ensure that a user requires authorization to start work under a different userid (Manual)

Profile Applicability:

- Level 1

Description:

The CICS SIT option XUSER determines if surrogate security is enabled in CICS. It can be set to the following:

- YES - Surrogate security is enabled
- NO - Surrogate security is disabled

Rationale:

Surrogate authority allows one user ID to allow to perform work on behalf of another user ID. This should be strictly limited to those cases where it is necessary to run work under a different user ID for functional reason, for example invoking a common service which can only run under a specific user ID.

Impact:

Introducing surrogate security will require planning to identify which RACF groups should be allowed surrogate access to specific user IDs.

Audit:

Issue the z/OSMF Compliance data collection REST API to drive collection of compliance evidence in the SMF 1154 record.

```
https://{host}:{port}/zosmf/compliance/rest/v1/facts
```

1. Wait for the data to be collected; this may take up to a minute in some regions.
2. Customize and run the DFH\$54P sample JCL to create a spreadsheet containing data for all of the CICS TS regions.
3. Open the spreadsheet and review the settings of the XUSER column. They should all be set to YES.
4. List the FACILITY class by using the RACF command RLIST FACILITY.
5. Look for the CICS profiles with the following suffixes: DFHSTART, DFHINSTL, DFHEXCI, DFHQUERY.

Follow these guidelines:

- All profiles must be defined with UACC(NONE).
- The users given access to profiles should be defined in groups.
- The groups should match the roles of users allowed the specific type of surrogate access.
- The reason for this surrogate access should be documented.

Remediation:

Define surrogate profiles as follows:

```
RDEFINE FACILITY *.DFHSTART OWNER(admin) UACC(NONE)
RDEFINE FACILITY *.DFHINSTL OWNER(admin) UACC(NONE)
RDEFINE FACILITY *.DFHEXCI OWNER(admin) UACC(NONE)
RDEFINE FACILITY *.DFHQUERY OWNER(admin) UACC(NONE)
SETROPTS RACLIST(FACILITY) REFRESH
```

Investigate if surrogate security is needed anywhere if so you will need to defined specific profiles similar to the following

The following is an example of this:

```
RDEFINE FACILITY executionUserid.DFHSTART OWNER(admin) UACC(NONE)
PERMIT executionUserid.DFHSTART CLASS(FACILITY) ID(group) ACCESS(READ)
SETROPTS RACLIST(FACILITY) REFRESH
```

- Set XUSER=YES
- Restart CICS







Default Value:

XUSER=YES

References:

1. [Surrogate security](<https://www.ibm.com/docs/en/cics-ts/6.1?topic=cics-surrogate-security>)
2. [Compliance data collection](<https://www.ibm.com/docs/en/cics-ts/6.1?topic=audit-compliance-data-collection.html>)
3. [z/OSMF Compliance data collection REST API](<https://www.ibm.com/docs/en/zos/2.5.0?topic=facility-zos-management-programming-guide>)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.			

2 Logging and Auditing

Logging of data is important for diagnosis and auditing. CICS has various mechanism for this. This data may contain confidential information, therefore it is important that all logs are secured. Some data may be sufficiently sensitive that it is normally redacted before it is logged.

2.1 System Settings

2.1.1 Ensure that passwords are redacted in line traces (Manual)

Profile Applicability:

- Level 1

Description:

CICS traces out information in a trace data, and in dumps for diagnostic purposes. CICS does not display sensitive information in traced internal function calls, but may display information in certain network trace information. The CONFDATA parameter can be used to redact known sensitive information in network trace information.

It can be set to the following:

- HIDE - Sensitive information is redacted
- SHOW - Sensitive information is visible

In addition CONFDATA is an option on a transaction definitions It can be set to the following:

- YES - Sensitive data is redacted unless CONFDATA=SHOW is specified
- NO - Sensitive information is visible

Rationale:

Setting this value to SHOW can reveal passwords and similar sensitive information to someone investigating diagnostic.

Impact:

None.

Audit:

Issue the z/OSMF Compliance data collection REST API to drive collection of compliance evidence in the SMF 1154 record.

```
https://{host}:{port}/zosmf/compliance/rest/v1/facts
```

1. Wait for the data to be collected; this may take up to a minute in some regions.
2. Customize and run the DFH\$54P sample JCL to create a spreadsheet containing data for all of the CICS TS regions.
3. Open the spreadsheet and review the settings of the CONFDATA column. They should all be set to HIDE.

Remediation:

Setting this value to SHOW can reveal passwords and similar sensitive information to someone investigating diagnostic.

Default Value:





CONFDATA=HIDE

Transaction definitions default to CONFDATA(NO)

References:

1. [Removing sensitive data from CICS trace using CONFDATA](<https://www.ibm.com/docs/en/cics-ts/6.1?topic=trace-removing-sensitive-data-from-cics-using-confdata>)
2. [Compliance data collection](<https://www.ibm.com/docs/en/cics-ts/6.1?topic=audit-compliance-data-collection.html>)
3. [z/OSMF Compliance data collection REST API](<https://www.ibm.com/docs/en/zos/2.5.0?topic=facility-zos-management-programming-guide>)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 <u>Encrypt Sensitive Data in Transit</u> Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).			
v7	16.5 <u>Encrypt Transmittal of Username and Authentication Credentials</u> Ensure that all account usernames and authentication credentials are transmitted across networks using encrypted channels.			

3 Confidentiality

Network traffic should be encrypted to prevent interception. In particular network traffic containing user credentials is particularly sensitive and must always be encrypted.

3.1 Network Traffic

3.1.1 Ensure that no unencrypted IP connections use BASICAUTH (Manual)

Profile Applicability:

- Level 1

Description:

Passwords should not appear in unencrypted connections. Therefore if basic authentication is specified as the authentication mechanism for a connection, the connection must be secure by TLS. This can be done using configuration options in CICS TS or AT-TLS.

TCPIP SERVICE definitions with a PROTOCOL(HTTP) or PROTOCOL(USER), and AUTHENTICATE(BASIC) must be secured either by setting SSL(YES) or by using an AT-TLS policy.

Rationale:

Passwords should not appear in unencrypted connections.

Impact:

None.

Audit:

Issue the z/OSMF Compliance data collection REST API to drive collection of compliance evidence in the SMF 1154 record.

```
https://{host}:{port}/zosmf/compliance/rest/v1/facts
```

1. Wait for the data to be collected; this may take up to a minute in some regions.
2. Customize and run the DFH\$54P sample JCL to create a summary of all of the CICS TS regions.
3. Look at the ABBREV section of the output. Search for all entries with SMF1154_80_S4_NAME.
4. SMF1154_80_S4_NAME is the name of a TCPIP SERVICE definition. To find the region page back to look at the 1154 Common Header which will give the Jobname and LPAR SystemName.

Remediation:

Either

Configure all TCPIP SERVICE definitions with AUTHENTICATE(BASIC) to have SSL(YES)

Or

Create policy definitions in AT-TLS so that all TCPIP SERVICE definitions with AUTHENTICATE(BASIC) use TLS

Restart CICS





Default Value:

N/A

References:

1. [TCPIP SERVICE resources](<https://www.ibm.com/docs/en/cics-ts/6.1?topic=attributes-tcpip-service-resources>)
2. [Compliance data collection](<https://www.ibm.com/docs/en/cics-ts/6.1?topic=audit-compliance-data-collection.html>)
3. [z/OSMF Compliance data collection REST API](<https://www.ibm.com/docs/en/zos/2.5.0?topic=facility-zos-management-programming-guide>)
4. [Application Transparent Transport Layer Security data protection](<https://www.ibm.com/docs/en/zos/2.5.0?topic=applications-application-transparent-transport-layer-security-data-protection>)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 <u>Encrypt Sensitive Data in Transit</u> Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).			
v7	16.5 <u>Encrypt Transmittal of Username and Authentication Credentials</u> Ensure that all account usernames and authentication credentials are transmitted across networks using encrypted channels.			

Appendix: Summary Table

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1	Authorization and Access Control Management		
1.1	RACF Options		
1.1.1	Ensure that RACF changes are accepted immediately (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
1.2	Resource Protection		
1.2.1	Ensure that only authorized users can run transactions (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
1.2.2	Ensure that only authorized users can access resources (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
1.3	System Settings		
1.3.1	Ensure that SIT parameter SEC=YES is set in all regions (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
1.4	User Privilege		
1.4.1	Ensure that only authorized users can issue SPI commands (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
1.4.2	Ensure that a user requires authorization to start work under a different userid (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2	Logging and Auditing		
2.1	System Settings		
2.1.1	Ensure that passwords are redacted in line traces (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
3	Confidentiality		
3.1	Network Traffic		

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
3.1.1	Ensure that no unencrypted IP connections use BASICAUTH (Manual)	<input type="checkbox"/>	<input type="checkbox"/>

Appendix: Change History

Date	Version	Changes for this version
June 17, 2022	1.0.0	Published