Customizing System Security

System security is an important consideration in data processing. Products like Access Control Facility 2 (CA-ACF2), CA-TOP SECRET, or Resource Access Control Facility (RACF) help many installations protect valuable data and preserve system integrity.

The following sections describe the security configuration procedures, as required by several security products.

Note The examples use default class and profile names for illustration only; alternate name selection is possible. Read the description of the SECURITY statement in the IJTCFG*xx* member for details.

- Overview

  Describes the security options available to Cisco IOS for S/390 users.

- Security Information in the Log File

  Describes a parameter used to display information about the user sign-on.

- Configuring Cisco IOS for S/390 Terminal Security

  Describes the parameters that support the security products for the Cisco IOS for S/390 Terminal security or Source security feature.

- CA-ACF2 Options

  Describes the CA-ACF2 security options.

- CA-TOP SECRET Options

  Describes the CA-TOP SECRET security options.

- RACF Options

  Describes the RACF security options.

Overview

In installations using external security systems, the security administrator usually establishes data access restrictions. The security administrator must ensure that Cisco IOS for S/390 does not circumvent these restrictions.

Cisco IOS for S/390 interfaces to the MVS security system, via the SAF router, to perform these functions:

- User ID and password validation

  The user ID and password are validated when sent to Cisco IOS for S/390. Validation occurs at these points:

  — direct sign-ons through VTAM to Cisco IOS for S/390

  — interface calls to the ACTEST debugging service through the VTAM interface by entering:

  ```
  ;VTAMTEST
  ```

  — after connecting to FTP

  — the first time a user tries to use Server Telnet commands that are protected by external security

  — calls to the trace program TCPEEP

- User privileges verification

  FTP uses the validated user security authority to determine if the user is permitted access to specific data sets. Access to data sets is determined by the security information associated with the user, not the security information for the job.

- User authority verification to run ACTEST

  Cisco IOS for S/390 validates a user's authority to execute the ACTEST debugging service through the VTAM interface.

  At CA-ACF2, RACF, and CA-TOP SECRET sites, the user ID associated with the Cisco IOS for S/390 job needs no special privileges assigned, such as NON-CNCL, OPERATIONS, or DASDVOL authority, or PPTNOPAS specified in the Program Properties Table. Also, the Cisco IOS for S/390 user ID does not need access to user data sets for FTP to function properly.

  The user ID associated with a Cisco IOS for S/390 job or started task is not allowed access to any services of Cisco IOS for S/390.

Security Information in the Log File

Security activity can be monitored by activating appropriate options, either at startup or dynamically via ACTEST. Several categories of security related events can be displayed at execution via messages T00IF070 through T00IF088. Many of these events are frequent occurrences and may quickly flood a log file.

The security categories eligible for monitoring can be initially activated via the XSEC keyword of the SECURITY statement in the IJTCFG*xx* member and can later be enabled or disabled via the ACTEST **XSEC** command.

The following events are eligible for monitoring:

- ACSECPC—all security calls
- COMMAND—command authorization calls (for example, ACTEST)

- DATASET—data set authorization calls
- LOGON—System entry attempts
- LOGOFF—System departures
- ACEE—All ACEE-associated activity

Two other global options are also in effect and are capable of totally disabling either ALL security calls, or just command authorization calls. If security functions are disabled at a global level, monitoring cannot be done. See your system administrator about selective security activation.

For example, you may need to monitor sign-ons, signoffs, and filename accesses for a period of time. If the startup IJTCFG*xx* SECURITY statement contains XSEC(LOGON LOGOFF DATASET), then ACTEST can be executed with XSEC(LOGON LOGOFF DATASET OFF) after the monitoring period is over.

Alternatively, no change needs to be made to IJTCFG*xx* at startup, but ACTEST can be run specifying XSEC(LOGON LOGOFF DATASET ON). After the monitoring period, ACTEST can be again executed with the OFF option.

Configuring Cisco IOS for S/390 Terminal Security

This section describes the parameters to support the Cisco IOS for S/390 Terminal security or Source security feature.

Cisco IOS for S/390 Terminal Security Configuration

The following parameters of the XSEC parameter on the SECURITY statement in IJTCFG*xx* member are:

- TERMID causes the Cisco IOS for S/390 security interface to place a terminal ID into the Terminal field of the sign-on parameter list for any user attempting a sign-on to Cisco IOS for S/390. The terminal ID passed during sign-on attempts is either the remote IP address of the originating host for the user or a VTAM APPL LU name.
- NOTERMID causes the Cisco IOS for S/390 security interface to not use the Terminal field in the sign-on parameter list during sign-on attempts.

Cisco IOS for S/390 defaults to NOTERMID.

Note In order to create separate VTAM resources for FTP, define an LUPOOL for FTP usage separate from the one used for Telnet. This allows different security rules to be defined for each set of LU names. See the *Cisco IOS for S/390 Customization Guide* for more information.

Telnet Sign-on Checking

Normally, the user ID of a Telnet user is not validated at sign-on because the service being accessed (typically, TSO) does validation. Sensitive commands, such as ACTEST and SYSSTAT, are validated. The following technique enables sign-on checking for general user access.

Add the CPASSWORD option to all SERVICE statements in the APPCFG*xx* member for Telnet ports (typically, 23,1023). Users are prompted for a user ID and password prior to the display of the “Enter command or Help” message or display of the USSTAB panel.

Cisco IOS for S/390 Terminal Security Settings

Under ACTEST the XSEC command accepts a new parameter called TERMID. The command XSEC TERMID ON|OFF used under ACTEST is used to dynamically alter the passing of Terminal IDs in the sign-on parameter list during sign-on attempts in an active Cisco IOS for S/390 address space.

Terminal Security Activation

When an ACTEST user enters the following command, the Cisco IOS for S/390 security interface places a terminal ID into the Terminal field of the sign-on parameter list for any user attempting a sign-on to Cisco IOS for S/390:

```
XSEC TERMID ON
```

The terminal ID passed during sign-on attempts is either the remote IP address of the originating host for the user or a VTAM APPL LU name. Then the XSEC command prints its global external security block and the following setting displays on Line 2 of the output:

```
TERMINAL SEC ACTIVE: YES
```

This is equivalent to specifying TERMID in the IJTCFG*xx* member.

Terminal Security Deactivation

When an ACTEST user enters the following command, the Cisco IOS for S/390 security interface does not use the Terminal field in the sign-on parameter list during sign-on attempts:

```
XSEC TERMID OFF
```

The XSEC command prints its global external security block and the following setting displays on Line 2 of the output:

```
TERMINAL SEC ACTIVE: NO
```

This is equivalent to specifying NOTERMID in the IJTCFG*xx* member.

CA-ACF2 Options

This section describes the CA-ACF2 security options. Refer to the appropriate CA-ACF2 procedures in the following sections, according to the version you are running.

- Customizing CA-ACF2 Version 5.2 or Earlier
- Customizing CA-ACF2 Version 6 or Later

Types of CA-ACF2 Security

Cisco IOS for S/390 uses these types of security with CA-ACF2:

- Sign-on security

  All user ID and password combinations are validated by CA-ACF2

- Data set security

  All FTP file transfers are validated by CA-ACF2

- Command security

  Restricts service to SYSSTAT, ACTEST, and TCPEEP

- Source level security for FTP IP addresses, VTAM LUs, and Telnet services

The command security interface restricts access to application segment services. By default, the ACTEST, SYSTAT and TCPEEP are restricted under command security.

To maintain system security, only system programmers and operations personnel should have access to these services. Inexperienced users can cause serious damage to system performance and reliability through the ACTEST, SYSTAT, and TCPEEP services.

Because CA-ACF2 denies all access until permitted, additional steps are required to bring up Cisco IOS for S/390 at a site where CA-ACF2 is installed.

Customizing CA-ACF2 Version 5.2 or Earlier

1 Create a logon ID (LID) record to associate with the Cisco IOS for S/390 address space.

Follow the installation procedures of your site to create an LID record; make sure the following parameters are set in the Privileges Section - Group 2:

- MUSASS
- NONO-SAF
- NO-INH
- BDT

Read the *CA-ACF2 Administrator's Guide* for help on creating the LID record.

Place the LID in the USER field of the start-up JCL job card.

You may have to set the NON-CNCL attribute in the LID record to be associated with the Cisco IOS for S/390 job. If your site runs CA-ACF2 version 5.2 with APAR TW95626, it is not necessary to place NON-CNCL in the Cisco IOS for S/390 LID record. If your site runs CA-ACF2 version 5.2 without APAR TW95626 you need to place NON-CNCL on the LID record.

Note To prevent unauthorized users from attempting to use the production user ID for Cisco IOS for S/390, the TCP base product rejects all logon attempts to Cisco IOS for S/390 from programs like FTP and ACTEST that use this ID.

2 Update the GSO records to allow SAF Processing.

Use the following commands to check the CA-ACF2 GSO record to see if SAF processing is allowed:

- ACF
- SET CONTROL(GSO)
- LIST OPTS
- If the output does not indicate that SAF is allowed, enter these commands:
- CHANGE OPTS SAF REP
- END

3 Update the SAFMAPS records to let Cisco IOS for S/390 use SAF.

The Cisco IOS for S/390 command class is AC#CMD. Cisco IOS for S/390 uses the SAF interface for general resource class checking. Use the following commands to check the SAFMAPS GSO records in the CA-ACF2 GSO record to see if SAF processing is allowed:

- ACF
- SET CONTROL(GSO)
- LIST SAFMAPS
- If the output does not indicate that SAF processing is allowed (SAF/-), enter these commands:
- INSERT MAPS(SAF/AC#CMD)
- END

4 Follow these guidelines to set up the SAFPROT records to intercept Cisco IOS for S/390 calls to SAF:

- Enter the SAFPROT records exactly as shown.
- Do not change the SUBSYS(SNSTCP) in the first SAFPROT record.
- SNSTCP in the SUBSYS parameter relates to parameters on the SAF security calls, not the CA-ACF2 LID chosen by the site.

To make sure that SAF calls from Cisco IOS for S/390 are processed by CA-ACF2, use the following commands to update the SAFPROT records in the GSO record:

```
ACF
SET CONTROL( GSO )
INSERT SAFPROT.AC#CMD     CLASS( - ) REP   CNTLPTS( ACSECPC )      SUBSYS( SNSTCP )
INSERT SAFPROT.ACCPEEP    CLASS( - ) REP   CNTLPTS( ACCPEEP )      SUBSYS(-)
INSERT SAFPROT.FTP        CLASS( - ) REP   CNTLPTS( FTP )          SUBSYS( - )
INSERT SAFPROT.FTP2       CLASS( - ) REP   CNTLPTS( FTP2 )         SUBSYS( - )
INSERT SAFPROT.ACCFTP2    CLASS( - ) REP   CNTLPTS( ACCFTP2 )      SUBSYS( -)
INSERT SAFPROT.FTP3       CLASS( - ) REP   CNTLPTS( FTP3 )         SUBSYS( - )
END
```

5 Set proper authority over mail data sets for the Cisco IOS for S/390 LID.

The LID associated with the Cisco IOS for S/390 job must have allocation access authority to the HLQ(s) on the PATH parameter of the SMTP statement in member APPCFG*xx*. When you set the rules for the LID, set the ALLOC parameter to ALLOC(A).

The PATH parameter of the SMTP statement specifies the HLQ(s) for mail DASD data set names. SMTP requires that a data set naming convention be established for outgoing mail data sets. The HLQ(s) for mail should be unique. For example, if the HLQ for Cisco IOS for S/390 data sets is Cisco IOS for S/390, you could use a two-level qualifier and define the HLQ for mail as PATH(TCPACCES.EMAIL). If you specify PATH(TCPACCES) on the SMTP statement, the client mail handler will attempt to send all the Cisco IOS for S/390 system data sets as mail data sets.

If the PATH parameter on the SMTP statement contains PATH(TCPACCES.EMAIL) and the Cisco IOS for S/390 LID is TCPACCES, use the following CA-ACF2 commands to permit the TCPACCES and SYS1 LIDs alter authority:

```
ACF
SET RULE
COMPILE
$KEY( TCPACCES )
$OWNER(‘Production TCPACCES’)
- UID( TCPACCES ) READ( A ) WRITE( A ) ALLOC( A ) EXEC( A )
- UID( SYS1- )  READ( A ) WRITE( A ) ALLOC( A ) EXEC( A )
- UID( - ) READ( A )
EMAIL.- UID( TCPACCES ) READ( A ) WRITE( A ) ALLOC( A ) EXEC( A )
EMAIL.- UID( SYS1- ) READ( A ) WRITE( A ) ALLOC( A ) EXECA( A )
EMAIL.- UID( - ) READ( A )
END
STORE
END
```

Adjust the UID to the installation’s naming conventions.

To avoid data set enqueue conflicts, choose a unique PATH name for every Cisco IOS for S/390 address space running at a site. PATH names of TCPACCES.EMAIL and TCPACCES.EMAIL2 are valid for separate Cisco IOS for S/390 address spaces because the second level in the name is unique. The names TCPACCES.EMAIL and TCPACCES.EMAIL.A are not recommended as the second PATH name is a subset of the first.

6 User validation is required for access to Cisco IOS for S/390 to internal debugging services ACTEST and SYSSTAT; validation occurs by checking resource name SYSTRAN in the SAF Resource Rule Entry.

Users are prompted for a user ID and password when they invoke ACTEST or SYSSTAT. The user ID and password are validated by the CA-ACF2 security system. If the user ID and password are valid according to the LID record, the security system also checks to see if the user is authorized to access the resource name SYSTRAN in the SAF Resource Rule Entry. If the user is not authorized for a minimum of read access to the SYSTRAN resource name in the SAF Resource Rule Entry, then access to ACTEST or SYSSTAT is denied.

In this example, user ID USER01 will be the only user ID that will have access to the Cisco IOS for S/390 debugging services. You should replace the user ID USER01 with the user ID of your local Cisco IOS for S/390 systems programmer.

Use these commands to define the SAF Resource Rule Entry for resource name SYSTRAN:

```
ACF
SET RESOURCE( SAF )
COMPILE STORE
$KEY( SYSTRAN ) TYPE( SAF )
UID( USER01 ) ALLOW SERVICE( READ )
```

Note If the resource name SYSTRAN in the SAF Resource Rule Entry does not exist, user access to the Cisco IOS for S/390 internal debugging services TCPEEP, ACTEST, and SYSSTAT is denied automatically by CA-ACF2.

7 Activate Resource Rule Entry for Cisco IOS for S/390 application services.

You can use command security to limit access to the Cisco IOS for S/390 application with an APPL statement in member APPCFG*xx*. Set the SECURITY parameter to something other than the default of SECURITY(NO).

The Telnet commands ACTEST and SYSSTAT use the SYSTRAN resource name in the SAF Resource Rule Entry. To change the SYSTRAN resource name or to add security to other commands, use the SECURITY parameter of the APPL statement in member APPCFG*xx*. Read the *Cisco IOS for S/390 Customization Guide* for more information.

Whenever an application defaults to or sets APPL SECURITY(NO) in member APPCFG*xx*, Cisco IOS for S/390 allows universal access to the service.

Define a NETSTAT application service in member APPCFG*xx* as follows:

```
APPL NAME( NETSTAT ) SECURITY( YES )
```

Provide a valid user ID and password combination to Cisco IOS for S/390 that has been authorized for access to the NETSTAT resource name in the SAF Resource Rule Entry to use the NETSTAT command.

The NETSTAT resource name in the SAF Resource Rule Entry should be the same as its service NAME (in this case, NETSTAT) with SECURITY(YES) specified on an APPL statement. Cisco IOS for S/390 checks the NETSTAT resource name in the SAF Resource Rule Entry for command security authorization before allowing a user ID access to the NETSTAT command.

Use this command to define the NETSTAT resource name in the SAF Resource Rule Entry:

```
ACF
SET RESOURCE( SAF )
COMPILE STORE
$KEY( NETSTAT ) TYPE( SAF )
UID( USER01 ) ALLOW SERVICE( READ )
```

Define a NETSTAT application service in member APPCFG*xx* as follows:

```
APPL NAME( NETSTAT ) SECURITY( SYSTEM )
```

Provide a valid user ID and password combination to Cisco IOS for S/390 that has been authorized for access to the SYSTEM resource name in the SAF Resource Rule Entry to use the NETSTAT command.

Cisco IOS for S/390 checks the SYSTEM resource name in the SAF Resource Rule Entry (as specified on the SECURITY parameter) for command security authorization before allowing a user ID access to the NETSTAT command. Issue these commands to define the SYSTEM resource name in the SAF Resource Rule Entry:

```
ACF
SET RESOURCE( SAF )
COMPILE STORE
$KEY( SYSTEM ) TYPE( SAF )
UID( USER01 ) ALLOW SERVICE( READ )
```

8 To activate the changes in numbers 2 through 7, perform an IPL or issue a GSO console operator refresh. Use this command for the refresh:

```
F ACF2,REFRESH( ALL )
```

Customizing CA-ACF2 Version 6 or Later

1 Create a logon ID (LID) record to associate with the startup JCL.

Follow the installation procedures of your site to create an LID record; make sure these parameters are set in the Privileges Section - Group 2:

```
MUSASS
NO-INH
BDT
```

Read the CA-ACF2 Administrator's Guide for instructions on creating LIDs.

Place the LID in the USER field of the start-up JCL job card.

If your site runs CA-ACF2 6.0 or higher, it is not necessary to set NON-CNCL in the Cisco IOS for S/390 LID record.

Note To prevent unauthorized users from attempting to use the production user ID for Cisco IOS for S/390, the TCP base product rejects all logon attempts to Cisco IOS for S/390 from programs like FTP and ACTEST that use this ID.

2 Update GSO records for Cisco IOS for S/390.

Enter all commands exactly as shown. Do not change the SUBSYS=SNSTCP in the first SAFDEF record. SNSTCP in the SUBSYS parameter relates to parameters on the SAF security calls (not the LID chosen by the site).

```
ACF
SET CONTROL( GSO )
INSERT CLASMAP.AC#CMD RESOURCE( AC#CMD ) RSRCTYPE( SAF )     ENTITYLN( 8 )
CHANGE INFODIR TYPES( D-RSAF )
INSERT SAFDEF.ACSECPC ID( ACSECPC )    MODE( GLOBAL )
       PROGRAM(BYPASS#1) RACROUTE(SUBSYS=SNSTCP,REQSTOR=ACSECPC)
INSERT SAFDEF.ACSECPC ID( ACSECPC )    MODE( GLOBAL )
       PROGRAM(BYPASS#2) RACROUTE(SUBSYS=SNSTCP,REQSTOR=ACSECPC)
INSERT SAFDEF.ACSECPC ID( ACSECPC )    MODE( GLOBAL )
       PROGRAM(BYPASS#3) RACROUTE(SUBSYS=SNSTCP,REQSTOR=ACSECPC)
INSERT SAFDEF.ACSECPC ID( ACSECPC )    MODE( GLOBAL )
       PROGRAM(BYPASS#4) RACROUTE(SUBSYS=SNSTCP,REQSTOR=ACSECPC)
INSERT SAFDEF.ACCFTP2 ID(ACCFTP2)      MODE(GLOBAL)
       PROGRAM(ACCFTP2) RACROUTE(REQUEST=EXTRACT)
INSERT SAFDEF.FTP ID(FTP)                          MODE(GLOBAL) PROGRAM(FTP)
       RACROUTE(REQUEST=EXTRACT)
INSERT SAFDEF.FTP2 ID(FTP2)                        MODE(GLOBAL) PROGRAM(FTP2)
       RACROUTE(REQUEST=EXTRACT)
INSERT SAFDEF.FTP3 ID(FTP3)                        MODE(GLOBAL) PROGRAM(FTP3)
       RACROUTE(REQUEST=EXTRACT)
END
```

3 Use this command to build the INFODIR SAF records for Cisco IOS for S/390:

```
F ACF2,REBUILD( SAF ),CLASS( R )
```

4 Update GSO records to allow password extraction for TCPEEP and FTP2.

Certain Cisco IOS for S/390 programs can extract encrypted passwords. The encrypted passwords can be used to sign a user on to the Cisco IOS for S/390 address space. CA-ACF2 6.0 (and higher) systems can globally enable or disable password extraction.

On systems running CA-ACF2 6.0, use these commands to see if password extraction is globally enabled or disabled:

```
ACF
SET CONTROL(GSO)
SHOW STATE
```

If NOPSWDXTR is indicated, encrypted password gathering has been globally disabled at the CA-ACF2 6.0 level.

Use these commands on systems running CA-ACF2 6.1 or higher, to see if password extraction is globally enabled or disabled:

```
ACF
SET CONTROL(GSO)
LIST PSWD
```

If NOPSWDXTR is indicated, encrypted password gathering has been globally disabled.

To globally enable encrypted password gathering (on systems running CA-ACF2 6.0 or higher) issue these commands:

```
ACF
SET CONTROL(GSO)
CHANGE PSWD PSWDXTR
```

Use this operator command to activate the change to the GSO record:

```
F ACF2,REFRESH(PSWD)
```

Before an CA-ACF2 LID record that has the NOPSWD-XTR field set can use the changes described here for PSWDXTR, these steps must occur:

— The NOPSWD-XTR field in the LID record must be changed to PSWD-XTR.

— The user ID must be signed on to MVS and its password must be changed so the updated password can be stored in the CA-ACF2 data base in a way that encrypted password sign-ons can be used.

Note You cannot use the ACF CHANGE command to turn on or off password extraction for individual LID records. The PSWD-XTR field cannot be set directly in the LID record (as it depends on the GSO option and the expiration of passwords). Read the PSWD section in the GSO records chapter of the CA-ACF2 6.X MVS Administrator Guide for information about how to change PSWD-XTR for the user community.

5 Set proper authority over mail data sets in the Cisco IOS for S/390 LID record.

The LID associated with the Cisco IOS for S/390 job must have allocation access authority to the HLQ(s) on the PATH parameter of the SMTP statement in member APPCFG*xx*. When you set the rules for the LID, set the ALLOC parameter to ALLOC(A).

The PATH parameter of the SMTP statement specifies the HLQ(s) for mail DASD data set names. SMTP requires that a data set naming convention be established for outgoing mail. The HLQ(s) for mail should be unique. If the HLQ for Cisco IOS for S/390 data sets is TCPACCES, consider defining the HLQ for E-mail as PATH(TCPACCES.EMAIL). If you assign PATH(TCPACCES) as the HLQ, the client mail handler tries to send all the Cisco IOS for S/390 system data sets as mail data sets.

If the PATH parameter on the SMTP statement contains PATH(TCPACCES.EMAIL) and the Cisco IOS for S/390 LID is TCPACCES, use the following CA-ACF2 commands to permit the TCPACCES and SYS1 LIDs alter authority:

```
ACF
SET RULE
COMPILE
$KEY(TCPACCES)
$OWNER(‘Production TCPACCES’)
- UID(TCPACCES) READ (A) WRITE(A) ALLOC(A) EXEC(A)
- UID(SYS1-)  READ (A) WRITE(A) ALLOC(A) EXEC(A)
- UID(-) READ(A)
EMAIL.- UID(TCPACCES) READ(A) WRITE(A) ALLOC(A) EXEC(A)
EMAIL.- UID(SYS1-)  READ(A) WRITE(A) ALLOC(A) EXECA(A)
EMAIL.- UID(-) READ(A)
END
STORE
END
```

Adjust the user ID to the naming conventions of the installation site.

To avoid data set enqueue conflicts, choose a unique PATH name for every Cisco IOS for S/390 address space running at a site. PATH names of TCPACCES.EMAIL and TCPACCES.EMAIL2 are valid for separate Cisco IOS for S/390 address spaces because the second level in the name is unique. The names TCPACCES.EMAIL and TCPACCES.EMAIL.A are not recommended because the second PATH name is a subset of the first.

6 Protecting packet trace programs from unauthorized use.

Packet tracing programs must be protected from unauthorized usage. Program T03PTCPE, and its alias TCPEEP, traces packets in and out of the network. Logon IDs, passwords, and perhaps proprietary installation data, can be seen with the packet trace programs.

Resource rules at the program level is the mechanism within CA-ACF2 to protect programs. The following commands can be used to protect program T03PTCPE and its alias, TCPEEP, in library TCPACCES.LINKLIB where UIDs beginning with SYS1 are granted access:

```
ACF
SET RULE
COMPILE
$KEY(TCPACCES)
$OWNER(‘Production TCPacces’)
LINKLIB UID(SYS1-) PGM(T03PTCPE) EXEC(A) READ(A) WRITE(A) ALLOC(A)
LINKLIB UID(SYS1-) PGM(TCPEEP) EXEC(A) READ(A) WRITE(A) ALLOC(A)
LINKLIB UID(-) EXEC(A) READ(A)
END
STORE
END
```

7 User validation is required for access to Cisco IOS for S/390 internal debugging services ACTEST and SYSSTAT; validation is performed by checking resource name SYSTRAN in the SAF Resource Rule Entry.

Users are prompted for a user ID and password when they invoke ACTEST or SYSSTAT. The user ID and password are validated by the CA-ACF2 security system. If the user ID and password are valid, the security system also checks to see if the user is authorized to access the resource name SYSTRAN in the SAF Resource Rule Entry. If the user ID is not authorized for a minimum of read access to the SYSTRAN resource name in the SAF Resource Rule Entry, then access to ACTEST or SYSSTAT is denied.

In this example, user ID USER01 will be the only user ID that will have access to the Cisco IOS for S/390 debugging services. Replace user ID USER01 with the user ID of your local Cisco IOS for S/390 systems programmer.

Use these commands to define the SAF Resource Rule Entry for resource name SYSTRAN:

```
ACF
SET RESOURCE( SAF )
COMPILE STORE
$KEY( SYSTRAN ) TYPE( SAF )
UID( USER01 ) ALLOW SERVICE( READ )
```

Note If the resource name SYSTRAN in the SAF Resource Rule Entry does not exist user access is automatically denied by CA-ACF2 to the Cisco IOS for S/390 internal debugging services ACTEST and SYSSTAT.

8 Activate Resource Rule Entry for Cisco IOS for S/390 application services.

You can use Cisco IOS for S/390 command security to limit access to an application for any APPL statement in member APPCFG*xx*. Set the SECURITY parameter to something other than the default of SECURITY(NO).

The Telnet commands ACTEST and SYSSTAT use the SYSTRAN resource name in the SAF Resource Rule Entry. To change the SYSTRAN resource name or to add security to other commands, use the SECURITY parameter of the APPL statement in member APPCFG*xx*. Read the *Cisco IOS for S/390 Customization Guide* for more information.

Whenever an application defaults to, or sets, APPL SECURITY(NO) in member APPCFG*xx*, Cisco IOS for S/390 allows universal access to the service.

Define a NETSTAT application service in member APPCFG*xx* as follows:

```
APPL NAME(NETSTAT) SECURITY(YES)
```

Provide a valid user ID and password combination to Cisco IOS for S/390 that has been authorized for access to the NETSTAT resource name in the SAF Resource Rule Entry to use the NETSTAT command.

The NETSTAT resource name in the SAF Resource Rule Entry name would be same as its service NAME (in this case NETSTAT) with SECURITY(YES) specified on an APPL statement. Cisco IOS for S/390 checks the NETSTAT resource name in the SAF Resource Rule Entry for command security authorization before allowing a user ID access to the NETSTAT command. Issue this command to define the NETSTAT resource name in the SAF Resource Rule Entry:

```
ACF
SET RESOURCE( SAF )
COMPILE STORE
$KEY( NETSTAT ) TYPE( SAF )
UID( USER01 ) ALLOW SERVICE( READ )
```

Define a NETSTAT application service in member APPCFG*xx* as follows:

```
APPL NAME( NETSTAT ) SECURITY( SYSTEM )
```

Provide a valid user ID and password combination to Cisco IOS for S/390 that has been authorized for access to the SYSTEM resource name in the SAF Resource Rule Entry to use the NETSTAT command.

Cisco IOS for S/390 checks the SYSTEM resource name in the SAF Resource Rule Entry (as specified on the SECURITY parameter) for command security authorization before allowing a user ID access to the NETSTAT command.

Use this command to define the SYSTEM resource name in the SAF Resource Rule Entry:

```
ACF
SET RESOURCE( SAF )
COMPILE STORE
$KEY( SYSTEM ) TYPE( SAF )
UID( USER01 ) ALLOW SERVICE( READ )
```

9 CA-ACF2: Using The Source Security Within Cisco IOS for S/390.

Cisco IOS for S/390 has the ability to pass a Source terminal ID to CA-ACF2 during sign-on attempts. Cisco IOS for S/390 passes either the remote IP address or the actual VTAM terminal ID in the Terminal field during sign-on attempts.

Source security customization is an optional feature. Any site that does not currently implement Source security can skip this step.

For more detailed information about Source security for terminals, see the *CA-ACF2 MVS Administrator Guide*.

To use the Source security within Cisco IOS for S/390, follow these steps:

Step 1 SAMP member A03ACCES shows the VTAM APPL names beginning with A03VLT. This member is a model to use or modify for local use.

The CA-ACF2 security administrator should group all the VTAM APPL names associated with Cisco IOS for S/390 into an X-SGP source record. Currently, there is no mechanism within Cisco IOS for S/390 to map VTAM LU usage to specific logon IDs at the VTAM logon points. You do not know which LU will be allocated at these logon points. The LUs used at VTAM logon points within Cisco IOS for S/390 are allocated by ACCPOOL. Do not confuse the LUPOOL capability to map IP addresses to logon IDs with ACCPOOL LU customization. All logon ID records that need access to Cisco IOS for S/390 through VTAM can then have the new source group added to their source GROUP records.

The CA-ACF2 security administrator can create X-SGP source records for the A03ACCES SAMP member by issuing these commands for VTAM usage:

```
          SET ACF
          SET X(SGP)

INSERT A03VLT SOURCE INCLUDE(A03VLT-) ADD
```

The CA-ACF2 security administrator should check with both the Cisco IOS for S/390 and VTAM systems programmers to identify which VTAM LUs are being used by the site for access within Cisco IOS for S/390.

Step 2 All logon IDs who want to sign on to Cisco IOS for S/390 must be permitted Source authority to the Cisco IOS for S/390 IP address(es) as specified on the IP address parameter for every NETWORK statement in TCPCFGxx member.

A sample NETWORK statement in member TCPCFG*xx* may begin like this:

```
NETWORK IPADDRESS(138.42.224.15)
```

The security system accepts source IDs only in hexadecimal form, so the above IP address must be converted. IP address 138.42.224.15 would use a terminal ID of 8A2AE00F (where 138 = 8A, 42 = 2A, 224 = E0, and 15 = 0F).

Use these commands to create an X-SGP Source record at a site to sign on to Cisco IOS for S/390 using its default IP address of 138.42.224.15 for source 8A2AE00F:

```
SET ACF
SET X(SGP)
INSERT 8A2AE00F SOURCE INCLUDE(8A2AE00F) ADD
```

All logon ID records that need access to Cisco IOS for S/390 must then have the new source entry 8A2AE00F added to their source GROUP records.

Step 3 Any individual logon ID that uses authorized Telnet commands or FTP from a remote site needs READ access authority for the terminal IP address of the remote site. The originating remote IP address is used for all sign-on attempts.

To create an X-SGP Source record at a site to sign on to Cisco IOS for S/390 using its host IP address 138.42.224.250 for source 8A2AE0FA, issue the following commands:

```
SET ACF
SET X( SGP )
INSERT 8A2AE0FA SOURCE INCLUDE( 8A2AE0FA ) ADD
```

This X-SGP source record can now be placed in the source group record for any logon IDs coming in from host 138.42.224.250.

Step 4 A CA-ACF2 administrator can create a generic X-SGP Source record for 8A2AE0- for the local network of 138.42.220 with the following commands:

```
SET ACF
SET X( SGP )
INSERT 8A2AE0 SOURCE INCLUDE( 8A2AE0** ) ADD
```

This X-SGP source record can now be placed in the source group record for any logon IDs coming in from the local network.

Step 5 Activate the X-SGP records with these CA-ACF2 operator console command:

```
F ACF2,NEWXREF,TYPE( SGP )
```

Step 6 Configure Cisco IOS for S/390 to place the terminal ID on all security parameter lists passed to CA-ACF2 for all sign-on attempts to Cisco IOS for S/390. If you place TERMID into the XSEC parameter list on the SECURITY statement in the IJTCFG*xx* member, this happens automatically. By default, terminal IDs are not passed on any sign-on call.

To activate passing Source terminal IDs on the security parameter list to CA-ACF2 for an active Cisco IOS for S/390 address space, issue the following command under ACTEST:

```
XSEC TERMID ON
```

To deactivate passing Source terminal IDs on the security parameter list to CA-ACF2 for an active Cisco IOS for S/390 address space, use this command under ACTEST:

```
XSEC TERMID OFF
```

Step 7 To enable sign-on checking for Telnet users, add the CPASSWORD option to the Telnet related SERVICE statement(s) in APPCFG*xx* for Telnet ports (typically, 23,1023).

Caution Activate Source security checking only after all CA-ACF2 customization for Cisco IOS for S/390 has been completed. CA-ACF2 Source security can prevent anyone from signing on to MVS, as well as Cisco IOS for S/390, if the customization is performed incorrectly.

Jobs submitted by TERMID checked logon IDs will fail security unless explicit user IDs and passwords are given when NO-INH is associated with the logon ID of the submitter.

10 To activate the changes in numbers 2 through 8, perform an IPL or issue a GSO console operator refresh. Use this command for the refresh:

```
F ACF2,REFRESH( ALL )
```

CA-TOP SECRET Options

This section describes the types of security options available to sites running CA-TOP SECRET.

Types of CA-TOP SECRET Security

Cisco IOS for S/390 uses these types of security with CA-TOP SECRET:

- Sign-on Security

  All user ID/password combinations are validated by CA-TOP SECRET
- Data set Security

  All file transfers under FTP are validated by CA-TOP SECRET
- Resource Security

  Restricts service in the Server Telnet control table.
- Source level security for FTP IP addresses, VTAM LUs, and Telnet services

The Cisco IOS for S/390 command security interface restricts access to services in the Server Telnet control table. ACTEST and SYSSTAT services should be protected with resource security

To maintain system security, restrict access to system programmers and operations personnel. Inexperienced users can cause serious damage to system performance and reliability through the ACTEST and SYSSTAT services.

CA-TOP SECRET Customization

The Cisco IOS for S/390 address space functions as a true FACILITY to CA-TOP SECRET. Use this setup to enable Cisco IOS for S/390 with CA-TOP SECRET:

1 Set up an Cisco IOS for S/390 FACILITY entry with CA-TOP SECRET options as shown in this example:

```
FAC( USERx=NAME=TCPACCES )
FAC( TCPACCES=PGM=ACB )
FAC( TCPACCES=ACTIVE,NOABEND,NOASUBM,NOAUDIT,AUTHINIT,ID=c )
FAC( TCPACCES=NOINSTDATA,KEY=8,LCFCMD,LOCKTIME=0,NOLUMSG,LOG( NONE ) )
FAC( TCPACCES=NOMRO,MULTIUSER,NOPSEUDO,NORNDPW,RES,SIGN( M ) )
FAC( TCPACCES=SHRPRF,NOSTMSG,TENV,NOTSOC,WARNPW,NOXDEF )
```

In the above example, the Cisco IOS for S/390 FACILITY is named TCPACCES. You can use any name up to eight bytes in length. If another name is used, it must be substituted in the setup examples.

USER*x* can be any user-defined resource type available at the installation and the x value can be any keyboard character.

For ID=c, c is equal to a single alphanumeric that represents the FACILITY for reporting purposes (see FACILITY under CA-TOP SECRET control options).

RNDPW (RaNDomPassWords, or return expired new random passwords) can be set on the TCP base product FACILITY. However, only FTP will return all the messages from CA-TOP SECRET when the password expires. When RNDPW is placed on your FACILITY definition in a CA-TOP SECRET environment, CA-TOP SECRET returns a new randomly generated password when an expired password associated with an ACcessor ID (ACID) has been correctly presented during sign-on.

Note Do not place operands NOPSEUDO, NOMRO, and TENV on the FACILITY definition under CA-TOP SECRET 4.3 or above; these operands are no longer supported.

2 Give ACIDs access to the Cisco IOS for S/390 FACILITY.

To permit ACID USER01 access to the Cisco IOS for S/390 FACILITY (TCPACCES), the security administrator must issue this command:

```
TSS ADD( USER01 ) FAC( TCPACCES )
```

3 Create the Cisco IOS for S/390 ACID.

Build the ACID for the Cisco IOS for S/390 address space with the TSS CREATE command. The following command creates ACID TCPACCESA to run as a started task:

```
TSS CREATE( TCPACCSA ) NAME( 'TCPACCES ACID' ) FAC( STC ) TYPE( USER )
PASS( NOPW ) DEPT( dept_name ) MASTFAC( TCPACCES )
```

Note To prevent unauthorized users from attempting to use the production ACID for Cisco IOS for S/390, the TCP base product rejects all logon attempts to Cisco IOS for S/390 from programs like FTP and ACTEST that use this ACID.

4 The Cisco IOS for S/390 ACID must have authority to access the data sets it needs to function in the customer's environment.

If you unloaded all the Cisco IOS for S/390 data sets with the HLQ TCPACCES and the Cisco IOS for S/390 ACID is TCPACCSA, then the security administrator can grant access to the Cisco IOS for S/390 ACID TCPACCSA by issuing this command:

```
TSS PERMIT( TCPACCSA ) DSN( TCPACCES ) ACCESS( UPDATE )
```

5 Protecting packet trace programs from unauthorized use.

Packet tracing programs must be protected from unauthorized usage. Program T03PTCPE, and its alias TCPEEP, traces packets in and out of the network. ACIDs, passwords, and perhaps proprietary installation data, can be seen with the packet trace programs.

Resource rules at the program level is the mechanism within CA-Top Secret to protect programs. The following commands can be used to protect program T03PTCPE and its alias, TCPEEP, where department SYKSDEPT owns the programs and ACID SYSUSER has access:

```
TSS ADD( SYSDEPT ) PROG( T03PTCPE )
TSS ADD( SYSDEPT ) PROG( TCPEEP )
TSS PER( SYSUSER ) PROG( T03PTCPE )
TSS PER( SYSUSER ) PROG( TCPEEP )
```

6 Set up Cisco IOS for S/390 as a started task.

If Cisco IOS for S/390 runs as a started task, the relationship also must be established in the CA-TOP SECRET STC record. The following TSS ADDTO command connects the started task with the ACID defined by the TSS CREATE command. This example assumes that the Cisco IOS for S/390 PROC name is SWPROC and the ACID defined for use by the Cisco IOS for S/390 Task is TCPACCSA:

```
TSS ADDTO( STC ) PROC( SWPROC ) ACID( TCPACCSA )
```

7 Set up Cisco IOS for S/390 as a batch job.

If Cisco IOS for S/390 is run as a batch job, the relationship is established by the USER= value coded on the job card. In this example, the Cisco IOS for S/390 job must be coded with USER=TCPACCSA.

8 If the SMTP E-mail services are being used, that is, the PATH parameter of the SMTP statement in member APPCFG*xx* is specified, then the ACID associated with the Cisco IOS for S/390 job or started task must have CREATE and SCRATCH access to the HLQ specified on the PATH parameter.

If the PATH parameter is specified as PATH(TCPACCES.EMAIL) and the ACID associated with the Cisco IOS for S/390 job or started task is TCPACCSA, then the security administrator can allow access by issuing this command:

```
TSS PER( TCPACCSA ) DSN( TCPACCES.EMAIL.% ) ACCESS( CREATE )
```

To avoid data set enqueue conflicts, choose a unique PATH name for every Cisco IOS for S/390 address space running at a site. PATH names of TCPACCES.EMAIL and TCPACCES.EMAIL2 are valid for separate Cisco IOS for S/390 address spaces because the second level in the name is unique. The names TCPACCES.EMAIL and TCPACCES.EMAIL.A are not recommended because the second PATH name is a subset of the first.

If you assign PATH(TCPACCES) as the HLQ, the client mail handler tries to send all the Cisco IOS for S/390 system data sets as mail data sets.

9 User validation is required for access to Cisco IOS for S/390 internal debugging services ACTEST and SYSSTAT; validation is performed by checking to see if an ACID has access to entry SYSTRAN in CA-TOP SECRET's User Resource Class UR1.

Users are prompted for an ACID and password when they invoke ACTEST or SYSSTAT. The ACID and password are validated by the security system and if valid, the security system also validates the user ID for authority to access the SYSTRAN entry in CA-TOP SECRET's User Resource Class UR1. If the user is not permitted a minimum of read access to the SYSTRAN entry in the User Resource Class UR1, access to ACTEST and SYSSTAT is denied.

Use the following CA-TOP SECRET command to find the resource entry names being used:

```
TSS WHOOWNS UR1( * )
```

Use the following command to define Cisco IOS for S/390 entry SYSTRAN in User Resource Class UR1 owned by user USER01:

```
TSS ADDTO( USER01 ) UR1( SYSTRAN )
```

The security administrator can now permit user USER02 to use the SYSTRAN entry in class UR1 with this command:

```
TSS PERMIT( USER02 ) UR1( SYSTRAN ) ACCESS( READ )
```

This permits user USER02 access to the ACTEST and SYSSTAT debugging services.

Note If the Cisco IOS for S/390 entry SYSTRAN in User Resource Class UR1 does not exist, user access is denied by CA-Top Secret to the Cisco IOS for S/390 internal debugging services ACTEST and SYSSTAT.

10 You can use command security to limit access to any application with an APPL statement in member APPCFG*xx*. Set the SECURITY parameter to something other than the default of SECURITY(NO).

The Telnet commands ACTEST and SYSSTAT use the entry SYSTRAN in User Resource Class UR1. To change the SYSTRAN entry or to add security to other commands, use the SECURITY parameter of the APPL statement in member APPCFG*xx*. Read the *Cisco IOS for S/390 Customization Guide* for more information.

Whenever an application defaults to, or sets, APPL SECURITY(NO) in member APPCFG*xx*, Cisco IOS for S/390 allows universal access to that particular application.

Use the following command to define a NETSTAT application service in member APPCFG*xx* as:

```
APPL NAME(NETSTAT) SECURITY(YES)
```

Provide a valid ACID password combination to Cisco IOS for S/390 that has access to the NETSTAT entry in the User Resource Class UR1 to use the NETSTAT command.

The NETSTAT entry in the User Resource Class UR1 should be same as its service NAME (in this case NETSTAT) with SECURITY(YES) specified on an APPL statement. Cisco IOS for S/390 checks the NETSTAT entry in the User Resource Class UR1 for command security authorization before allowing an ACID access to the NETSTAT command.

Use the following command to define the NETSTAT entry in the User Resource Class UR1:

```
TSS ADDTO( USER01 ) UR1( NETSTAT )
TSS PERMIT( USER02 ) UR1( SYSTRAN ) ACCESS( READ )
```

In the above example the NETSTAT entry in User Resource Class UR1 is owned by ACID USER01. ACID USER02 has authority to issue the NETSTAT command.

Define a NETSTAT application service in member APPCFG*xx* as follows:

```
APPL NAME( NETSTAT ) SECURITY( SYSTEM )
```

Provide a valid ACID password combination to Cisco IOS for S/390 that has access to the SYSTEM entry in the SAF Resource Rule Entry to use the NETSTAT command.

Cisco IOS for S/390 checks the SYSTEM entry in User Resource Class UR1 (as specified on the SECURITY parameter above) for command security authorization before allowing an ACID access to the NETSTAT command.

Use the following command to define the SYSTEM entry in the User Resource Class UR1:

```
TSS ADDTO( USER01 ) UR1( SYSTEM )
TSS PERMIT( USER02 ) UR1( SYSTEM ) ACCESS( READ )
```

In the above example the SYSTEM entry in User Resource Class UR1 is owned by ACID USER01. ACID USER02 has authority to issue the NETSTAT command.

11 CA-TOP SECRET: Using The Terminal Security Class Within Cisco IOS for S/390.

Terminal security customization is an optional feature. Any site that currently does not implement Terminal security may skip this step.

Step 1 Cisco IOS for S/390 can pass a terminal ID to CA-TOP SECRET during sign-on attempts. Cisco IOS for S/390 passes either the remote IP address or the actual VTAM terminal ID in the Terminal field during sign-on attempts.

To use the Terminal security class within Cisco IOS for S/390, complete the remaining steps.

Step 2 Read the *CA-TOP SECRET Implementation: General Guide* for information on Terminal security. Be careful when activating Terminal security for the first time. If done incorrectly, no one will be able to sign on to either MVS or Cisco IOS for S/390.

Research these sample commands for turning on Terminal security:

```
TSS LIST( RDT ) RESCLASS( TERMINAL )
TSS REPLACE( RDT ) ATTR( GENERIC,NODEFPROT ) DEFACC( READ )
```

Issuing the following CA-TOP SECRET command prevents all undefined terminals from signing on to an address space using Terminal security access to your site. This can be very useful in restricting access to Cisco IOS for S/390 via IP addresses. Undefined IP addresses will not be permitted to sign on to Cisco IOS for S/390.

```
TSS REPLACE( RDT ) ATTR( GENERIC,DEFPROT ) DEFACC( NONE )
```

Step 3 All ACIDs must be permitted READ access authority to the VTAM Terminal APPL names (not ACBNAMEs) that need to access Cisco IOS for S/390 through VTAM logon points.   There is no current mechanism within Cisco IOS for S/390 to map VTAM LU usage to specific ACIDs at the VTAM logon points. You do not know which LU will be allocated at these logon points. The LUs used at VTAM logon points within Cisco IOS for S/390 are allocated by ACCPOOL. Do not confuse the LUPOOL capability to map IP addresses to an ACID with ACCPOOL LU customization.

SAMP member A03ACCES shows VTAM APPL names beginning with A03VLT. This member is a model to use or modify for local use.

The CA-TOP SECRET security administrator can use the following CA-TOP SECRET commands to define the terminals and designate which ACID can access Cisco IOS for S/390 via VTAM utilizing the A03VLT*xx* VTAM APPLs:

```
TSS ADD( acid ) TERM( A03VLT )
TSS PER( acid ) TERM( A03VLT ) ACCESS( READ )
```

If the CA-TOP SECRET system administrator gives access to Cisco IOS for S/390 via the VTAM interfaces only to departments SYS1 and ENG, the terminals can be protected as defined in A03ACCES with the following CA-TOP SECRET commands:

```
TSS ADD( SYS1 ) TERM( A03VLT )
TSS PER( ENG ) TERM( A03VLT ) ACCESS( READ )
```

The CA-TOP SECRET security administrator should check with both the Cisco IOS for S/390 and VTAM system's programmers to identify which VTAM LUs are being used by the site for access within Cisco IOS for S/390.

Step 4 All ACIDs wanting to sign on to Cisco IOS for S/390 must be permitted READ access authority to the Cisco IOS for S/390 IP address(es) as specified on the IP address parameter for every NETWORK statement in the TCPCFG*xx* member.

A sample NETWORK statement in member TCPCFG*xx* may begin like this:

```
NETWORK IPADDRESS(138.42.224.15)
```

The security system accepts terminal IDs only in hexadecimal form, so the above IP address must be converted. IP address 138.42.224.15 uses a terminal ID of 8A2AE00F (where 138 = 8A, 42 = 2A, 224 = E0, and 15 = 0F).

To allow all ACIDs at a site to sign on to Cisco IOS for S/390 for a default IP address of 138.42.224.15 with terminal 8A2AE00F, issue these commands:

```
TSS ADD(acid) TERM(8A2AE00F)
TSS PER(ALL) TERM(8A2AE00F) ACCESS(READ)
```

If you replace ACCESS(READ) on the above command with ACCESS(NONE), the CA-TOP SECRET security administrator must use the CA-TOP SECRET PERMIT command to allow READ access to all ACIDs or departments that need to sign on to Cisco IOS for S/390.

Step 5 Any individual ACID using authorized Telnet commands or FTP from a remote site into Cisco IOS for S/390 must have READ access authority for the terminal that represents the IP address of the remote site. The originating remote IP address is used for all sign-on attempts to Cisco IOS for S/390 once a connection to Cisco IOS for S/390 is made.

If local ACID USER01 comes off the local network from host 138.42.224.250, then this ACID needs to be permitted access to this IP address via terminal 8A2AE0FA. This can be done with the following commands:

```
TSS ADD(acid) TERM(8A2AE0FA)
TSS PER(USER01) TERM(8A2AE0FA) ACCESS(READ)
```

A CA-TOP SECRET administrator can allow everyone on his local network (138.42.224) access to Cisco IOS for S/390 with the following CA-TOP SECRET commands:

```
TSS ADD(acid) TERM(8A2AE0)
TSS PER(ALL) TERM(8A2AE0) ACCESS(READ)
```

Step 6 Configure Cisco IOS for S/390 to place the terminal ID on all security parameter lists passed to CA-TOP SECRET for all sign-on attempts to Cisco IOS for S/390. If you place TERMID into the XSEC parameter list on the SECURITY statement in the IJTCFGxx member, this happens automatically. By default, Cisco IOS for S/390 does not place the terminal ID on any sign-on call.

To activate passing terminal IDs on the security parameter list to CA-TOP SECRET for an active Cisco IOS for S/390 address space, use the following command under ACTEST:

```
XSEC TERMID ON
```

You can deactivate passing terminal IDs on the security parameter list to CA-TOP SECRET for an active Cisco IOS for S/390 address space by issuing the following command under ACTEST:

```
XSEC TERMID OFF
```

Step 7 To enable sign-on checking for Telnet users, add the CPASSWORD option to the SERVICE statement in the APPCFG*xx* member for Telnet ports (typically, 23,1023).

RACF Options

If a computer site runs RACF, the Cisco IOS for S/390 RACF interface automatically becomes active upon installation. This section describes the types of security options available to sites running RACF and how to customize security for Cisco IOS for S/390.

Types of RACF Security

With RACF, these types of security are active in Cisco IOS for S/390:

- Sign-on security

  All user ID/password combinations are validated by RACF

- Data set security

  All file transfers under FTP are validated by RACF

- Source level security for FTP IP addresses, VTAM LUs, and Telnet services

In addition to automatic data set and sign-on security, Cisco IOS for S/390 provides command security. Read Customizing Command Security with RACF for instructions on customizing security.

The Cisco IOS for S/390 security interface for commands restricts access to application segment services defined in member APPCFG*xx*. Cisco IOS for S/390 command security protects the following:

- ACTEST
- SYSSTAT

To maintain a high level of system security, only system programmers and operations personnel should have access to these services. Inexperienced users can cause serious damage to system performance and reliability through the ACTEST and SYSSTAT services.

Customizing Command Security with RACF

Cisco IOS for S/390 uses the local installation-defined resource classes of RACF to implement command security. Refer to IBM document SPL: RACF SC28-1343 for additional information regarding the macros and tables described in this section.

1 Modify the installation local class descriptor table.

Place member ICHERCDE in the SAMP data set in your installation source of ICHRRCDE (local class descriptor table).

Follow your site’s installation procedures to update the local class descriptor table ICHERCDE.

Member ICHRRCDE in the SAMP data set is an example of the general resource class AC#CMD of Cisco IOS for S/390. The Cisco IOS for S/390 general resource class description must be used as shown except for the ID, OPER, and POSIT parameters:

AC#CMD ICHERCDE CLASS=AC#CMD	class name; do not change
ID=128	Unique ID between 128 and 255
MAXLNTH=8	Up to 8 character profile name
FIRST=ALPHA	First character is alphabetic
OPER=YES	Allow operations people free reign
OTHER=ALPHANUM	
POSIT=25	Must be in range 25 and 55
DFTUACC=NONE	Must be NONE

Note The first four characters of each resource class name must be different from the first four characters of all other class names. One of the four characters should be a national or numeric character to avoid inadvertently choosing a future IBM class name.

2 Modify the local installation-defined router table.

Member ICHRFRTB in the SAMP data set is an example of the Cisco IOS for S/390 router entry. Add the following line from member ICHRFRTB in the SAMP data set into your installation source of ICHRFR01 (local router table) exactly as shown. Do not modify any of its parameters.

```
AC#CMD  ICHRFRTB CLASS=AC#CMD,ACTION=RACF
```

Follow the installation procedures of your site to update the local router table ICHRFR01.

3 Perform an IPL on the system with a CLPA to activate the local installation router and class descriptor tables.

4 Activate the AC#CMD resource class with the following command:

```
SETROPTS CLASSACT(AC#CMD)
```

5 Follow the installation procedures of your site to create a user ID associated with the Cisco IOS for S/390 job or started task.

This sample ADDUSER command creates user ID TCPACCES associated with Cisco IOS for S/390 in group PROD:

```
ADDUSER TCPACCES OWNER(PROD) DFLTGRP(PROD)
   NAME('TCPACCESACCESS') DATA('production job')
```

6 If your site is running Cisco IOS for S/390 as a started task, update member ICHRIN03.

Note To prevent unauthorized users from attempting to use the production user ID for Cisco IOS for S/390, the TCP base product rejects all logon attempts to Cisco IOS for S/390 from programs like FTP and ACTEST that use this ID.

7 Give the Cisco IOS for S/390 user ID proper authority over mail data sets.

The user ID associated with the Cisco IOS for S/390 job must have an access level of ALTER for the high-level qualifier (HLQ) on the PATH parameter on the SMTP statement in member APPCFG*xx*.

The PATH parameter of the SMTP statement specifies the HLQ for mail DASD data set names. SMTP requires that a data set naming convention be established for outgoing mail data sets.

The HLQ for mail must be unique. For example, if the HLQ for Cisco IOS for S/390 data sets is TCPACCES, define the E-mail HLQ as two levels, such as in PATH(TCPACCES.EMAIL). If the HLQ for E-mail is not unique, the client mail handler will attempt to send all the Cisco IOS for S/390 system data sets as mail data sets.

If the PATH parameter on the SMTP statement contains PATH(TCPACCES.EMAIL) and Cisco IOS for S/390 user is TCPACCES, the security administrator could use these RACF commands to permit alter authority for the TCPACCES user ID:

```
ADDSD 'TCPACCES.EMAIL.*' UACC( NONE ) OWNER( TCPACCES )
   DATA( 'TCPACCES MAIL DATA SET ')
PERMIT 'TCPACCES.EMAIL.*' ID( TCPACCES ) ACCESS( ALTER )
```

To avoid data set enqueue conflicts, choose a unique PATH name for every Cisco IOS for S/390 address space running at a site. PATH names of TCPACCES.EMAIL and TCPACCES.EMAIL2 would be valid for separate Cisco IOS for S/390 address spaces because the second level in the name is unique. The names TCPACCES.EMAIL and TCPACCES.EMAIL.A are not recommended because the second PATH name is a subset of the first.

8 Protecting packet trace programs from unauthorized use.

Packet tracing programs must be protected from unauthorized usage. Program T03PTCPE, and its alias TCPEEP, traces packets in and out of the network. User IDs, passwords, and perhaps proprietary installation data, can be seen with the packet trace programs.

Program control is a mechanism within RACF to protect programs. The following command turns on program control within RACF:

```
SETROPTS WHEN(PROGRAM)
```

The LINKLIB data set should contain programs T03PTCPE and its alias, TCPEEP. To protect these programs from unauthorized usage in library TCPACCES.LINK on VOLSER SYS001 where user SYSUSER can execute these unauthorized programs, issue the following commands:

```
ADDSD ‘TCPACCES.LINK’ UACC(EXECUTE)

RDEFINE PROGRAM T03PTCPE
ADDMEM(‘TCPACCES.LINK’/SYS001K/PADCHKK) UACC(NONE)
RDEFINE PROGRAM TCPEEP
ADDMEM(‘TCPACCES.LINK’/SYS001/PADCHK) UACC(NONE)
PERMIT T03PTCPE ID(SYSUSER) ACCESS(EXECUTE)
PERMIT TCPEEP ID(SYSUER) ACCESS(EXECUTE)
SETROPTS WHEN(PROGRAM) REFRESH
```

9 User validation is required for access to the Cisco IOS for S/390 internal debugging services ACTEST and SYSSTAT.

Users are prompted for a user ID and password when they invoke ACTEST and SYSSTAT. The user ID and password are validated by the security system. If the user ID and password are valid, the security system also checks to see if the user is authorized to access the SYSTRAN resource profile in the AC#CMD resource class. If the user is not authorized for a minimum of read access to the SYSTRAN resource profile, then access to ACTEST or SYSSTAT is denied.

Use the following command to define the Cisco IOS for S/390 profile SYSTRAN in resource class AC#CMD:

```
RDEFINE AC#CMD ( SYSTRAN ) UACC( NONE )
```

Use the following command to permit group SYS1 and user USER01 to use the SYSTRAN profile in class AC#CMD:

```
PERMIT SYSTRAN CLASS( AC#CMD ) ID( SYS1,USER01 ) ACCESS( READ )
```

This gives group SYS1 and user USER01 access to the ACTEST and SYSTAT debugging services.

Note If the RACF profile SYSTRAN does not exist or if the AC#CMD resource class is not defined and activated, user access is automatically allowed to the service.

10 Activate profiles for Cisco IOS for S/390 application services.

You can use command security to limit access to any application with an APPL statement in member APPCFG*xx*. Set the SECURITY parameter to something other than the default of SECURITY(NO) and use the SYSTRAN profile.

To change the profile or to add security to other commands, use the SECURITY parameter of the APPL statement in member APPCFG*xx*. Read the *Cisco IOS for S/390 Customization Guide* for more information.

Whenever an application defaults to or sets APPL SECURITY(NO) in member APPCFG*xx*, Cisco IOS for S/390 allows universal access to the service.

Define a NETSTAT application service in member APPCFG*xx* as follows

```
APPL NAME( NETSTAT ) SECURITY( YES )
```

Provide a valid user ID and password combination to Cisco IOS for S/390 that has been authorized for access to the NETSTAT profile. SECURITY(YES) tells Cisco IOS for S/390 to make command security calls using the service name for the profile name. In this example the NETSTAT profile name is NETSTAT.

Use the following command to define the NETSTAT profile in class AC#CMD:

```
RDEFINE AC#CMD ( NETSTAT ) UACC( NONE )
```

Use the following command to give group SYS1 and user ID USER01 permission to use the NETSTAT profile in class AC#CMD:

```
PERMIT NETSTAT CLASS( AC#CMD ) ID( SYS1,USER01 ) ACCESS( READ )
```

Define a NETSTAT application service in member APPCFGxx as follows:

```
APPL NAME( NETSTAT ) SECURITY( SYSTEM )
```

Provide a valid user ID and password combination to Cisco IOS for S/390 that has been authorized for access to the SYSTEM profile to use the NETSTAT command.

In this example the NETSTAT profile name is SYSTEM, as specified on the SECURITY parameter.

Use the following command to define the SYSTEM profile in class AC#CMD:

```
RDEFINE AC#CMD ( SYSTEM ) UACC( NONE )
```

Use the command to permit group SYS1 and user ID USER01 to use the SYSTEM profile in class AC#CMD:

```
PERMIT SYSTEM CLASS( AC#CMD ) ID( SYS1,USER01 ) ACCESS( READ )
```

Note Any new user ID defined to RACF while the Cisco IOS for S/390 address space is actively running, will not be allowed access to resources protected by command security (ACTEST SYSTAT) or any protected application services. Once the Cisco IOS for S/390 address space has been brought down and restarted, the new user ID will be allowed access to these services.

RACF: Using The Terminal Security Class within Cisco IOS for S/390

Cisco IOS for S/390 has the ability to pass a terminal ID to RACF during sign-on attempts. Cisco IOS for S/390 passes either the remote IP address or the actual VTAM terminal ID in the Terminal field during sign-on attempts.

Terminal security customization is an optional feature. Any site that currently does not implement Terminal security may skip this step.

To use the Terminal security class within Cisco IOS for S/390, follow these steps:

1. Read the RACF Security Administrator’s Guide (SC23-3726) for information on Terminal security.

   Be very careful when activating Terminal security for the first time. If done incorrectly, no one will be able to sign on to either MVS or Cisco IOS for S/390.

   Research these sample commands for turning on Terminal security:

   ```
   SETROPTS TERMINAL(READ)
   SETROPTS CLASSACT(TERMINAL) RACLIST(TERMINAL)
   ```

   Issuing the RACF command SETROPTS TERMINAL(NONE) prevents all undefined terminals from signing on to an address space using Terminal security. This can be useful in restricting access to Cisco IOS for S/390 via IP addresses. Undefined IP addresses will not be permitted to sign on to Cisco IOS for S/390.

2. All users that need to access Cisco IOS for S/390 through VTAM logon points must be permitted READ access authority to the VTAM Terminal APPL names (not ACBNAMEs). Currently, there is no mechanism within Cisco IOS for S/390 to map VTAM LU usage to specific user IDs at the VTAM logon points. You do not know which LU will be allocated at these logon points. The LUs used at VTAM logon points within Cisco IOS for S/390 are allocated by ACCPOOL. Do not confuse the LUPOOL capability to map IP address to user IDs with ACCPOOL LU customization.

   SAMP member A03ACCES shows VTAM APPL names beginning with A03VLT. This member is a model to use or modify for local use.

   The RACF security administrator can use the RDEFINE TERMINAL... and the PERMIT RACF commands to designate which users can access Cisco IOS for S/390 via VTAM using the A03VLT*xx* VTAM APPLs.

   If the RACF system administrator decides to allow access to Cisco IOS for S/390 via the VTAM interfaces only to groups SYS1 and ENG, the terminals can be protected as defined in the SAMP member A03ACCES with the following RACF commands:

   ```
   RDEFINE TERMINAL A03VLT* UACC(NONE)
   PERMIT A03VLT* CLASS(TERMINAL) ID(SYS1,ENG) ACCESS(READ)
   ```

The RACF security administrator should check with both the Cisco IOS for S/390 and VTAM systems programmers to identify which VTAM LUs are being used by the site for access within Cisco IOS for S/390.

3. All users who want to sign on to Cisco IOS for S/390 must have READ access authority to the Cisco IOS for S/390 IP address(es) as specified on the IP address parameter for every NETWORK statement in the TCPCFGxx member.

   A sample NETWORK statement in member TCPCFG*xx* may begin like this:

```
NETWORK IPADDRESS(138.42.224.15)
```

   The security system accepts terminal IDs only in hexadecimal form, so the above IP address must be converted. IP address 138.42.224.15 would use a terminal ID of 8A2AE00F (where 138 = 8A, 42 = 2A, 224 = E0, and 15 = 0F).

   To allow all users at a site to sign on to Cisco IOS for S/390 for a default IP address of 138.42.224.15 with terminal 8A2AE00F, issue the following command:

```
   RDEFINE TERMINAL 8A2AE00F UACC(READ)
```

   If you replace UACC(READ) on the above command with UACC(NONE), the RACF security administrator must use the RACF PERMIT command to allow READ access to all users or groups that need to sign on to Cisco IOS for S/390.

4. Individual users must be permitted to use their own IP addresses. If local user USER01 comes off the local network from host 138.42.224.250, this user must be permitted access to this IP address via terminal 8A2AE0FA. This can be done with the following commands:

```
   RDEFINE TERMINAL 8A2AE0FA UACC(NONE)
   PERMIT 8A2AE0FA CLASS(TERMINAL) ID(USER01) ACCESS(READ)
```

   A RACF administrator could allow everyone on his local network (138.42.224) access to Cisco IOS for S/390 with the following RACF command:

```
   RDEFINE TERMINAL 8A2AE0* UACC(READ)
```

5. Configure Cisco IOS for S/390 to place the terminal ID on all security parameter lists passed to RACF for all sign-on attempts to Cisco IOS for S/390. If you use the TERMID option on the XSEC parameter of the SECURITY statement in the IJTCFG*xx* member, this happens automatically. By default, Cisco IOS for S/390 does not place the terminal ID on any sign-on call.

   To activate passing terminal IDs on the security parameter list to RACF for an active Cisco IOS for S/390 address space, issue the following command under ACTEST:

```
   XSEC TERMID ON
```

   You can deactivate passing terminal IDs on the security parameter list to RACF for an active Cisco IOS for S/390 address space by issuing the following command under ACTEST:

```
   XSEC TERMID OFF
```

6. To enable sign-on checking for Telnet users, add the CPASSWORD option to the Telnet related SERVICE statement(s) in the APPCFG*xx* member for Telnet ports (typically, 23,1023).

⚠ **Caution** Activate Terminal security checking only after all RACF customization for Cisco IOS for S/390 has been completed and the RACLIST profiles have been refreshed (SETROPTS REFRESH TERMINAL). RACF Terminal security can prevent sign-on to MVS, as well as Cisco IOS for S/390, if the customization is performed incorrectly.