

Remote Access - Verify I Con-nect System File

This chapter covers the following topics:

- Description
 - Procedure
 - Batch Example
-

Description

Program

B74051

Function

Verify remote access authorization records in Con-nect against the central directory file. If a discrepancy occurs, data in the central directory are assumed to be correct and the Con-nect system file is updated.

If you want to display the discrepancies between the Con-nect system file and the central directory's authorization tables, mark both fields. In this case, the records are not modified.

Online Input Screen

```
7:37 AM          * * * C O N - N E C T 3 * * *          14.Feb.94
Cabinet LS      Remote Cabinet Access          B74051

Recover Con-nect System File

Mark _ with any character
to start recover procedure
for node Node-Name

Mark _ with any character
to run this function
with mode = 'report-only'

Enter-PF1---PF2---PF3---PF4---PF5---PF6---PF7---PF8---PF9---PF10--PF11--PF12---
Menu Quit
Complete the information above and press ENTER to continue
```

Utility Parameters

Parameter	Format	Description
Start Recover	A1	
Report Only	A1	

Procedure

This utility verifies and modifies only the records applicable to your Con-nect node.

Processing Sequence

When this utility is run, the following steps are performed.

1. Check table of users - Central Directory

All authorized users in the central directory's authorization tables are verified against the Con-nect system file. If a user is not authorized in Con-nect, authorization for the user is restored. However, if a user is not defined in Con-nect, authorization for that user is deleted from the authorization tables.

2. Check table of users - Con-nect

All authorized users defined in the Con-nect system file are verified against the central directory's authorization tables. If a record for a user is not present in the authorization tables, authorization for that user is deleted from Con-nect.

3. Check table of cabinets - Central Directory

All authorized public cabinets defined to the central directory's authorization tables are verified against the Con-nect system file. If a cabinet is not authorized in Con-nect, authorization for the cabinet is restored. However, if a cabinet is not defined in Con-nect, authorization for that cabinet is deleted from the authorization tables.

4. Check table of cabinets - Con-nect

All authorized public cabinets defined in the Con-nect system file are verified against the central directory's authorization tables. If a record for a cabinet is not present in the authorization tables, authorization for that cabinet is deleted in Con-nect.

5. Check table of members - Central Directory

All authorized memberships defined to the central directory are verified against the Con-nect system file. The following occurs:

- If a shared cabinet is not defined in Con-nect, authorization for the cabinet is deleted from the central directory.
- If an external membership is not authorized in Con-nect and the external user is defined in the authorization table (as an authorized user on his local Con-nect), authorization for the membership is restored in Con-nect.
- If an external membership is not authorized in Con-nect and the external user is not defined in the authorization tables (as an authorized user on his local Con-nect), authorization for the external user is deleted from the authorization tables.

6. Check table of members - Con-nect

All authorized memberships defined in the Con-nect system file are verified against the central directory's authorization tables. If a record for a membership is not present in the authorization tables, authorization for that membership is deleted from Con-nect.

Batch Example

Verify remote access authorization records in Con-nect against the central directory's authorization tables. If a discrepancy occurs, data in the central directory are assumed to be correct and the Con-nect system file is to be updated. This would be coded as follows:

```
LOGON SYSCNT2B  
MENU  
B74051 X,  
FIN
```