MITEL NETWORKS

Technical | Service Bulletin

| | |
|---|---|
| NUMBER: | 09-5127-0021 Rev 2 |
| ISSUE: | Rev 2 |
| RELEASED: | April 2009 |
| PRODUCT(S) AFFECTED: | Mitel Networks™ 3300 Integrated Communications Platform (ICP) |
| SEVERITY: | ☒ Critical (Service Affecting)<br>☐ Non-Critical (Information Only) |
| AUDIENCE: | Customer Service personnel involved in programming end-points and trunks for the Mitel Networks 3300 ICP. |
| SUMMARY | Dealers and site managers are hereby warned that fraudulent use of the 3300 ICP system is possible.<br><br>Examples provided in this Technical Service Bulletin (TSB) show how to use CDE to minimize toll fraud by internal users and external callers.<br><br>The TSB highlights areas, which, if not programmed correctly, can allow unauthorised toll access.<br><br>Mitel disclaims any express or implied warranty that its equipment is technically immune from or prevents fraudulent intrusion into, or unauthorized use of, its telecommunications system, including its interconnection to the long distance network. |

## Using CDE to Prevent Toll Fraud on the 3300 ICP

Mitel strongly recommends that PBX owners and/or the Service personnel, program an appropriate COR to all system ports to control external dialing capabilities (i.e. Station Ports, Voice Mail Ports, DISA Trunks and all Dial-In-Trunks). This approach has proven effective in implementing a system that minimizes the occurrence of toll fraud.

The 3300 ICP ESM forms are designed to offer a very flexible and highly customized programming structure.

ESM must be carefully programmed to prevent users from defeating your toll restriction plan.

**Types of Telephone Fraud**

**External**

All 3300 ICP systems with any combination of Direct Inward System Access (DISA) and/or Dial-in Trunks integrated with Auto Attendant or peripheral interfaced Auto Attendant/Voicemail and RAD groups are susceptible to being "hacked into" by external callers. Precautions must be taken during CDE entry to minimise the possibility of system abuse.

**Internal**

Company employees could abuse telephone privileges. Some areas of concern are EXTERNAL CALL FORWARD, TRUNK-TO-TRUNK CONNECTION WITHOUT THIRD PARTY, and 1-800 AND 1-900 NUMBERs for North America, and other toll free numbers ie 1300 .

**Document Description**

This document covers the above functionality,

ARS programming using class of restriction (COR) group assignments is the only proper way to minimise toll fraud; therefore, ARS will be discussed extensively in this TSB.

**ARS Digit String**

Automatic route selection (ARS) digit-string entries are the heart of every toll-control plan and should be analysed very closely.

Programmers should also look at “services” offered by the carrier, such as per call CLI blocking, Call Forwarding, etc, where users dial a predefined digit string, and get dial tone returned. Please check with carrier for what features are available, and test accordingly

It is extremely important that the programmer clearly understands which digit-string entries the system will find to be the closest match to the digit string dialled. What ARS finds to be the closest match will not always be the same digit-string entry that the programmer intended the dialled digits to match.

Consider the following example: A programmer expects that users dialling Ars Leading digit 9 followed by “901” would access route 2 only and that those dialling “90 would access route 1. Similarly, one might expect someone dialling “1212xxxxxxx would access route 2, and all other 1x would follow route 1.

| Leading Digits | Second Dial Tone | COR Group Number |
|---|---|---|
| 9 | YES | |

| Digits Dialled | Number of Digits to Follow | Termination Type | Termination Number |
|---|---|---|---|
| 90 | UNKNOWN | Route 1 | |
| 901 | UNKNOWN | Route 2 | |
| 1 | UNKNOWN | Route 1 | |
| 12 | UNKNOWN | Route 2 | |

Generally, the programming works; however, there is a small chance that users may be able to beat the system by making a “901” call via route 1, with no SMDR record. To defraud the system, users dial “90,” wait for the inter-digit timer to expire, and then dial “1.” After the inter-digit time-out, the closest match to the digit string dialled is “90.” The system then dials “0” via route 1 and connects the station directly to the CO trunk with no further Toll Control. Digits dialled after the inter-digit time-out will not be captured in the SMDR. Same applies for the example of user dialling 1212, if they just dial 1 and wait the system will dial the 1 with no further toll checking

To prevent the system from accessing the undesired route, the entry of the “Digits Dialled” should be programmed to avoid non-unique match or ambiguous entries, as shown below. “9-0” calls (with no further digits dialled) will be blocked because there is no match in the “Digits Dialled “ field after the inter-digit time-out. Same with digit”1”

| Leading Digits | Second Dial Tone | COR Group Number |
|---|---|---|
| 9 | YES | |

| Digits Dialled | Number of Digits to Follow | Termination Type | Termination Number |
|---|---|---|---|
| 901 | UNKNOWN | Route 2 | |
| 902 | UNKNOWN | Route 1 | |
| 903 | UNKNOWN | Route 1 | |
| 904 | UNKNOWN | Route 1 | |
| 905 | UNKNOWN | Route 1 | |
| 906 | UNKNOWN | Route 1 | |
| 907 | UNKNOWN | Route 1 | |
| 908 | UNKNOWN | Route 1 | |
| 909 | UNKNOWN | Route 1 | |
| 900 | UNKNOWN | Route 1 | |
| 1201 | UNKNOWN | Route 1 | |
| 1212 | UNKNOWN | Route 2 | |

**COR Group Assignment**

The COR group assignment form is used to gather COR numbers into groups to enforce toll restriction. Do not confuse the COR group with the COR number. A COR number is assigned to individual stations and trunks in the Station Service Assignment and Trunk Service Assignment fields, respectively. A COR *group* number (not a COR number) is assigned to the Route Assignment form of the ARS programming.

The following examples show how to restrict internal, local, and long distance calls, using COR.

**Note:** The examples provided below do not, in any way, imply that ARS should be programmed this way.

**Example 1: No Restriction from the Leading Digit "9"**

Not all stations are COR-restricted from the leading digit "9." The entry "0-9" is intended to pick up all local and long-distance calls, leaving the 3300 ICP customers specified above wide open to all long-distance calls and, potentially, to a very high telephone bill. The following should *not* be a typical ARS program because it does not provide any toll-control protection.

| Leading Digits | Second Dial Tone | COR Group Number |
|---|---|---|
| 9 | YES | |

| Digits Dialled | Number of Digits to Follow | Termination Type | Termination Number |
|---|---|---|---|
| 0 | UNKNOWN | Route 1 | |
| 1 | UNKNOWN | Route 1 | |
| 2 | UNKNOWN | Route 1 | |
| 3 | UNKNOWN | Route 1 | |
| 4 | UNKNOWN | Route 1 | |
| 5 | UNKNOWN | Route 1 | |
| 6 | UNKNOWN | Route 1 | |
| 7 | UNKNOWN | Route 1 | |
| 8 | UNKNOWN | Route 1 | |
| 9 | UNKNOWN | Route 1 | |

**Example 2: Internal Restriction**

All stations and trunks with COR defined in COR group 2 will be restricted from the leading digit "9." This way we can restrict certain stations and trunks from accessing the local and long-distance network. A typical application for this ARS program is on a lobby phone that has numerous users.

| Leading Digits | Second Dial Tone | COR Group Number |
|---|---|---|
| 9 | NO | 2 |

| Digits Dialled | Number of Digits to Follow | Termination Type | Termination Number |
|---|---|---|---|
| 0 | UNKNOWN | Route 1 | |
| 1 | UNKNOWN | Route 1 | |
| 2 | UNKNOWN | Route 1 | |
| 3 | UNKNOWN | Route 1 | |
| 4 | UNKNOWN | Route 1 | |
| 5 | UNKNOWN | Route 1 | |
| 6 | UNKNOWN | Route 1 | |
| 7 | UNKNOWN | Route 1 | |
| 8 | UNKNOWN | Route 1 | |
| 9 | UNKNOWN | Route 1 | |

COR Group Assignment:

| Number | Classes of Restriction for Group |
|---|---|
| 1 | |
| 2 | 3, 4, 5 |
| 3 | |
| 4 | 6-64 |
| 5 (and up) | |

Station Service Assignment

| Directory Number | Intercept Number | Class of Service | | | Class of Restrictions | | | Default Account Code |
|---|---|---|---|---|---|---|---|---|
| | | Day | Night1 | Night2 | Day | Night1 | Night2 | |
| 1000 | 1 | 1 | 1 | 1 | 3 | 3 | 3 | |
| 1001 | 1 | 1 | 1 | 1 | 3 | 3 | 3 | |
| 1002 | 1 | 1 | 1 | 1 | 5 | 5 | 5 | |
| 1003 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | |
| 1004 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | |

**NOTE**: The selection of “Alternate” second dial tone is *not* designed for N.A. operation.

**Example 3: Long-distance Call Restriction**

All stations with COR numbers 3, 4 or 5 in (COR) group 2 will be restricted from long-distance “0” and “1” calls. In this set-up, all extensions have access to the local network, but only selective extensions will have access to the toll network.

Class of Restriction Group Assignment

| Number | Classes of Restriction for Group |
|---|---|
| 1 | |
| 2 | 3,4,5 |
| 3 | |
| 4 | 6-64 |
| 5 (and up) | |

**Note**: The COR number is assigned in Station and Trunk Service Assignment

In the following form, the directory numbers 1000,1001, and 1002 have been COR-restricted in day and night service.

Station Service Assignment

| Directory Number | Intercept Number | Class of Service | | | Class of Restrictions | | | Default Account Code |
|---|---|---|---|---|---|---|---|---|
| | | Day | Night1 | Night2 | Day | Night1 | Night2 | |
| 1000 | 1 | 1 | 1 | 1 | 3 | 3 | 3 | |
| 1001 | 1 | 1 | 1 | 1 | 3 | 3 | 3 | |
| 1002 | 1 | 1 | 1 | 1 | 5 | 5 | 5 | |
| 1003 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | |
| 1004 (and up) | 1 | 1 | 1 | 1 | 1 | 1 | 1 | |

In the Route Assignment form, the route number that is to be COR-restricted should be assigned a **COR *group number* that contains the COR *number***.

Route Assignment

| Route Number | Trunk Group Number | COR Group Number | Digit Modification Number | Digits Before Outpulsing | XNET Trunk Group Number | Route Type | Compression |
|---|---|---|---|---|---|---|---|
| 1 | 1 | 1 | 1 | | | | |
| 2 | 1 | 2 | 1 | | | | |
| 3 | 1 | 3 | 1 | | | | |
| 4 (and up) | | | | | | | |

In the Leading Digits Assignment form, the system is programmed so that leading digits “0” and “1” take route 2, forcing Toll Control on any member in COR group 2 to access route 2.

| Leading Digits | Second Dial Tone | COR Group Number |
|---|---|---|
| 9 | NO | 4 |

| Digits Dialled | Number of Digits to Follow | Termination Type | Termination Number |
|---|---|---|---|
| 0 | UNKNOWN | Route 2 | |
| 1 | UNKNOWN | Route 2 | |
| 2 | UNKNOWN | Route 1 | |
| 3 | UNKNOWN | Route 1 | |
| 4 | UNKNOWN | Route 1 | |
| 5 (and up) | UNKNOWN | Route x | |

**Example 4: Maximum Digits**

To further secure the restriction level shown in Example 3, we can limit the maximum digits able to be dialled on a trunk by a station. These limits are defined below. All stations with COR numbers 3, 4, and 5 cannot dial more than 10 digits against the COR (including leading digit "9").

With this level of security, whether stations (for example, COR 2 and 3) are COR-restricted from accessing route 2 or not, they will be prevented from making long-distance calls (dialling more than 10 digits).

**Note:** This example does not apply to areas in which users must dial an area code to make a local call.

Maximum Digits

| Class of Restriction | Number of Digits Allowed |
|---|---|
| 1 | Unlimited |
| 2 | 10 |
| 3 | 10 |
| 4 | Unlimited |
| 5 (and up) | Unlimited |

**Trunk Class of Restriction**

All dial-in-trunks including DISA, TIE, DID and ISDN should be considered for COR restriction. If these dial-in-trunks are accessible by external users then these trunks should be treated like an extension and should only be allowed certain privileges.

If we follow this rule then the trunk service assignment would have the following set up:

Based on the above ARS programming, once COR restriction is applied to trunk service number 1 and 2, any trunk assigned to either service number will be restricted from placing long-distance calls beginning with "0" or "1." If possible, the programmer should also limit the maximum number of digits to be dialled on another trunk, as shown in the preceding table.

Trunk Service Assignment:

| | |
|---|---|
| Trunk service assignment | 1 |
| Release Link trunk | |
| Class of Service | 1 |
| Class of Restriction | 3 |
| Baud Rate | |
| Intercept Number | 1 |
| Non-Dial-in Trunk Answer Point: Day | 300 |
| Non-Dial-in Trunk Answer Point: Night1 | 300 |
| Non-Dial-in Trunk Answer Point: Night2 | 300 |
| Dial Trunks Incoming Digit Modification: Absorb | |
| Dial Trunks Incoming Digit Modification: Insert | |
| Trunk Label | DISA |
| Trunk service assignment | 2 |
| Release Link trunk | |
| Class of Service | 1 |
| Class of Restriction | 3 |
| Baud Rate | |
| Intercept Number | 1 |
| Non-Dial-in Trunk Answer Point: Day | |
| Non-Dial-in Trunk Answer Point: Night1 | |
| Non-Dial-in Trunk Answer Point: Night2 | |
| Dial Trunks Incoming Digit Modification: Absorb | 0 |
| Dial Trunks Incoming Digit Modification: Insert | |
| Trunk Label | TIE/ISDN |

| | |
|---|---|
| Trunk service assignment | 3 |
| Release Link trunk | |
| Class of Service | 1 |
| Class of Restriction | 1 |
| Baud Rate | |
| Intercept Number | 1 |
| Non-Dial-in Trunk Answer Point: Day | |
| Non-Dial-in Trunk Answer Point: Night1 | |
| Non-Dial-in Trunk Answer Point: Night2 | |
| Dial Trunks Incoming Digit Modification: Absorb | 0 |
| Dial Trunks Incoming Digit Modification: Insert | |
| Trunk Label | |

**DISA and Dial-in Trunks**

DISA presents the greatest potential for abuse by external callers. Two levels of security can be provided by restricting the COR and class of service (COS) of the DISA trunk from making external calls unless a Verified Account Code is dialled after the DISA access code. The Verified Account Code changes the COR and COS of the normally-restricted DISA trunk, allowing external access for legitimate users. The use of 12-digit account codes results in the greatest number of possible account-code combinations and presents the greatest deterrent for system abuse.

All Dial-in Trunks must be COR restricted from directly placing external calls. In most applications, only a limited number of digit strings will ever be dialled inward on E&M or DID trunks, but it is important to be aware that these trunks can directly access ARS.

**Risks with DISA and Dial-in Trunks**

It is very important to note that if the system is programmed to allow users to call into the switch and then call back out, no matter how complex the dialling process is, maximum protection from fraudulent calls cannot be achieved without the implementation of COR, COS, and Independent Account Codes against the incoming trunk, with the provision that there can be no guarantees when dealing with fraudulent behaviour.

If DISA is only used to call internal extensions, then Interconnect Restrict the DISA trunk from all outgoing trunks. When enabling COS Options, caution should be given to INDIVIDUAL TRUNK ACCESS and INDEPENDENT ACCOUNT CODES. COR assignments must be enabled for Dial-in Trunks. Forced Account codes must be used wherever possible and the maximum account-code digit-string length should be used. The maximum number of digits dialled, which is defined by COR, should also be carefully considered.

Trunk-protocol errors can be encountered during “release state” initiated by the PBX, resulting in toll fraud. These errors occur when the internal PBX port hangs up, but the external party stays off-hook longer than the Release Acknowledge Timer (as programmed in the Trunk Circuit Descriptor on the PBX) and shorter than the release timer of the Central Office equipment. The PBX treats this as a new call, opening the door for “hackers.”

**Important:** The appropriate COR and COS must be programmed against the incoming trunks as described in this document in order to minimise Toll Fraud. In addition, the trunk circuit descriptor can be adjusted for proper trunk protocol handling with the Telco by increasing the Release Acknowledge Timer to a value that exceeds that of the release timer of the Central Office Equipment.

**Miscellaneous Assignment Form**

In the 3300 ICP system, the DISA directory number is programmed in the MISCELLANEOUS ASSIGNMENT FORM. There are two types of DISA assignments: DISA without account codes and DISA with forced account codes.

**DISA Directory Number**

If the installer programs the section DISA DIRECTORY NUMBER, then anybody dialling this number will receive DISA dial tone and can access any ARS without dialling an account code. This can be very dangerous if this is the trunk answer point and the trunk is not COR restricted.

Let’s assume that the DISA trunk is COR-restricted and cannot access any toll trunks, and the DISA trunk is not forced to dial account codes at this point. If legitimate users access the DISA trunk, they would dial the feature access code for the account code (which can be up to 4 digits in length and can include ***** and **#)**, and then the independent account code (which can be up to 12 digits in length). When the proper account code is entered, it changes the COR and allows a toll call. Thus, an authorised caller is required to dial up to 16 digits, including a feature access code, before making a toll call. This does not prevent hackers from breaking in, but it makes it more difficult.

**Note:** The DISA trunk will only allow three attempts at the correct password. After that, the user will be restricted from dialling any more digits until the next time the trunk is accessed.

**DISA Forced Account Code**

If the installer programs the section DISA FORCED ACCOUNT CODE DIRECTORY NUMBER, the system will force an account code, but the feature access code for the account code is not required. This account code would be programmed in the INDEPENDENT ACCOUNT CODE DEFINITION form. The longer the account code is, the more difficult it is to break in. In this form, the system can also control the COS and COR of the DISA trunk. The COS of both the DISA trunk and the INDEPENDENT ACCOUNT CODE DEFINITION should have limited options; for example, it should not have the option of INDIVIDUAL TRUNK ACCESS. If this option is enabled, the DISA trunk will be able to access trunks and override all toll restrictions. It is very important that caution be exercised when assigning a COS to a DISA trunk and to an INDEPENDENT ACCOUNT CODE.

If a customer wishes to make it more difficult for the DISA trunk to access the ARS network, then the COS for that account code could force a user to enter yet another account code, thus adding more digits for the user to dial.

**Example: Independent Account Code**

A user accesses the DISA and receives dial tone. The system is set up for a 12-digit account code. The user dials 057912543349 and receives a second dial tone. The COS in the INDEPENDENT ACCOUNT CODE form forces the user to enter a second account code, so the user must now dial the same 12-digit account code or a different code. This creates a total of 24 digits that the DISA user must dial to access the toll network.

**Note:** It is not recommended to use the exact account code shown in this example.

**Auto Attendant**

The 3300 ICP Auto-Attendant PBX feature is very similar to DISA, in its operation. The only difference between DISA and the auto attendant is that the caller listens to a recorded announcement instead of a dial tone. This means that if the caller is on a Dial-in Trunk and is not COR-restricted, the caller can dial ARS leading digits and place an outgoing call. Even a COR-restricted trunk can dial a verified account code that could allow access to external trunks. For this reason, all sites with auto attendant, dial-in trunks, and non-dial-in trunks should be Toll Controlled, with limited COS options and a 12-digit account code to increase the level of difficulty encountered by unauthorised callers attempting to place external calls.

If the 3300 ICP auto attendant is not to permit external calls, use Interconnect Restriction to control it. Consideration should also be given to limiting the maximum digits dialled (as defined by the COR number) to enhance the security.

**Any Type of Interfaced Voice Mail/Auto Attendant (e.g., COV/ONS/E&M VM/AA)**

Proper consideration should be made for Toll Control of COV and ONS VM/AA ports. Many peripheral systems will simply perform a blind transfer to any digit sequence entered by the incoming trunk. Some ONS VM/AA systems use station ports looped back onto loop-start trunks for message-sending set-ups. All station ports used in loop-backs should be properly Toll Controlled, only have the minimum required COS options, and be COR restricted. For programming considerations, see Page 9, “Example 4: Maximum Digits,” and Pages 11-13, “DISA and Dial-in Trunks” to “Auto Attendant.” These devices can also be toll-controlled by using the Interconnect Restriction table.

Voicemail systems that allow users to set up Personal Contacts or set up their mailbox for Message forwarding, or use of single digit trees to forward to external numbers should be taken into account. When a user has ability to change the number from their own mailbox, you should set necessary restrictions to ensure to limit possibility of hacker changing number to an alternate destination fully unrestricted.

**Networking**

**Notes:**

- Networking trunks can also be XNET, QSIG, ISDN, IP-trunking or SIP. . (“Networking trunks” are referred to in this section only by MSDN/MSAN as an example.)

- If the public-to-public network option is disabled in the COS of a T1 trunk, it will have no effect unless “Public Trunk” is enabled in the trunk COS. (The T1 trunk is not considered a public trunk unless “Public Trunk” is enabled in the COS of the trunk.)

3300 ICP systems can be networked together using the MSDN/MSAN feature. To users, the network looks like one huge PABX. Proper consideration should be made for the remote PABXs to ensure that Toll Control is consistent in all switches. This requires that MSDN/MSAN trunks have the proper COS/COR enabled. If auto attendant and DISA are being used in the remote switches, see Pages 11-13, “DISA and Dial-in Trunks” to “Auto Attendant,” for programming considerations in all switches. There are other COS options that must be considered when using MSDN/MSAN and ISDN trunks: PUBLIC NETWORK TO PUBLIC NETWORK and PUBLIC NETWORK ACCESS VIA DPNSS. These COS options are enabled in the extension COS and the trunk COS of the Host PABX. The incoming MSDN/MSAN trunks are COR-restricted, based on what is enabled in the TRUNKS SERVICE ASSIGNMENT form and on what the site requirements are.

**Note:** ISDN trunks are treated as part of the DPNSS access.

In situations where AAN is not used, an outgoing call across MSDN uses the COS and COR assigned to the MSDN trunk on the receiving side. In a networking situation, every outgoing call from a PBX has the same COS and COR at the receiving node.

The following scenario depicts a situation in which toll fraud could occur:

In the example below, Extension 5000 is COR-restricted from dialling “9” plus any number; however, if the station is intercepted to the RAD group or dials the RAD group directly on PBX B, the COR of the MSDN trunk on PBX B is used.

If the MSDN on PBX B is not COR-restricted to dial “9” plus any number, then once extension 5000 is answered by RAD group 6000, Extension 5000 is free to dial any number.

PBX A Ext. 5000-------→MSDN-----→PBX B--------→RAD Group 6000 (Pilot)

Intercepted to 6000 6001} Member

Or dials 6000 Directly 6002} Member

***Caution: COR-restricting the RAD members does not prevent the caller from dialing out unless the call is made from the RAD extension itself.**

**Possible solutions:**

1. The most obvious solution is to disallow the calling party from PBX A from dialing or from being intercepted to a RAD group on PBX B.

2. The AAN feature package enhances the features of the network by providing Travelling Class Marks, which provide users with a different COS and COR at the receiving node in the network. This is done by transmitting account code information in the digit stream and by assigning account code values for specific COS and COR values in the receiving nodes Independent Account Code Assignment form.

3. If you re-route to a RAD group, the DTMF receiver is dropped, and you cannot dial any digits. As a result, one possible solution to intercept to the RAD group on PBX B is to intercept to an extension on PBX B that is always re-routed to the RAD group.

**Supplementary information on RAD’s Toll Fraud security**

This section will provide detailed description on RAD security enhancement. Prior to Rel. 9.0 UR2, RAD security had been dependent on programming choices, which is based on the implementation of COR and interconnect-restriction.

In Rel. 9.0 UR2 or higher, the RAD security is enhanced. The RAD device is securely locked down; Callers who do not terminate on RADs directly will not have dialing capabilities; while callers who terminate on RADs directly are restricted to dial only local extensions, remote directory numbers and system speed call number. See Table 1 for RAD security summary.

The enhanced RAD security will prevent potential Toll Fraud abuse via RAD devices. Please bear in mind that toll fraud security is not restricted to only RAD devices. One should review the overall system security such as physical access security, remote access security, ARS programming and the like. For detailed information on potential Toll Fraud Control and Abuse, please consult 3300 on-line help/ edocs *(contents...maintaining the system...procedure...preventing toll fraud...Use CDE to prevent Toll Fraud on 3300 ICP)*

**Definition of RAD Device**

RAD device = any station / Hunt group that has RAD and/or Advanced RAD enabled in COS.

**Summary of RAD security at a glance**

Originator Categories

I> Trunk = T1, E1 Pri, LS, SIP trunk, T1 Tie trunk

II>Internal = local station, RDN (Remote directory number)

Networked DN = remote DN but not programmed in RDN (i.e. not cluster)

**Networked DN is routed via normal ARS and will be blocked by RAD security

**Table 1 summarizes the change in RAD security**

| Originator | 1st Answer point - direct | 2nd routing condition by 1st answer point | Permission to dial by originator on RAD device |
|---|---|---|---|
| Trunk | RAD | N/A<br>i.e. no other routing to follow. | i>Local station, RDN, system speed call *(note1)<br>ii>No ARS (including networked DN), no FAC |
| Trunk | Local Station or<br>Remote Station | Station transfers to RAD locally or via IP / MSDN trunk<br>Station reroutes to RAD locally or via IP / MSDN trunk<br>Station forwards to RAD locally or via IP / MSDN trunk<br>Station intercepts to RAD locally or via IP / MSDN trunk | Dead end<br>-No DTMF receiver is allocated in this scenario<br>-No dialing |
| Internal | RAD | N/A | No restriction on dialing;<br>Follow standard toll fraud control |
| Internal | Local Station or<br>Remote station | Under any routing conditions to RAD | No restriction on dialing;<br>Follow standard toll fraud control. |

**Internal Fraud**

It is very important that only employees who require toll access be given telephone privileges. For example, a lobby telephone would be denied toll access unless it is authorised through attendants.

COS options should be controlled with

- "Individual Trunk Access," which will bypass all ARS and COR restrictions
- "Public Network to Public Network Connection Allowed" to allow trunks to be connected together without a third party
- Call Forwarding (External Destination) to allow extension users to forward their telephone to external trunks.

800-numbers are traditionally free calls; however, some Central Offices can allow the reversal of 800-charges. Therefore, if necessary, programmers can designate 800-calls as toll calls for the company.

900-numbers and any information service calls should be COR-restricted from all users except those who require access for their job function.

Station Message Detailed Recording (SMDR) can be used to track internal users and control their calls. This tracking is a deterrent for toll abuse by internal callers.

**System Speed Call**

It is important to note that in the 3300 ICP, Speed Call be subject to Toll Control. Access to system speed calls should be controlled through the SYSTEM SPEED CALL ASSIGNMENT form, in which Toll Control can be enabled.

It is also important to note that Speed Call via the keys located on a set will be subject to Toll Control *only if* the set is COR restricted.

**Emergency Services Access**

In most applications, users are allowed to access 911 or other emergency access numbers without restriction; however, the DISA-trunk automated attendant (which allows the transfer to an external call) should be considered to be COR-restricted from dialling 911 to avoid any possibility of abuse from this source.

**Passwords**

In the User Authorisation Profiles in ESM, you need to change the default username and password for the System User Profile login ID. Ensure that any other user profile login IDs that are created, only have the required access level.

## Preventing toll fraud through Embedded Messaging on the 3300 ICP

. Mitel systems allow the administrator to set the following restrictions on the Embedded voice mail related passcodes:

- Passcode length – the default is 4 numeric characters, but can be 3-6 characters long.
- Mailbox lockout capability, after three failed attempts. (Release 9.0 UR1 and later) Furthermore, Mitel systems require the end user to change the default passcode on first login.

**Toll fraud attacks can be prevented by following the security recommendations described below:**

- Use passcodes with a length of 6 characters to decrease vulnerability to brute force attacks.
- Use passcodes that are not easy to guess (avoid passcodes like 123456, 987654 or 444444).
- Ensure that administrator and user mailbox passcodes are changed frequently based on the organization's security policies.
- Ensure that only appropriate personnel have mailbox create permissions to prevent toll fraud attacks originating from within the network.
- Use strong passwords (at least 8 characters with numbers and special characters) for all GUI-based administration/management interfaces.
- On creating a new mailbox, it is recommended that the administrator immediately change the default passcode, and provide this new passcode to the user. This will prevent toll fraud attacks occurring during the interval from creating a mailbox and the user changing the default passcode.
- Use appropriate call routing restriction rules to control outbound calling.
- If Recorded Announcement Devices (RAD's) are implemented on the Embedded Messenger, ensure appropriate security measures are in place to prevent unauthorized Dial through. Refer to Rad section of this document for additional information

**External Voicemail systems.**

External voice mail systems connected directly to a modem should also be connected to a surveillance device. Also, most voice mail systems require a password before access; therefore, ensure that this password is complicated. It is also very important to change all passwords periodically, especially when anyone with system access quits the job from either the site or the service provider.

**General Guidelines for implementing ESM / DISA Trunk Access Security**

With all security features in place, Customers become responsible for their PBX security and are expected to do the following when the PBX is installed. They are also reminded that the username and password for SYSTEM profile in ESM should be restricted to only reliable, responsible personnel, at the owner's discretion. As a general rule of thumb, System Level access should not be assigned to routine service personnel.

1. Create the necessary user profiles.

   When installing the 3300 ICP login as System with correct username and password in ESM, create the required profiles needed for the 3300 ICP. Remember to change these on a regular basis to help keep the system as secure as possible.

2. Make and keep a backup copy of new usernames and passwords.

   Whenever usernames and passwords are changed, make sure that the updated usernames and passwords are recorded and saved in a secure area. These records should be accessible to any service personnel, if needed.

3. Backup your database.

   Backup the database regularly and whenever there have been changes made to it.