

# **TEMENOS T24**

# Security Management System

**User Guide** 

No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of TEMENOS Holdings NV.

Copyright 2005 TEMENOS Holdings NV. All rights reserved.



### **Table of Contents**

Introduction	4
Application Overview	4
ARC-IB SMS and External users	4
USER	5
Identification	5
Permitted Times Of Use	6
Permitted Customers and Accounts for external users	8
USER.EXTERNAL.FIELDS	9
Permitted Activity1	0
All Programs – All Functions 1	4
ENQUIRY.SELECT1	5
ENQUIRY 1	5
Activity Logging1	6
PASSWORD VALIDATION	8
Re-Enabling User Profiles1	9
Activating programs at SIGN In / SIGN Out2	20
Setting a user with a new password2	21
Setting a user with a new random password2	21
Logging in based on days of a week2	25
Defining USER.SMS.GROUP 2	26
Linking USER.SMS.GROUP to USER 2	28
Security Violations	29
Access to T242	29
Restrictions3	30
Maintenance3	30
Times	31
OVERRIDE	32
OVERRIDE CLASS	35
Override Management – Auto Override Processing	38
Introduction3	38
Installation	38
Using Auto Override Processing 4	1
Multi-valued DATE.TIME audit information4	13
User Attributes 4	15
Intelligent Override Processing - The Dispo System	<b>1</b> 7



Introduction	47
OVERRIDE	47
DISPO.PARAMETER	49
DISPO.OFFICER	50
ACCOUNT & CUSTOMER	51
USER	52
Using Intelligent Overrides	53
Adding Comments to Dispo Items	54
Manual Routing	56
Automatic DISPO Routing	57
Pending Status	58
Tracking updates made to Dispo Items	58
Approving Dispo Overrides	58
DISPO.ITEMS,COMMENTS – AUTH.ROUTINE field	59



# Introduction

# **Application Overview**

The Security Management System (SMS.) controls who is allowed to use **T24** when they are allowed to use it and to what parts of the System they can have access. It will detect, stop and record any attempt at unauthorised use of the System. S.M.S. can also, if required, record all activities performed by selected Users.

Details of each authorised User are held in the *USER* file. These details include Sign On name, Password, permitted times of use and what parts of T24 may be accessed. Before being allowed to use **T24** each User must be identified to SMS by their Sign On name and Password, all subsequent activity is then checked against their User details before being permitted. For Internet Banking users, the *IB.USER* file uses the same functionality to provide an equal level of security.

Access to applications within **T24** can be controlled by the name of the application, the function they are allowed to perform, Input, Authorisation etc., and can even be controlled by the data itself. E.g., you can allow someone full functional access to the *ACCOUNT* application except, for staff accounts - where staff accounts are identified by the CATEGORY field in the *ACCOUNT* record.

SMS operates only within **T24** It is the responsibility of the installation security manager to ensure security of access to the network, the operating system and jBase. For example, ftp access to **T24** files should not be allowed.

Due to the manner in which with Windows NT is administered, a security issue has had to be overcome. Since on traditional UNIX systems the 'Sign-on' to **T24** is a two-stage process, first to the server followed by the **T24** system. Although SMS can only work within **T24**, a utility has been developed to allow the initial server login details to be shielded from the user, effectively automatically performing the server login and taking the user directly to the second **T24** sign on screen. This utility can be used by system administrators in conjunction with the **T24** SMS to provide a higher level of system security.

### Important

For ease of implementation, **T24** is delivered with a LOGIN file that allows an exit to a jBase prompt. This should be altered before going live so that the exit is disabled. If the associated question and response is removed ("**START T24 Y/N=**") then the wait and response will have to be removed from the Desktop or T24 Browser login scripts.

# **ARC-IB SMS and External users**

The information on configuring SMS and External users for the ARC-IB (internet banking) applications is provided in in the ARC-IB User Guide as it is part of the inherent usage of ARC-IB.



# USER

For every person who is allowed direct access to **T24** (i.e. by directly keying information into the system, rather than through the Internet Banking Interface), a record must be created on the *USER* file. This contains identification details and specifies precisely which information and facilities are available, the dates and times at which the system may be accessed and other information required for Security Management.

Although explained in more detail later it is important to note that it would be very unusual for every user to have a completely individual profile listing every application and function allowed/disallowed. The more normal practice would be to establish group records for business or departmental privileges and add or remove functionality on the individual user profiles.

But first the basic information and details are shown by usage type.

### Identification

These fields specify for each user a unique Sign On Name, Name, Classification ('External' customer or 'Internal' employee of the bank) and Department. In addition, user preferences such as the language in which messages etc. should be displayed can be specified.

🕘 USER PROF	ILE	- Microsoft Internet Explorer	
	×	📈 💌 💌 🎑 🔽 More Actions	v 🗗 🤺
Base Details			
USER,DETS			
User Name	Sa	nple USER record	
Sign On Name	SA	MPLER	
Classification	INT		
Language	1	English	
Department Code	1	Implementation	
Time Out Minutes	10		
Attempts	5		
Clear Screen	Y		
Amount Format	$\mathbf{e}$		
Validity Function	ons	Reports Logging Dispo Misc	
Password Valid	lity 0	1 NOV 2006 M0601	
Start Date Profile	e C	1 JAN 1985	~
200606 - 1.6/0	0605	01   S.DONEY   Temenos Bank   07-SEF	🧐 Local intranet

#### **Figure 1 Identity details**



### **Permitted Times Of Use**

Details specifying when each User can access the System include Start Date, End Date, Start Time, End Time, the maximum time during which the User may be inactive without being Signed Off automatically. The number of unsuccessful attempts to Sign On allowed before the Password is disabled, the frequency with which the Password must be changed and dates between which the Password should be deactivated.

🛃 USER PROF	ILE - Microsoft Internet Explorer	
	💌 📈 💌 🗊 🦱 💽 More Actions 🔍 🕞	~
Base Details SAMPLE		
USER,DETS		
User Name	Sample USER record	
Sign On Name	SAMPLER	
Classification	INT	
Language	1 English	
Department Code	1 Implementation	
Time Out Minutes	10	
Attempts	5	
Clear Screen	Y	
Amount Format		
Validity Function	ons Reports Logging Dispo Misc	
Password Valid	lity 01 NOV 2006 M0601	
Start Date Profile	e 01 JAN 1985	
End Date Profile	31 DEC 2009	
Start Time.1	08:30	
End Time.1	12:00	
Start Time.2	13:00	
End Time.2	17:30	
Max Sessions	5	
Attributes.1	SUPER.USER	
Allowed Days.1	1	
Day St Time.1.1	08:00	
Day End Time.1.	1 17:00	-
200606 - 1.6/0	J60501   S.DOWEY   Temenos Bank   07-2	

Figure 2 User profile: Permitted times of use

The time specified in the fields START.TIME & END.TIME applies for all days of the week. Different access times for each day of the week can also be set using the fields ALLOWED.DAYS, ST.DAY.TIME & ST.END.TIME



🕘 USER PROFIL	E - Mic	rosoft Internet Explorer 📃 🗖 🔀
Validity SAMPLE		More Actions
Password Validity	*	01 NOV 2006 M0601
Start Date Profile	*	01 JAN 1985
End Date Profile	*	31 DEC 2009
Start Time.1	<b>H-</b> *	0830
End Time.1	=*	1200
Start Time.2	<b>H-</b> *	1300
End Time.2	=*	1730
Passw End Date Deactivation Date Reactivation Date		
Max Sessions		5
Attributes.1	F	SUPER.USER
Allowed Days.1	Ξ	6 🗸
Day St Time.1.1	ÞE	0800
Day End Time.1.1		1700
Allowed Days.2	Ξ	
Day St Time.2.1	ÞE	0900
Day End Time.2.1		1300
🥘 200606 - 1.6/060	)501   S	.DONEY   Temenos Bank   07 🛛 🔄 Local intranet 🛒

# Figure 3 Allowed Days

It should be noted that the days of the week are numbered from 1-7 representing Monday (1) through to Sunday (7).



### Permitted Customers and Accounts for external users

Where a user is classified as 'EXTERNAL' (through the CLASSIFICATION field), it is possible to restrict the *CUSTOMER* and *ACCOUNT* details to which they may be allowed access for specific applications. This may be done through the CUSTOMER and ACCOUNT fields.

With the second sec	🛃 USER PROFILE	- Microsoft Internet Explorer	
User Name       External Client USER record         Sign On Name       EUSER01         Classification       EXT         Language       1       English         Company Code.1       US0010001         Department Code       1       Implementation         Password Validity       01 NOV 2006 M0601         Start Date Profile       01 JAN 1985         End Date Profile       31 DEC 2009         Start Time.1       08:30         End Time.1       12:00         Start Time.2       13:00         End Time.2       23:00         Time Out Minutes       10         Attempts       3         Customer.1       E42781         Account.1.1       E42781         Frank Pemberton USD Curr Acct         Account.1.2       E42787         Frank Pemberton USD Save Acct         Company Restr.1       US0010001         Application.1       S         Company Restr.2       US0010001	USER EXTERNAL1	📈 🕞 🕞 🎑 P More Actions	
Customer.1I 300054Frank PembertonAccount.1.1I 42781Frank Pemberton USD Curr AcctAccount.1.2I 42797Frank Pemberton USD Save AcctCompany Restr.1US0010001Application.1CUSTOMERFunction.1SCompany Restr.2US0010001Application.2FUNDS.TRANSFER	User Name Sign On Name Classification Language Company Code.1 Department Code Password Validity Start Date Profile End Date Profile Start Time.1 End Time.1 Start Time.2 End Time.2 Time Out Minutes Attempts	External Client USER record EUSER01 EXT 1 English US0010001 1 Implementation 01 NOV 2006 M0601 01 JAN 1985 31 DEC 2009 08:30 12:00 13:00 23:00 10 3	
Function.2 S	Customer.1 Account.1.1 Account.1.2 Company Restr.1 Application.1 Function.1 Company Restr.2 Application.2 Function.2	Image: Source	×

Figure 4 User profile for external user

In the above screenshot, the user is able to use the *FUNDS.TRANSFER* application to see transactions involving his *CUSTOMER* and/or *ACCOUNT* details.

In order to enable this functionality, it is important to note that the application *USER.EXTERNAL.FIELDS* also needs to be set up.



#### USER.EXTERNAL.FIELDS

This table will allow the user to specify for each **T24** application, which field number(s) identify a 'Customer' or 'Account' field. This must be set up in order to enable SMS settings established for EXTERNAL type users, to limit the user to only seeing the records where their *ACCOUNT/CUSTOMER* ids appear in the field number(s) defined here.

🕘 USER. EXTER	NAL.F	TELD - Microsoft Internet Explorer 📃 🗖 📔	R
USER.EXTERN US-001-0001	X VAL.FI emenos	A Core Actions Core Actions	~
Application.1	<b>HH</b> *	CUSTOMER	
Customer Fd.1.1	DE	0	_
Account Fd.1.1	ÞF		=
Application.2	<del>!</del>	ACCOUNT	
Customer Fd.2.1	DF	1	
Account Fd.2.1	DF	0	
Application.3	<b>H-</b> *	FUNDS.TRANSFER	
Customer Fd.3.1	ÞF	95	
Customer Fd.3.2	PF	96	
Account Fd.3.1	DF	2	
Account Fd.3.2	D	11	
Anneniste A			
😂 200606 - 1.6/0	60501	S.DONEY   Teme S.DONEY   Teme	

Figure 5 Setting up User external fields

So in the above screenshot an external user, when using the *FUNDS.TRANSFER* application, would only be able to view those contracts where their account number appeared in the DEBIT.ACCT.NO field or CREDIT.ACCT.NO field.



## **Permitted Activity**

For all Users the information and facilities which may be accessed are specified at 4 levels: COMPANY; APPLICATION (and VERSION), FUNCTION and FIELD so that it is possible to specify precisely which records, belonging to which company, may be accessed and what may be done with them. Up to 999 combinations of Company, Application, Function and Field are allowed.

Access to applications must be granted positively except for *ENQUIRY.SELECT*, which is used to run enquiries.

🕘 USER PROF	ILE - Microsof	t Internet Ex	plorer			_ 🗆 🛛
	$\times [\checkmark] \land$		More Actions	÷	✓ →	
Base Details						
SAMPLE						
USER,DETS						
User Name	Sample USER re	cord				
Sign On Name	SAMPLER					
Classification	INT					
Language	1 English					
Department Code	1 Implementati	on				
Time Out Minutes	10					
Attempts	5					
Clear Screen	Y					
Amount Format	P					
Validity Function	ons Reports	_ogging  Dispo	o [Misc]			
Company Code :	1 US0010001					
Company Restr	1 US0010001					
Application 1	ØBASIC					
Company Restr.	2 US0010001					
Application.2	FUNDS.TRAN	SFER				
Function.2	A2BCDEF	HILPRSV				
Company Restr.	3 US0010001					
Application.3	CUSTOMER					
Version.3						
Function.3	LSP					
Field No.3	10					
Data Compariso	n.3 NE					
Data From.3	3400					
Override Class.	BMW					
Override Class.:	2 FORD					
						$\sim$
🥘 200606 - 1.6/0	60501   S.DONE	Y   Temenos Ban	k   07-SEP-2001   1	250-16		🧐 Local intranet 🔬

Figure 6 User permitted activity

In the above *USER* record the user is restricted to a few functions on *CUSTOMER* using a *VERSION*; the *FUNDS.TRANSFER* application and those specified in the *USER.SMS.GROUP* record '*BASIC*'.



To restrict the users access to particular data the following can be entered:

🛃 USER PROF	LE - Microsoft Internet Explorer	
	🗙 🐼 💽 🗃 🖪 👔 More Actions 🔍 🏹	^
Base Details		
SAMPLE		
USER,DETS		
User Name	Sample USER record	
Sign On Name	SAMPLER	
Classification	INT	
Language	1 English	
Department Code	1 Implementation	
Time Out Minutes	10	
Attempts	5	
Clear Screen	Y	
Amount Format	P v2 Development Development D	
Validity Functi	ons Reports Logging Dispo Misc	
		=
Company Code.	US0010001	
Company Restr.	1 US0010001	
Application.1	FOREX	
Function.1	ISDPL	
Field No.1	FOREX>CURRENCY.BOUGHT	
Data Compariso	n.1 EQ	
Data From.1	USD	
Company Restr.	2 US0010001	
Application.2	FUNDS.TRANSFER	
Function.2	A2BCDEFHILPRSV	
Company Restr.	3 US0010001	
Application.3	CUSTOMER	
Version.3		
Function.3	LSP	
Field No.3	10	
Data Compariso	1.3 NE	~
	KOEDI   S. DONEY   Temperer Back   07 SED 2001  E04 22	

Figure 7 Restrict User's Access to data that can be entered

**Note.** Field numbers can be used but this would entail keeping them updated whenever a new release adds new fields to the application.

Here the user is further restricted to processing only USD contracts, where USD is the currency bought.



As previously mentioned it is more advantageous to set access rights & restrictions by using *USER.SMS.GROUP* and then linking these to the relevant *USER* records. For example a basic access group could be defined and set on each *USER* record.

🔄 USER.SMS.GR	OUP -	Microsoft Internet Explorer	2	
USER.SMS.GRO BASIC	OUP	K D 🗃 🖪 ? More Actions 🗹 🗗	2	
GB Description	<b>H</b> *	jasic Apps		
Application.1	<b>HH</b> *	LD.LOANS.AND.DEPOSITS		
Version.1	E			
Function.1		A2BCDEFHILPRSV		
Field No.1				
Data Comparison.1		<b>v</b>		
Data From.1			=	11
Data To.1	E			
Temp Function.1	E			
Start Date.1	E			
End Date.1	E			
Application.2	• <b>•</b>	MM.MONEY.MARKET		
Version.2				
Function.2		A2BCDEFHILPRSV		
Field No.2				
Data Comparison.2	2 🗖 🚽			
Data From.2	E			
Data To.2	E			
Temp Function.2	E			
Start Date.2	E			
End Date.2	8			
Application.3	<b>E=</b> *	FOREX		
Version.3	E			
Function.3	E	A2BCDEFHILPRSV		
Field No.3	8			
Data Comparison.3	8 🗖			
Data From.3	E			
C 200606 - 1.6/060	JSO1   S.	DONEY   Temenos Bank   07-SEP-2001	S Local intranet	





Here a group *BASIC* has been defined to enable access to a few basic applications. This can be linked to a *USER* profile by entering "@BASIC" in the APPLICATION field e.g.

🔄 USER PROF	ILE - Microsoft Internet Explorer	_ 🗆 🛛
	💌 🛹 💌 🖃 🔼 🕐 More Actions 🔍 🏹	~
Base Details		
SAMPLE		
USER,DETS		
User Name	Sample USER record	
Sign On Name	SAMPLER	
Classification	INT	
Language	1 English	
Department Code	1 Implementation	
Time Out Minutes	10	
Attempts	5	
Clear Screen	Y	
Amount Format	P	
Validity Function	ons Reports Logging Dispo Misc	
Company Code.	1 US0010001	
Company Restr.	1 US0010001	
Application.1	@BASIC	
Company Restr.	2 US0010001	
Application.2	FUNDS.TRANSFER	
Function.2	A2BCDEFHILPRSV	
Company Restr.	3 US0010001	
Application.3	CUSTOMER	
Version.3		
Function.3	LSP	
Field No.3	10	
Data Compariso	n.3NE	
Data From.3	3400	
Override Class.	1 BMW	
Override Class.:	2 FORD	
		~
200606 - 1.6/0	060501   S.DONEY   Temenos Bank   07-SEP-2001  1250-16	net 🦽

### Figure 9 Adding USER.SMS.GROUP to USER record

In a site with a large number of users the use of *USER.SMS.GROUP* is strongly recommended.



## All Programs – All Functions

There is an option to set a User record to have access to all the applications in the system (entering ALL.PG in the APPLICATION field) and to have all the allowed functions (by entering ALL in the FUNCTION field which will then expand into the standard functions).

Unusual functions are not included in the ALL category, for example the 'Q' function is reserved for auditors and would not normally be used by anyone else.

In standard mode (exclusive) **T24** will check the *USER* applications and functions and build a list of the permitted applications & functions in a logical manner. What this means is that if a *USER* is given the first option to use ALL.PG in the applications field and ALL in the functions field and then has another multi-value set listing *CUSTOMER* with just the 'L S P' functions then the restriction on *CUSTOMER* will be respected and only the functions listed will be allowed. This method can be used to give power users a more manageable profile by just restricting any sensitive applications.

There is another option that can be set (the ALL.PG.INC field on *SPF*) which is by default blank and allows the standard mode mentioned above to continue. However, if is set then it has a very specific change in the way the ALL.PG setting works in combination with other listed applications. This non-standard mode (inclusive) will add any functions listed under ALL.PG to any applications listed individually as well as any they have listed already. For example if ALL.PG was given passive functions such as 'L S P' and *CUSTOMER* was set as 'I D A' then the user would be allowed to use functions 'L S P I D A' on *CUSTOMER* 

So the use of the ALL.PG, ALL & ALL.PG.INC settings should be used with due consideration to the effect they can have.



# **ENQUIRY.SELECT**

Access to *ENQUIRY.SELECT* is granted without restriction if the application does **not** occur in the *USER* record or in an associated *USER.SMS.GROUP*. If you want to restrict a user to running particular enquiries, then you must grant access to the application *ENQUIRY.SELECT* and restrict it appropriately, perhaps by the enquiry name or part of the description field.

🕘 USER PROF	ILE - Microsoft Internet Explorer	
	🔀 📈 💌 🖃 🔼 🕐 More Actions	<u> </u>
Base Details		
ENQ.RESTRICTED		_
USER,DETS		
User Name	ENQ.REST.USER	
Sign On Name	ENQUIRYMAN	
Classification	INT	
Language	1 English	
Department Code	1 Implementation	
Time Out Minutes	5	
Attempts	4	
Clear Screen	Y	
Validity Function	ons Reports Logging Dispo Misc	_
Company Code.	1 US0010001	
Company Restr.	1 US0010001	
Application.1	ENQUIRY.SELECT	
Function.1	L Contraction of the second	
Field No.1	0	
Data Compariso	n.1 LK	
Data From.1	STMT	
		~
<	Ш	
🕘 200606 - 1.6/0	060501   S.DONEY   Ter 📃 😒 Local intr	ranet 📑

Figure 10 Restrict a User to certain Enquiries

In the above screenshot the user will only be able to use enquiries whose name starts with STMT.

## **ENQUIRY**

The SMS restrictions on a *USER* that refer to a file or application can be applied when an *ENQUIRY* is run. By default the enquiry returns data **without** reference to SMS but the fields SMS.APPLICATION, SMS.ID and SMS.ABORT can be set to use the restrictions on the data. This is covered in the ENQUIRY section of the User Guides.

TEMENOS T24 User Guide



# **Activity Logging**

You can specify on the USER profile the level of user activity you wish to record. This can be at:

SIGN.ON.OFF	signing on and off
SECURITY.MGMT.L	running an SMS application
APPLICATION.LOG	running any application
FUNCTION.ID.LOG	entering a function and record id

Any combination of these can be chosen. Note: all security violations are recorded regardless of the logging specified here. The data is recorded in the *PROTOCOL* file, e.g.

🕘 PROTOCOL Default List - Microsoft Internet Explorer 🛛 📃 🗖 🔀							
Page	e1 - 2 💟 🔼 💟 🕞 (	Ø 💽 (	) <b>i</b>				^
	ØD	K.USER	APPLICATION	LEVEL.FUNCTION	PROCESS.DATE	ID	1
۹	200605100002543760.00			0		0	
٩	200605100002543765.00	S.DONEY	SIGN.ON		07 SEP 2001		
۹	200605100002543776.00	S.DONEY	USER.SMS.GROUP		07 SEP 2001		
٩	200605100002543777.00	S.DONEY	USER.SMS.GROUP	L	07 SEP 2001		
۹	200605100002543781.00	S.DONEY	USER.SMS.GROUP	L	07 SEP 2001		≡
۹	200605100002543781.01	S.DONEY	USER.SMS.GROUP	I	07 SEP 2001	IB.BADMIN	
۹	200605100002550618.00	S.DONEY	DE.FORMAT.SVMFT		07 SEP 2001		
۹	200605100002550622.00	S.DONEY	DE.FORMAT.SVMFT	S	07 SEP 2001		
۹	200605100002550624.00	S.DONEY	DE.FORMAT.SVMFT	s	07 SEP 2001	350.1.1	
٩	200605100002552819.00	S.DONEY	SIGN.OFF		07 SEP 2001		
٩	200605110000249448.00			0		0	
٩	200605110000249452.01	S.DONEY2	SIGN.ON		07 SEP 2001		
٩	200605110000249465.00	S.DONEY2	USER,		07 SEP 2001		
٩	200605110000249465.01	S.DONEY2	USER,	s	07 SEP 2001		
٩	200605110000249465.02	S.DONEY2	USER,	S	07 SEP 2001	S.DONEY	
٩	200605110000249466.00	S.DONEY2	USER,	с	07 SEP 2001		
٩	200605110000249468.00	S.DONEY2	USER,	с	07 SEP 2001	SAMPLE	
٩	200605110000249506.00	S.DONEY2	USER,	s	07 SEP 2001		
٩	200605110000249512.00	S.DONEY2	USER,	с	07 SEP 2001		
٩	200605110000249514.00	S.DONEY2	USER,	с	07 SEP 2001	SAMPLE	
٩	200605110000250599.00	S.DONEY2	USER		07 SEP 2001		<b>~</b>
<b>E</b> 2	00606 - 1.6/060501   S.DO	NEY   Teme	nos Bank   07-SEP-2	0	Nocal i	ntranet	

Figure 11 Details of all activity record on the PROTOCOL file

The *PROTOCOL* record holds details of the activity, the user, the application, the time, the terminal etc.



🛃 PROTOCO	L - Microsoft Internet Explorer
Jump to: %PROT	OCOL >
PROTOCOL 2006051100002	49468.00
Process Date	07 SEP 2001
Date Version	1
Time	13:44:28
Terminal Id	210
Company Id	US-001-0001 Temenos Bank
User	S.DONEY2
Application	USER,
Level Function	10
ld	SAMPLE
	~
🕘 200606 - 1.6	/060501   S.DONEY   👘 🛛 🔛 Local intranet

Figure 12 A PROTOCOL record.

In addition to on-line enquiries a protocol report is produced during the Close of Business using a REPGEN *PROTOCOL*.



## PASSWORD VALIDATION

It is now possible to define the minimum length of all **T24** user passwords. **T24** can also check the integrity of the syntax of the **T24** user password. The password parameters are now defined in the *SPF*, *SYSTEM* record of the **T24** system. Passwords can now consist of a certain amount of characters from each group in the *SPF*, *SYSTEM* record i.e. uppercase alphabetic, lowercase alphabetic, numeric and other characters. The **T24** administrator will maintain these password parameters.

After the minimum length of the password has been increased in the *SPF*, *SYSTEM* record, then when existing **T24** users sign onto the system using passwords based on the previous minimum length, they will have to be informed that their passwords have been terminated and that they must capture new passwords that conform to the parameters defined in the *SPF*, *SYSTEM* record.

🕙 SPF - Microsoft I	Internet Explorer	
Active User Batch	~	
Pass Min Length	8	
Pass Upper Alpha	3	
Pass Lower Alpha	2	
Pass Numeric	2	
Pass Other	*	
Version Auth Ctrl	▼	
No Indexes	~	
Reserved1		
Info Journal	~	
Browser Rec Lock	▼	
Commit Time Out		(1)
Min Password Days		
Global Process	× I	×
<	1111	>
🥘 200606 - 1.6/060501	S.DONEY   Temenos Ban	Second Se

Figure 13 Password validation parameters

In this example, the administrator has defined the password parameters for all **T24** users on this system. So when users log in, the system lets the user know that their passwords must change to consist of 3 uppercase alphabetic, 2 lowercase alphabetic, 2 numeric characters and must consist of a "\*". The password cannot be less than 8 characters long.



# **Re-Enabling User Profiles**

The system administrator will be required to re-enable a users profile when the user has forgotten their password, wishes to sign-on during a deactivated period or when the operating system has logged him out.

To re-enable the user profile the application *PASSWORD.RESET* should be run.

PASSWORD.RESET - Microsoft Internet Explorer	_ 🗆 🔀
PASSWORD.RESET, DEMO	
Liser Pw Attempt 1 🖶 SAMPLE	
Liser Attemnt 1	
No Of Attempts 1	
User Deact Perd.1	
Deactiv Period.1	
User Reset.1	=
User Password.1	
User Pwd.1	
Record Status	
Curr No	
Inputter.1	
Date Time.1	
Authoriser	
Co Code	
Dept Code	
Auditor Code	
Audit Date Time	<b>*</b>
🕘 200606 - 1.6/060509   S.DONEY   Temenos 🛛 📃 👘 😒 Local intrane	et 🦽

Figure 14 PASSWORD.RESET to re-enable a User profile

If the operating system logs out a user i.e. through a machine failure or UNIX kill, **T24** will still record them as signed on. Hence, if the user attempts to sign on again they will get the message:

To allow them to sign on again, the Administrator should run the application SIGN.ON.RESET.



🔄 SIGN.ON.RE	SET, - Microsoft Internet Explorer 📃 🗖	X
Image:	🗙 📈 💽 🗃 🌅 More Actions 🛛 💌 🗗	^
SIGN.ON.RES	ET,	
Userld.1 🚺	SAMPLE	
Record Status		
Curr No	1	
Inputter.1	24_S.DONEYOFS_GCS	
Date Time.1	18 MAY 06 16:32	
Authoriser	24_S.DONEY_OFS_GCS	
Co Code	US0010001 Temenos Bank	
Dept Code	1	
Auditor Code		
Audit Date Time		
<u> </u>		$\sim$
ど 200606 - 1.6/0	60509   S.DONEY   Te	

Figure 15 Sign On Reset to reset a User ID for use again

For both *PASSWORD.RESET* and *SIGN.ON.RESET*, multiple user profiles can be reset. Note: the Authorisation process resets the profiles; typically these would be used with a self-authorising *VERSION*; SMS regulations permitting.

# Activating programs at SIGN In / SIGN Out

SIGN.ON.ITEM field.

The name of any Application, Enquiry, Script, etc. can be entered into the multi-valued field.

Each multi-valued field will be processed in the order in which it appears during the Sign On process, with the commands at the beginning of the field processed first.

SIGN.OFF.ITEM field.

This field allows a user defined DataBasic subroutine that accepts one parameter to be invoked during the Sign Off process. Enter the name of the subroutine that needs to be invoked during Sign Off into this field.

During the Sign Off process, the subroutine will be passed one parameter. If the parameter returns with the values 'N', or 'NO' the Sign Off process will be halted. Any other value returned will cause T24 to continue the Sign Off process.

TEMENOS T24 User Guide



A *PGM*.*FILE* definition for the subroutine is required for the subroutine to be run during the Sign Off process.

# Setting a user with a new password

You can set a user password to a specific value for their first sign-on using the USER.RESET and USER.PASSWORD fields in the *PASSWORD.RESET* record.

E PASSWORD.RESE	T - Microsoft Internet Explorer	- 🗆 🗙
PASSWORD.RESE	✓ C D ( ) A ? More Actions Y → T,	
User Pw Attempt.1 🕀		
User Attempt.1		
No Of Attempts.1		
User Deact Perd.1 🔳		
Deactiv Period.1		≡
User Reset.1 🔳	SAMPLE	
User Password.1 🔳	QWERTY	
User Pwd.1		
User Reset.2 🔳	SETPASS	
User Password.2 🔳	123456	
User Pwd.2		
Record Status		
Inputter 1		
Date Time.1		
Authoriser		~
ど 200606 - 1.6/060509	)   S.DONEY   Temenos 🤤 Local intrane	t 🔐

Figure 16 Resetting USER with one-shot passwords

The passwords are cleared from the record when it is committed, so you have to remember or note them to tell the users. The users will have to set a new password in the process of logging on. This process retains old passwords thus preventing re-use.

# Setting a user with a new random password

A routine to generate random passwords (GEN.RANDOM.PSWD) is provided. To use it, set up a *VERSION* record with @GEN.RANDOM.PSWD in VALIDATION.RTN for *USER.PASSWORD*. For example:



🕙 VERSION - Microsoft Internet Explorer 📃 🗖 🔯				
	C 🐼 C D 😂 🔼 ? More Actions Y 🗗	^		
VERSION, DASSWORD DESET	DEMO			
PASSWORD.RESET	,DEMO			
Records Per Page	1			
Fields Per Line	1			
Language Code.1	1 English			
Field No.1	USER.RESET			
Field No.2	USER.PASSWORD			
Validation Fld.1	USER.PASSWORD			
Validation Rtn.1	@GEN.RANDOM.PSVVD			
Record Status	IHLD INPUT Held			
Inputter.1	11_S.DONEY2_I_IHLD_OFS_GCS			
Date Time.1	19 JUN 06 15:32			
Co Code	US-001-0001 Temenos Bank			
		$\checkmark$		
🥌 200606 - 1.6/060	0607   S.DONEY2   👘 🛛 🔍 😒 Local intranet			

Figure 17 A VERSION, which resets a USER with a random password

This routine allows only one *USER* per record to be reset. The USER.PASSWORD field is cleared when the record is committed so it must be remembered or noted on input or it will have to be reset again. The routine also blocks further input in the password field and you must quit the application before you input another record.



If you want to ensure that sign-on without an initial password is not allowed then set up the following subroutine for use and apply it as a BEFORE.AUTH.RTN in the VERSION you apply to authorise a USER record.

File GLOBUS.BP , Record 'BLOCK.PASSHORD' Command-> 0001 SUBROUTINE BLOCK.PASSHORD 0002 0003 \* This routine should be run from a VERSION record for the USER 0004 \* application and will write '\*\*\*\*' to the USER<PASSWORD> field 0005 \* on a new USER record. This will prevent access until PASSWORD.RESET is 0006 \* run to give the a password to login with. 0007 0008 \$INSERT I COMMON 0009 **\$INSERT I EQUATE** 0010 \$INSERT I F.USER 0011 0012 IF R.NEW(EB.USE.CURR.NO) = '1' THEN 0013 R.NEH(EB.USE.PASSHORD) = '\*\*\*\*\* 0014 END 0015 0016 RETURN 0017 AA18 END

Figure 18 Routine to prevent use of new USER until PASSWORD.RESET



🕘 VERSION - Mi	crosoft Internet Explorer					
	A Comparison of the section of th	<u>^</u>				
VERSION						
USER,DEMO						
Basanda Ban Bana						
Records Per Page						
Fields Per Line						
Language Code.1	1 English					
No Of Auth						
Val Assoc.1.1	START.TIME					
Val Assoc.1.2	END.TIME					
Val Assoc.2.1	CUSTOMER	=				
Val Assoc.2.2	ACCOUNT	=				
Val Assoc.3.1	COMPANY.RESTR					
Val Assoc.3.2	DATA.TO					
Val Assoc.4.1	RPT.TO.RECEIVE					
Val Assoc.4.2	(ST.SPOOL.TIME					
Val Assoc.5.1	I.USER.NAME					
Val Assoc.5.2	DATE.CREATED					
Val Assoc.6.1	ALLOWED.DAYS					
Val Assoc.6.2	DAY.END.TIME					
Sub Assoc.1.1	DAY.ST.TIME					
Sub Assoc.1.2	DAY.END.TIME					
Local Ref Field	LOCAL.REF					
Report Locks	YES					
Before Auth Rtn.1	@BLOCK.PASSWORD					
Curr No	1	~				
		<u> </u>				
200606 - 1.6/06	0509   S.DONEY   Temenos Bank   0 🛛 🛛 😽 Local intran	et 📰				

Figure 19 VERSION to prevent use of new USER until PASSWORD.RESET



# Logging in based on days of a week

🕘 USER PROF	ILE - Microsoft Internet Explorer	
	🗙 📈 💌 🖃 🔼 🕐 More Actions 🛛 💙 🗗	<u>^</u>
Base Details		
SAMPLE		
USER,DETS		
User Name	Sample USER record	
Sign On Name	SAMPLER	
Classification	INT	
Language	1 English	
Department Code	1 Implementation	
Time Out Minutes	10	
Attempts	5	
Clear Screen	Y	
Amount Format	<u>P</u>	
Validity Function	ons Reports Logging Dispo Misc	=
Dessword Valid	ty 01 NOV 2006 M0601	
Start Date Profile	01 IAN 1985	
End Date Profile	31 DEC 2009	
Start Time 1	08:30	
End Time 1	12:00	
Start Time 2	13:00	
End Time 2	17:30	
Max Sessions	5	
Attributes 1	SUPER USER	
Allowed Days,1	1	
Day St Time.1.1	08:00	
Day End Time.1.	1 17:00	
Allowed Days.2	2	
Day St Time.2.1	10:00	
Day End Time.2.	1 18:00	
		<b>~</b>
🥘 200606 - 1.6/0	160509   S.DONEY   Temenos Bank   07-SEP-2001  782-16-7	net 🦽

Figure 20 Day & Time checking

A special note: If in *USER* profile a different logging in time has been defined. It will override what has been defined in *USER.SMS.GROUP* 



# Defining USER.SMS.GROUP

🔄 USER. SMS. G	ROUP - Microsoft Internet Explorer	
	🗙 📈 💽 😂 🎦 More Actions 🛛 💌 🛃	^
USER.SMS.G	ROUP	
HVADENS		
GB Description	Traders	=
Application.1	FOREX	=
Function.1	A2BCDEFHILPRSV	
Application.2	SWAP	
Function.2	S S	
Allowed Days.1	*	
Day St Time.1.1	07:30	
Day End Time.1.1	1 17:30	
Curr No	1	~
200606 - 1.6/0	160509   S.DONEY2   Temenos Bank	et 🦼

#### Figure 21 SMS Grouping

The above set-up has been done in such a way that the group of users who are defined as *TRADERS* will be able to have all functionality for *FOREX* application, while only "See" functionality for *SWAP* and no access to any other application.

They have access to the system between 07:30 A.M. and 17:30 P.M.



🔄 USER.SMS.G	ROUP -	Microsoft Internet Explorer	×
	× ] 📈	💽 🕞 🧟 👔 More Actions 🛛 💌 🗗	
USER.SMS.GF TRADERS	ROUP		
GB Description	Traders		
Application.1	FOREX		
Function.1	A 2 B C	DEFHILPRSV	≣
Application.2	SWAP		
Function.2	S		
Allowed Days.1	*		
Day St Time.1.1	09:00		
Day End Time.1.1	19:00		
Allowed Days.2	2		
Day St Time.2.1	09:00		
Day End Time.2.1	10:00		
Day St Time.2.2	14:00		
Day End Time.2.2	15:00		
Record Status	IHLD	INPUT Held	
Curr No	1		$\mathbf{M}$
🕘 200606 - 1.6/0	60607   S	.DONEY2   Teme 😔 Local intranet	

**Figure 22 Group restrictions** 

Multiple timings within the same day can also be given. In the above example the user has rights to login on Tuesday between 09:00 AM and 10:00 AM. Also the user can login between 14:00 and 15:00 on the same day. The user is denied entry at any time other than the one set-up.



# Linking USER.SMS.GROUP to USER

🕘 USER PROFI	LE -	Microsoft Internet Explorer	- 🗆 🗙
Image: Contract of the second seco	$\times$	📈 < 🗈 🗃 🔼 😢 More Actions	^
Base Details			
USER, DETS			
User Name	<b>*</b> Sa	ample USER record	
Sign On Name	<b>*</b> S/	AMPLER	
Classification	* 11	іт 💌	
Language	* 1	English	≡
Department Code	* 1	Implementation	
Time Out Minutes	* 10		
Attempts	* 5		
Clear Screen	<b>*</b> Y		
Amount Format	e.		
Date Format			
Validity Functio	ons	Reports Logging Dispo Misc	
Company Code.1	Ŧ	* US0010001	
Init Application			
Customer.1	<b>[+</b> ]		
Account.1.1			
Company Restr.		3* US0010001	
Application.1		* @TRADERS	
Version.1	Ξ		
Function.1	E		
Field No.1	E		~
<		ш	
🥘 200606 - 1.6/0	60509	9   S.DONEY   Temenos Bank   07-SEP-2001  4235-78-4	t:

Figure 23 USER.SMS.GROUP

The *USER.SMS.GROUP* can be the sole set of rules/restrictions on the *USER* record or more usefully it can be combined with settings that are unique to that person.

These extra settings can add functionality; remove functionality or a combination of both on top of those in the specified *USER.SMS.GROUP* record.

# **Security Violations**

Protecting **T24** from access by unauthorised users and preventing users from using parts of the system they are expressly forbidden to use requires an approach that is helpful enough to legitimate users when they make a mistake or have a problem but does not provide useful information for the unauthorised.

In the examples below some of the texts have been changed from the non-descript 'Security Violation' to something more explanatory for the purpose of illustrating that the messages are individual – the SMS logs should be checked for the actual nature of the violations.

# Access to T24

The *USER* profile is set to restrict the actions of the staff member and depending on the way that each bank stipulates its security protocols the member of staff may encounter security warnings at various stages. The primary place of access is the sign-on screen where the user must enter both the user name and their individual password.

<b>€</b> TEMENOS™				<u>^</u>
FULL TOUR QUICK GUIDE	FAQ	HELP		
		Security Violatio	n (WHY)	E
	Sign On nam	es and passwords	are case sensitive	
	Nam Passwor	e •••••		
	Copyright © 1	femenos Holdings	NV. All rights reserved	
<		1111		×

Figure 24 Sign on Invalid – in this case it's an invalid name

- An invalid name will be given a security violation warning
- An incorrect password will be given a security violation warning
- Too many attempts will give the same warning



# Restrictions

The *USER* record will restrict the staff member (or external client) to certain parts of the database (by *COMPANY* code) and various applications and functions. Trying to use an application or function that is not allowed will trigger a security violation warning, which may be logged (if logging is activated).

🕙 T24 - Microsoft Internet Explorer 📃 🗔 🔯
File Edit View Favorites Tools Help
🕞 Back 🔹 📀 🕤 📓 🏠 🔎 Search 🤺 Favorites 🤣 🔗 🍚 📴 📑 🎼 🎊
Address 🗃 http://localhost:8080/BrowserWeb/servlet/BrowserServlet 🛛 💽 Go 🕴 Links 🎽 🍥 SnagIt 📑
Sample USER record
Last signed on 19 MAY 2006 at 14:58 with 0 attempts
* ? TZ4 () es x =
Syndicated Loans
New Delivery Service     Frior message - Microsoft Internet Explorer
Cashpooling
Direct Debits     Error message
Confirmation Matchin     Security Violation (Rights)
EQueries and Answer
ERepos Menu
🗄 Portfolio Managemen 🍘 200606 - 1.6/0605i 🛛 😌 Local intranet
ESecurities Front Office
ESecurities Back Office
🛨 Data Capture Menu 🛛
🔊 Done 🤤 Local intranet 🛒

Figure 25 Trying to use an application not on the USER record

# Maintenance

In instances where the USER profile is being modified and awaits authorisation **T24** will prevent access by that user on the basis of the change could be one removing access or privileges. Once the user record is authorised the person will be permitted to log in subject to the time & date restrictions imposed on them



### **Times**

Should access be attempted outside of the times permitted, or outside of the days permitted a security violation will be given (and optionally logged).

*USER* records can be deactivated for periods where the person is absent for a period of time such as annual leave.

<b>€</b> TEMENOS™		
FULL TOUR QUICK GUIDE	FAQ HELP	
	Access not within times permitted	≡
	Name Password ••••••	
	Copyright © Temenos Holdings NV. All rights reserve	d
٤)	ш	

Figure 26 User trying to access the system outside of the permitted hours

# **OVERRIDE**

In **T24** where circumstances occur that require the user to confirm an action which needs to be approved an override will be required. The concept of the override process spans from any user approving the override at input, up to a full system of tiered approval levels (using *DISPO.ITEMS* mentioned later in this document).

Overrides can be displayed as an Error, Message, Warning or Auto override. These are defined in the TYPE field on the *OVERRIDE* application.

In the following example, the first multi-value set (fields GB MESSAGE.1 to OVERRIDE ACTION.1) defines the default override settings. The CHANNEL.1 field must contain a Null value to ensure that a default setting is configured.

The *CALLCENTRE* channel in the following example is configured to display a Warning instead of the default override message.

Multiple channels can be defined in an *OVERRIDE* record. However, the same channel cannot be defined more than once in a single *OVERRIDE* record.

🕹 http://localhost:8080 - OVERRIDE - Mozilla Firefox	
GB Message.1 Inauthorised overdraft of & & on account &.	
Type.1 🔲 💌	
Channel.1 🔤	
Approve Method.1 😑	
Override Action.1 🗧	
Reserved12.1	
Reserved13.1	
Reserved14.1	
Reserved16.1	
GB Message 2 Warning - Unauthorised overdraft of & & on account &.	
Type.2	
Approve Method 2	
Override Action 2	
Reserved12.2	
Reserved13.2	
Reserved14.2	
Reserved15.2	
Reserved16.2	
Prev Message.1.1 CCOUNT & UNAUTHORISED OVERDRAFT &&	
Prev Message.2.1 BEE ACCOUNT & UNAUTHORISED OVERDRAFT &&	
Reserved04	>

#### **Figure 27 OVERRIDE**



The following example illustrates the input of a transaction via the *CALLCENTRE* Channel. In this instance the override is displayed as a Warning – as per the above OVERRIDE record: -

🕲 http://localhost:8080 - SECURITY.TRA	NSFER - Mozilla Fir	efox 🗖 🗖 🔁	<
⊖Errors Messages	SECURITY.TRANS	SFER	~
1 Warnings	Transaction Type	* TRI	3
Warning - Unauthorised overdraft of USD 2276030.1 on account 21717.	Security No Security Ccy I	* 100041-000	
	Depository	100317	
	Price Type	0	
	Trade Date	25 JUN 2003	
	Value Date	25 JUN 2003	
	Customer No	* 1006	
	Security Acc	1006-1	
	Nominee Code		
	No Nominal	* 10,000	
	Price	42.9	
	Cost	730,222.35	
	Gross Amt Sec Coy	429,000.00	
	Charges	0.00	
	Local Tax	0	
	Cu Commission		
	Cu Tax		
	Interest Amt		
	Net Amt Sec Coy	429,000.00	
	Sec Exch Rate		
	Cu Account No		-

Figure 28 CALLCENTRE override



In the following example a Channel has not been defined on the *OVERRIDE* record. In this instance the NUMERIC.ID field value is displayed in the override message: -

🕹 http://localhost:8080 - OVERRIDE - Mozilla Firefox	
🔽 📭 🖂 🔽 🗶 🖪 🖪 🕐 More Actions 🕑 🌶	^
OVERRIDE ACCT.UNAUTH.OD	=
GB Message.1 Inauthorised overdraft of & & on account &	
Type.1	
Channel.1	
Approve Method.1	
Override Action.1	
Reserved12.1	
Reserved13.1	
Reserved14.1	
Reserved15.1	
Reserved16.1	
Prev Message.1.1 EVE ACCOUNT & UNAUTHORISED OVERDRAFT &&	
Prev Message.2.1 EXE ACCOUNT & UNAUTHORISED OVERDRAFT &&	
Numeric Id O-11012	
ReservedD3	<u>×</u>
	>

#### **Figure 29 OVERRIDE**







# **OVERRIDE CLASS**

During the input of a transaction, **T24** can request the user to override a certain condition, e.g. an account is overdrawn or has a posting restriction. The overrides are recorded on the transaction so that the authoriser can view all overrides encountered during input.

The system administrator, normally in conjunction with the appropriate supervisor, can define certain conditions, which can only be overridden by a specific user. For example, you may wish to restrict the overrides of account overdrafts to supervisors only.

# ACCOUNT-123456 UNAUTHORISED OVERDRAFT GBP 5000.00

To do this you define a class for the override, or overrides, and then allow that class for certain users. To define the class, use the application *OVERRIDE.CLASS*.

🛃 OVERRIDE.CLASS - 1	Microsoft Internet Explorer	_ 🗆 🛛
OVERRIDE.CLASS DATA.CAPTURE	More Actions 💌 🗗	
Override Text.1 🔳 🖬 🕴	ACCOUNT-& UNAUTHORISED OVERDRAFT & &	≡
Override Detail.1 🖃 🛛		
Default Class.1 🔲 🛛	KS	
Override Text.2 🔳 🗮 🗄	EXCESS & & ID=&	
Override Detail.2 🖃 🛛		
Default Class.2 🔲 🛛	(S	
Reserved 3		
Reserved 2		~
<	1111	>
🕘 200606 - 1.6/060607   S	5.DONEY2   Temenos Bank   07-5E	Uccal intranet

Figure 31 Overriding Conditions – defining class of 'XS'

Here a class of "XS" has been defined in *DATA*. *CAPTURE* for the overdraft and limit excess overrides. Note: The "&" embedded in the text defines where variable information, such as amounts, will be displayed.

To allow a user to override these messages "XS" must be entered on his USER profile.



🕘 USER PROFILE - M	Microsoft Internet Explorer	- 🗆 🗙
	📈 💌 🖃 🔼 🕐 More Actions 🔍 🕞	^
USER,DEMO		
SAMPLE		
Liser Name	Sample USER record	
Sign On Name	SAMPLER	
Classification	INT	
Language	1 English	
Company Code.1	US0010001	
Department Code	1 Implementation	
Password Validity	01 DEC 2006 M0601	
Start Date Profile	01 JAN 1985	=
End Date Profile	31 DEC 2009	
Start Time.1	08:30	
End Time.1	24:00	
Time Out Minutes	10	
Attempts	5	
Company Restr.1	US0010001	
Application.1	ALL.PG	
Function.1	A2BCDEFHILPRSV	
Sign On Off Log	Y	
Security Mgmt L	Y	
Application Log	Y	_
Function Id Log	Y	
Input Day Month	DDMM	
Date Last Sign On	16 JUN 2006	
Time Last Sign On	18:00	
Passw Change Date	16 JUN 2006	
Clear Screen	Y	
Override Class.1	XS	
Override Class.2	DSP2	
Override Class.3	DSP3	
Override Class /	NGD4	<b></b>
😂 200606 - 1.6/060607	S.DONEY2   Temenos Bank   07-SEP-2001  71 🛛 🛛 😽 Local intrane	et:

Figure 32 Define class 'XS' in User Profile

It should be noted that the authority to approve the override is based on the User, not the (A)uthorise function. If the Department Manager has a specific class of override that they alone can approve, and they input a deal, then the override is deemed to be approved. However, it is normally the Authoriser that does have the necessary privileges and usually where the overrides are approved. If an Authoriser cannot 'approve' all the overrides, the message "YOU CAN'T APPROVE ALL OVERRIDES" is displayed and the record remains unauthorised.



The status of the override can be seen in the audit fields.

Override	Status
No Line Allocated	Standard – No privileges required. Any authoriser can approve deal.
No Line Allocated*MGR	Has an <i>OVERRIDE.CLASS</i> . Authoriser needed with class MGR on their <i>USER</i> profile
No Line Allocated*MGR*I	Has an <i>OVERRIDE.CLASS</i> , but the inputter has the class MGR on their <i>USER</i> profile.
No Line Allocated*MGR*UserName	The <i>OVERRIDE.CLASS</i> MGR has been approved by the <i>USER</i> who appears in the position shown here as UserName

#### Figure 33 Override audit fields

Overrides can also be classified by the variable information shown in the message. Hence, you could restrict approval of overdrafts greater than USD 10,000.00 to specific users. To do this you enter the details in the application *OVERRIDE.CLASS.DETAILS* and link them to the *OVERRIDE.CLASS* record.

OVERRIDE CLASS DETAILS - Microsoft Internet Explorer	_ 🗆 🔀
🔽 ≌ 🔲 🗙 🐼 💽 😂 🧖 🕐 More Actions 💌 🍠	^
OVERRIDE.CLASS.DETAILS EXCESS/0D	
	≡
Data Def.1	
Classification.1 💽 🛪 XS	
Data Def No.1.1 💽 🗶 1	
Comparison.1.1 * GT 🔽	
Data From.1.1 10000	
Data To.1.1	~
🕘 200606 - 1.6/060607   S.DONEY2   Temenos Bank   0; 🛛 🛛 😒 Local intr	ranet 📑

Figure 34 Specify overrides in the Override Class Details Record

In this example only users with the override class of "XS" can approve limit excess messages where the amount is greater than 10,000.00 US dollars. All other users can only approve amounts less than this.

See the helptext for the application *OVERRIDE.CLASS.DETAILS* for more information on the use of conversion routines and testing variable data.



# **Override Management – Auto Override Processing**

### Introduction

**T24** has the functionality to automatically decline or accept generated overrides when using OFS (Open Financial Service). The STP (Straight Through Processing) functionality uses OFS to process orders and requires Auto Override Processing to automatically validate overrides - avoiding user intervention.

### Installation

In order for Auto Override Processing to be enabled, certain steps must be taken to set up the validation process. This functionality enables the user to set up validations on overrides to apply to all applications or only to certain applications. It can also be set up to only perform certain validation depending on which OFS process is being performed.

For each override on the system, an *OVERRIDE* record exists which will contain the override text in the MESSAGE field of the *OVERRIDE* record. The MESSAGE text may contain one or more ampersands (&). These are known as variable placeholders. An example of a MESSAGE field within an *OVERRIDE* record can be seen in the screenshot below:

🔄 OVERRIDE - I	<i>d</i> icros	oft Internet Explorer	
	× ] [~	🛛 💽 🖃 🔼 😢 More Actions 🛛 🖌	
OVERRIDE			
ACCT.UNAUTH.OD			
GB Message	Unauth	orised overdraft of & & on account &.	
Prev Message.1.1	ACCO	JNT & UNAUTHORISED OVERDRAFT &&	
Data Type.1	CCY		≡
Data Type.2	AMT		
Data Type.3	ACC		
Application.1	*		
Class.1	DSP1		
Dispo.1	YES		
Dispo Officer.1	1120	Assistant Lending Officer	
Dispo Allowed	YES		
System	YES		
Curr No	6		~
<		Ш.	>
🕘 200606 - 1.6/06	60607	5.DONEY	

#### Figure 35 OVERRIDE Record example 1

The variable placeholders will be assigned data by the application that generated the override message, prior to the message being displayed. In the screenshot examples, the first variable placeholder will contain a Currency; the second variable placeholder will contain an Amount and the last the Account number.



🕘 OVERRIDE	- Microsoft Internet Explorer	X
	🗙 📈 🔹 🖻 🎒 🖪 🕐 More Actions 🛛 🗸 🌖	
OVERRIDE		
EXAMPLE		
Ofs Source.1	OFS OFS Batch	
App Version.1	SEC.TRADE,CUS	
Validation.1.1	CHECK.TRADE	
App Version.2	SEC.TRADE SEC.TRADE	
Validation.2.1	CHECK.TRADE	
App Version.3	SEC.OPEN.ORDER,BUY.MORE	=
Validation.3.1	CHECK.SECURITY	-
Condition.1	CHECK.TRADE	
Data Posn.1.1	2	
Operator.1.1	GT	
Value.1.1	1000	
Action.1.1	AND	
Data Posn.1.2	1	
Operator.1.2	RG	
Value.1.2	00500*99500	
Separator.1.2	*	
Action.1.2	ACCEPT	
Condition.2	CHECK.SECURITY	
Data Posn.2.1	3	
Operator.2.1	LT	
Value.2.1	000001-000	
Action.2	DECLINE	
GB Info.1	Override to check Security & Trade details	~
🥘 200606 - 1.6,	/060607   S.DONEY   Temer School Scho	

Figure 36 OVERRIDE record example 2

The following is a description of fields, which may have to be populated to enable the Auto Override functionality:

### **OVERRIDE**

Field Name	Description	
DATA.TYPE	This field is used to determine the data type of the data elements in the MESSAGE field which are represented by a (&).	
DATA.DESCRIPTION	A text description of the above data being passed in.	
OFS.SOURCE	Will contain the key to an <i>OFS.SOURCE</i> record, which contains the details of the OFS process to be used. This field will need to be input to perform Auto override processing.	
APP.VERSION	This determines which Applications or VERSIONS of applications will perform automatic Override validation during an OFS process	



SUBROUTINE	<ul><li>Enables the user to input a user defined subroutine to carry out the validation process. If this is the case, no further validation will be performed.</li><li>The subroutine should return either a "Y" or "NO" to indicate whether the Override is automatically approved or not.</li></ul>
VALIDATION	This determines which validation routines to run from the CONDITION field for the associated Application or Version.
CONDITION	If no input has been made into the associated SUBROUTINE field, the system will use the validation parameters stored on the OVERRIDE record. This field is multi-valued & determines the Validations to be used.
	As soon as a TRUE condition is met with a Valid ACTION then no further validation will be performed.
DATA.POSN	This field refers to the position of the data passed in from the calling routine that is represented by the '&' in the MESSAGE.
OPERATOR	The operator (e.g. EQ, NE, GT etc) that will be used in conjunction with DATA.POSN & VALUE to form a selection sentence.
VALUE	The value is to be compared with the value in the field specified by the DATA.POSN.
SEPARATOR	This field is used to separator multiple entries of data in the VALUE field.
ACTION	This is the action that will be performed assuming that the data validation performed is <i>TRUE</i> .
	AND – This will connect one validation with the next one assuming that the result of this validation was <i>TRUE</i> . ACCEPT - Assuming that the data validation is <i>TRUE</i> the Override will be automatically accepted. DECLINE - Assuming that the data validation is <i>TRUE</i> the Override will be automatically declined.
INFO	User can input text regarding the override.
SYSTEM	If 'Yes' then the record is a <i>TEMENOS</i> generated record.

# **VERSION**

Field Name	Description
AUTO.OVERRIDE	If this field is set to 'Yes', individual validation of overrides generated by this version will be performed.



# Using Auto Override Processing

In order for the automatic validation of overrides to be performed, a *VERSION* must be used to process the transaction. The field AUTO.OVERRIDES in the *VERSION* should be set to 'Yes'.

The field OFS.SOURCE on the *OVERRIDE* record of each of the overrides generated by the transaction will then be read to obtain the key to the *OFS.SOURCE* record. This record will contain details of the OFS process, which is to be used for this transaction (more than one OFS process may be specified in an *OVERRIDE* record to allow different processing states for individual versions or applications). A check will then be made to ensure that the *VERSION* or application being used to process the transaction is present in the APP.VERSION field of the *OVERRIDE* record. For example, if the current transaction is being processed through the version *SEC.TRADE,BUY*, in order for auto validation to be performed, the APP.VERSION field must contain one of the following:-

### 1. SEC.TRADE,BUY

The full version name.

### 2. SEC.TRADE

The process will be performed for any *VERSION* of *SEC.TRADE*.

### 3. \* (Asterisk)

The process will be performed for any Application or VERSION.

If either the AUTO.OVERRIDES field in *VERSION* is not set to 'Yes', a valid *OFS.SOURCE* record key has not been entered into the OFS.SOURCE field of the *OVERRIDE* record or valid input can not be found in the APP.VERSION field of *OVERRIDE*, then the existing functionality will be performed whereby the override will be displayed and a user response will be requested.

If a SUBROUTINE has been specified in the *OVERRIDE* record relating to the APP.VERSION being processed, then this will then be called to perform the override validation. Otherwise, any processes specified in the VALIDATION field relating to this APP.VERSION will be performed.

For each VALIDATION field associated with the APP.VERSION, there will be a CONDITION field with the same name. Within this CONDITION, one or more condition sentences can be specified – to be performed on the data contained within the override variable placeholders (&) in the MESSAGE field. If the condition statement performed on the data is found to be 'True' then the action outlined in the ACTION field will be performed. Valid input into the ACTION field is either 'ACCEPT', DECLINE' or AND'. The ACTION 'AND' can be used to link one or more condition statements to construct a string of linked conditions before a final 'ACCEPT' or 'DECLINE' is specified.

If a condition is found to be true, then the ACTION field for the CONDITION will determine the next process.

If the ACTION field is 'AND', the condition statement is part of a string of condition statements. The ACTION field on the final condition statement will either be 'ACCEPT' or 'DECLINE'

If the ACTION field for the condition is 'ACCEPT', then either the next VALIDATION will be performed for this APP.VERSION (if any) or the override will be automatically accepted (the equivalent of manually answering 'YES' to the override.

If the ACTION in a condition is 'DECLINE', then a message will appear on screen to notify the user that the override has been declined and an update will be made to the *EXCEPTION.LOG.FILE* with details of the declined override.



# Multi-valued DATE.TIME audit information

If required, it is possible to record the date and time of every action on a record since its creation or last authorisation, along with the function used and the status of the record at that time. This can be activated by setting the DATE.TIME.MV field on the *SPF SYSTEM* record to YES.

🕘 SPF - Microsoft	Internet Explorer	
SPF,MISC System	📈 🕞 🕞 🖪 🔋 More Actions 💌	] 🗗 – 🧖
User Code Txn Management Timeout Mode Pwd Repetition		
Database Type Gac Account <mark>Date Time Mv</mark>		
Pre Batch Rout.1		
<b>S</b> 200606 - 1.6/0606	07   S.DONEY   Temenos Bank   07	Vertical intranet

Figure 37 Flag to record the data & time of all record actions



🔄 SECTOR -	Microsoft Internet Explorer	
	🛛 🖂 💌 🖃 🧖 🕐 More Actions 🛛 💌 🗗	~
SECTOR		
1000		
GB Descriptio	on Financial Corporations	
GB Short Nar	ne Financial Corps	
Curr No	2	
Inputter.1	18_ANDREWVICKERS1	
Date Time.1	26 MAY 00 14:44	
Authoriser	18_ANDREWWICKERS1	
Co Code	US-001-0001 Temenos Bank	
Dept Code	1	
		$\sim$
🥘 200606 - 1.0	6/060607   S.DONEY   Teme	

### Figure 38 Record of Sector-Default action

🔄 SECTOR -	Microsoft Internet Exploi	rer	_ 🗆 🗙
		🔨 😰 More Actions 🛛 💌	<b>)</b>
SECTOR			
1000			
GB Description	n Financial Corporations.		
GB Short Nam	e Financial Corps		
Curr No	4		
Inputter.1	5_INPUTTER_I_INAU		
Inputter.2	5_S.DONEY_I_INAU		
Date Time.1	19 JUN 06 14:10		
Date Time.2	19 JUN 06 14:10		
Date Time.3	19 JUN 06 14:09		
Authoriser	5_AUTHORISER		
Co Code	US-001-0001 Temenos Bank		
Dept Code	1		
			~
🥘 200606 - 1.6	5/060607   S.DONEY   Ter	Succel intrane	et

# Figure 39 Multiple time and date record updates



# **User Attributes**

The field ATTRIBUTES on the USER profile can be used to control specific **T24** functionality. The following options are available and have the following affect:

COMMAND.LINE	The user is allowed the use of the command line in T24 Browser.		
DEV.STUDIO	Reserved for future use.		
EXPLORER	Allows the user to use the Application explorers		
LOCK.DEACTIVATION	Prevents USER access to the User Deactivation listed in Tools dropdown list.		
LOCK.DESIGNERS	Prevents USER access to the listed Designer Tools dropdown list.		
LOCK.MISC.ITEMS	Will bring up a Security Violation when the User Abbreviations Toolbar, Enquiry and Report lists are used.		
NO.ENQUIRY.EXPORT	Prevents USER Exporting Enquiry data from an Enquiry screen, the icon will be dimmed and non reactive.		
ENQUIRY.INDEX	Allows access to the enquiry index		
REALTIMEENQUIRY	Allows the use of real time enquiries for this user. When signing onto T24, Browser will create another session for use by the real time enquiries. This does use an additional database license, but not an additional T24 license.		
LOCK.PREFERENCES	If the user is given this option then the 'User Preferences' option under the 'Tools' menu on the Desktop toolbar will be disabled. This will prevent the user from gaining access to various Desktop settings including file locations and some system administrative functions.		
SUPER.USER	The user has access to all of the features detailed above, and for all future functionality with the exception of REALTIMEENQUIRY.		

Some of these fields are only used by the Desktop interface and are not used by BROWSER and as such may become obsolete when Desktop support ceases.



🛃 USER PROFILE - N	Aicrosoft Internet Explorer	
Last Spool Time.1 Amount Format Create Gi User Gi User Name.1 Date Created 1		^
Max Sessions		
Attributes.1 IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII	SUPER.USER  COMMAND.LINE  Ifficer  DEVSTUDIO Icer ENQUIRY.INDEX EXPLORER LOCK.DEACTIVATION LOCK.DESIGNERS LOCK.MISC.ITEMS LOCK.PREFERENCES NO.ENQUIRY.EXPORT REALTIMEENQUIRY SUPER.USER	
Allowed Days.1 Allowed Days.1 Day St Time.1.1 Day End Time.1.1 Ldap Id Ldap Dn		
<		>

Figure 40 Field ATTRIBUTES can be multi-valued to allocate specific User Attributes



# Intelligent Override Processing - The Dispo System

### Introduction

Dispo processing is the ability to direct overrides to the people whose attention the override requires, and is in addition to the functionality offered by *OVERRIDE.CLASS* and *OVERRIDE.CLASS.DETAILS*.

### OVERRIDE

The *OVERRIDE* table contains a list of the overrides that **T24** uses. The table contains overrides that are used by all modules of **T24**.

The *OVERRIDE* application will eventually supersede the *OVERRIDE.CLASS* application. A utility is provided to convert existing *OVERRIDE.CLASS* records into the appropriate *OVERRIDE* records. The utility is called *CONV.OVERRIDE.CLASS.G10.2*, and is run by verifying the *CONVERSION.DETAILS* record. The utility can be re-run multiple times.

For each *OVERRIDE*, the associated *OVERRIDE.CLASS* and *OVERRIDE.CLASS.DETAILS* information is entered for each application. The wildcard character (\*) is used to define all other applications that are not specifically defined.

The DISPO.ALLOWED field on the *OVERRIDE* records specifies if a given *OVERRIDE* is available for use with the DISPO system. Where set, the DISPO field accepts input and when an *OVERRIDE* is raised from the application a *DISPO.ITEM* record will be created.

#### Conditional Processing - CONDITIONAL.OVR

Some Dispo Overrides are dependent on other Dispo Overrides. For example, if a Funds Transfer transaction causes an account to go into overdraft and there is also a limit override, then both overrides are for Dispo processing. But if the account is not overdrawn, then the limit override is not for Dispo processing. The limit override is dependent/conditional on the overdraft override being present.

#### Transaction Indicator - TRANSACTION. IND

This field specifies if the *TRANSACTION* file needs to be checked to see if the transaction is exempt from Dispo processing. If YES is found in this field then the DISPO.EXEMPT field on the *TRANSACTION* file is checked. If the DISPO.EXEMPT field contains YES then the transaction is exempt from Dispo processing, and no further Dispo processing takes place. If DISPO.EXEMPT field contains NO then normal Dispo Override processing takes place.

#### **Precedence Processing** – PRECEDENCE

This signifies the order in which applications need to be checked and the field used to determine which *DISPO.OFFICER* the override must be routed to.

The syntax for each of the values in this field is as follows: *APPLICATION*>FIELDNAME



Where:

APPLICATION	The name of the APPLICATION to check
>	Separator
FIELDNAME	The name of the field containing DISPO Officer within the APPLICATION

APPLICATION is limited to the application specified in the APPLICATION field on the override table, *ACCOUNT*, *CUSTOMER*, *LIMIT* and *POSTING.RESTRICT* applications.

When the search fails to locate a *DISPO.OFFICER* in the **PRECEDENCE** list the *DISPO.OFFICER* on the Override record is used as the default *DISPO.OFFICER*.



#### **DISPO.PARAMETER**

This application stores settings for Dispo processing.

Only two fields are required in the *SYSTEM* record. The fields are:

#### OFS.SOURCE.ID - OFS Source Id.

When a contract is created in a multi-company environment in one company, and then Dispo items APPROVED in another company, an OFS message is created which authorises the original contract.

This field specifies the *ID* of a record in the *OFS.SOURCE* table that has been set up for BATCH processing. The Dispo System uses this data to locate the directory where the OFS message needs to be created.

Should this field not be defined at an instance of an OFS message needing to be created, a warning message is displayed requesting that the user changes company in order for the contract to be authorised.

#### DEFLT.CUR.DISP.OFF - Default Current Dispo Officer

Default current Dispo officer that **T24** uses to replace the Dispo officer, if all items on a Dispo Items record have been APPROVED.

🛎 DISPO Parameter table - Microsoft Internet Explorer	_ 🗆 🔀
DISPO.PARAMETER SYSTEM	
Ofs Source Id GCS Defit Cur Disp Off 1000 Reserved10 Reserved9 Reserved8 Reserved7	~
🕘 200606 - 1.6/060607   S.DONEY   Temenos 🛛 🛛 😒 Local intranet	

Figure 41 DISPO.PARAMETER record



#### **DISPO.OFFICER**

The *DISPO.OFFICER* file allows a hierarchy of officers to be defined that can approve overrides and the amounts that the officer can approve (the OVERDRAFT.AMT). The DISPO.AMOUNT field specifies the amount up to which the *DISPO.OFFICER* is able to make a comment, before routing the item for the attention of another officer.

In the event that a *DISPO.OFFICER* is unavailable for a period of time, messages can be routed to alternative officers for the duration of the period. The field ROUTE.TO is used to specify which officer messages are to be routed to. The DATE.FROM, DATE.TO, TIME.FROM, TIME.TO fields specify the period that the *DISPO.OFFICER* is unavailable for.

Automatic and manual routing is covered later in the guide.

Image: Construction of the image: Con	DISPO.OFFICER - Microsoft Internet Explorer	_ 🗆 🗙
GB Short Title Accounts Supervisor Override Id.1 ACCOUNT.INACTIVE Dispo Amount.1 Overdraft Amt.1 Next Dispo Off.1 Route To Date From Date To Time From Time From Time To Promeut	DISPO.OFFICER	^
Date From Date To Time From Time To	GB Short Title Accounts Supervisor   Override Id.1 ACCOUNT.INACTIVE   Dispo Amount.1 Image: Comparison of the second	Ш
Reserved6 Reserved5	Date From Date To Time From Time To Reserved7 Reserved6 Reserved5	~

Figure 42 DISPO.OFFICER record



### **ACCOUNT & CUSTOMER**

Both *ACCOUNT* and *CUSTOMER* may be linked to the *DISPO.OFFICER* table. The fields that are used and their meanings are detailed in this table:

Field	Table	Usage
DISPO.OFFICER	CUSTOMER and ACCOUNT	The officer who has the overall responsibility for the <i>ACCOUNT</i> or <i>CUSTOMER</i> . Where there is no <i>DISPO.OFFICER</i> specified at the <i>ACCOUNT</i> level, then the officer at the <i>CUSTOMER</i> level will be used instead.
STOP.OFFICER	ACCOUNT	The DISPO.OFFICER who is the responsible party for handling stopped cheques. When a STOP.OFFICER has not been defined then the one used on <i>ACCOUNT</i> takes precedence.
XX <post.restrict< td=""><td>ACCOUNT</td><td>The <i>POSTING.RESTRICTION</i> that the officer in the field RESTRICT.OFFICER is responsible for.</td></post.restrict<>	ACCOUNT	The <i>POSTING.RESTRICTION</i> that the officer in the field RESTRICT.OFFICER is responsible for.
XX>RESTRICT.OFFICER	ACCOUNT	The <i>DISPO.OFFICER</i> who is the responsible party for the restrictions defined in the field POST.RESTRICT. When a RESTRICT.OFFICER has not been defined then the one used on <i>ACCOUNT</i> takes precedence.



### USER

The final stage of the installation is to link *USER* records to *DISPO.OFFICER* records, which is done in the *USER* application:

🕘 USER PROFIL	E - N	icrosoft Internet Explorer	
🔽 🖹? 💷 D		🗸 🕞 🕞 🧖 🔋 More Actions	▶
Dispo S.DONEY			
User Name	*	S.C.DONEY	
Override Class.1	FF	BM/V	
Override Class.2	FF	FORD	
Dispo Officer		1000 Payments Officer	
Dispo Rights.1	Ŧ	2000 Accounts Supervisor	
Sign On Item.1	<b>+</b>		
Sign Off Item			
Process Dept.1	Ŧ	010	
200606 - 1.6/06	0607	S.DONEY   Temenos Bank   07-5E	Signal Local intranet

Figure 43 Linking USER records to DISPO.OFFICER records



### **Using Intelligent Overrides**

When an *OVERRIDE* is encountered which is flagged for Dispo processing for the application that raised the *OVERRIDE* (as defined in the *OVERRIDE* table), a *DISPO.ITEM* record will be produced for the contract. Whilst this item is in effect with a status of NEW, the contract may only be authorised by a *USER* whose DISPO.OFFICER (set on the *USER* profile) matches that of the item.

The *DISPO.SUMMARY ENQUIRY* displays, for each *DISPO.OFFICER*, the number of items pending both for today, and for previous days.

🐔 Dispo Item Summary - Microsoft Internet Explorer 📃 🗖						- 🗆 🗙	
Page 1 🔽 🖂 💌 💽 🕨 ፤						~	
ľ	Officer	Name	Total Items	Today's Items	Pending Items		)
	1000	Payments Officer	1	1		See Todays Items	
	1100	Lending Officer	1	1		See Todays Items	
							~
	ど 200606 - 1.6/060607   S.DONEY   Temenos Bank   I						::

Figure 44 Dispo Summary Enquiry

From this *ENQUIRY*, the *USER* may choose to show the details of today's items for a particular officer, or for the previous days. This invokes the *DISPO.DETAILS ENQUIRY* with the appropriate selection criteria.

The *ENQUIRY DISPO.DETAILS* provides a *USER* with information regarding overrides that require their attention.

4	🐔 Todays Dispo Items - Microsoft Internet Explorer						_ 🗆 🔀		
Page 1 🔽 🖂 💌 💽 🗈 👔						^			
	Todays Dispo Items t	for Officer :							≡
	Reference	Customer	Prev Dispo Off	Time	Ccy	Amount	Comment		
	FT0125000041*BNK	1035	Payments Officer	17:32	CHF			Add Comment	
Ļ							×		
1	🙆 200606 - 1.6/060607   S.DONEY   Temenos Bank   07-SEP-200:						anet ";;		

Figure 45 Dispo details enquiry



This is a real time enquiry. Refer to the *ENQUIRY* chapter of the System Administration User Guide for full details on installing and using real time enquiries.

To the user, this means that when an item becomes marked for their attention, the enquiry updates automatically.

From this *ENQUIRY*, the user may:

- Add a comment to the item and forward the item for the attention of another officer.
- Approve the item.
- View the item in full.

### Adding Comments to Dispo Items

Comments on a *DISPO.ITEMS* record can be used in two ways. The obvious one of making special notes on the record to record something but the more important usage in *DISPO.ITEMS* is for giving information to the next approver.

E DISPO.ITEMS - Microsoft Internet Explorer	_ 🗆 🔀
Jump to: DISPO.DETAILS >	~
🔽 ≌? 💷 🗙 📈 🖪 🕞 🕞 🖪 🖓 More Actions 💌 🅞	
Comments	
Pend Status :	
General Comments.1	
Item Text : .1 Account 18902 is inactive	
For the Attention of :	
Dispo Status * APPROVED 🗸	
Comments to be added by: 1010 Secondary Payments Officer	
Please check why this account is	
inactive.	
Add your Comments Here :	
	~
🕘 200606 - 1.6/060607   S.DONEY   Temenos Bank   07-SEP-2	net 🦽

Figure 46 Add a comment to a Dispo Item use DISPO.ITEMS, COMMENTS .

The COMMENT.OFFICER field is cleared, and the item is routed to the Supervisor.



It is quite normal in banking to seek an approval from a higher-ranking officer, for something like an overdraft, where a supervisor gathers any necessary information and confirms to the senior officer that the overdraft should be approved in this specific case as any necessary checks or controls have been made.

When a comment is processed in *DISPO.ITEMS* the comments are stored in the GENERAL.COMMENTS field and are appended with information on who created the comments.

🕘 DISPO. ITEMS - Microso	ft Internet Explorer		
	🕞 💽 🖪 🕐 More Actions	✓	<u>^</u>
Comments ET0125000041*BNK			
110123000041 BAIX			
Pend Status :	×		
General Comments.1	Please check why this account is		
General Comments.2	inactive.		
General Comments.3	1000*S.DONEY*17:53:11 16 JUN 2006		
Item Text : 1	Account 18902 is inactive		
For the Attention of :	1020 Deputy Payments Officer		
Dispo Status 🛛 🗶	APPROVED 💌		
Comments to be added by:	1010 Secondary Payments Officer		
		~	
Add your Comments Here :			
			~
🕙 200606 - 1.6/060607   S.DC	NEY   Temenos Bank   07-5EP-2001  35 📃 📃	Second Second Second Second	net 🙀

Figure 47 Adding more comments to DISPO.ITEMS record

Below the actual comments an audit type line is added which is comprised as follows:

#### DispoOfficer\*Operator\*DateTimeStamp

Dispo Officer	The Officer defined in the ${\tt DISPO.OFFICER}$	field on <u>USER</u> profile record.
Operator	The user that performed the update.	
DateTimeStamp	The date and time the update was made.	



### Manual Routing

There are two types of manual routing:

- Comment Routing
- Approval Routing

Comment routing allows multiple *DISPO.OFFICER* to comment on an item before it is routed to the *DISPO.OFFICER* to carry out the approval. It is the DISPO.OFFICER of the *DISPO.ITEMS* and not the COMMENT.OFFICER that controls which *USER* may approve an item.

Comment routing is achieved by entering a new *DISPO.OFFICER* into the COMMENT.OFFICER field on the *DISPO.ITEMS* 

Approval routing modifies the <u>USER</u> who may authorise the contract.

This is accomplished by modifying the DISPO.OFFICER field on the DISPO.ITEMS.

NB. The *DISPO.ITEMS* records may be updated only via a zero authoriser <u>VERSION</u>.



### **Automatic DISPO Routing**

Officer Code	Officer Description	Disposition Amount	Overdraft Competence	Next Level Disposition	of
1100	Account Office A	15,000	10,000	1101	
1101	Account Officer B	20,000	20,000	1105	
1105	Account Officer C	999,999,999,999	24,000		
2400	Top Management	0	999,999,999,999		

The examples are based on USD as the local currency, and the following information:

An overdraft excess of **USD 12,000** on a limit assigned to Loan Officer 1100 will be automatically routed to that Officer. The excess is lower than the Dispo amount of that Officer but higher than the Officer's competence amount. This officer can only route <u>manually</u> the transaction after having added their comments to the higher level of competence.

An overdraft excess of **USD 17,000** on a limit assigned to Loan Officer 1100 due to the fact that the excess is higher than the Dispo amount of this Officer will be automatically re-routed to the next disposition level => Officer 1101. This Officer has the competence to authorise the transaction.

An overdraft excess of **USD 27,000** on a limit assigned to Loan Officer 1100 due to the fact that the excess is higher than the Dispo amount of this Officer will be automatically re-routed to the next disposition level till the system finds the correct disposition officer => Officer 1105. This officer cannot approve the transaction because his competence level is lower than the overdraft excess. However, because of his Dispo limit, he receives this transaction to allow him to indicate his comments and forward the transaction to the Top Management for authorisation.

The overdraft is **USD 120,000**, but the limit of **USD 100,000** is not exceeded because the credit balance of **USD 50,000** from another account is being used to offset the debit balance. Should the credit balance be reduced below **USD 20,000** or removed from offsetting the facility, then overrides will be produced to alert the user that the limit will be exceeded.



# **Pending Status**

Each *DISPO.ITEMS* record has a Pending Status flag, which is stored in the field PEND.STATUS. This is used by T24 to determine which items are to be re-routed back to the officer that last had the item following overnight processing. If an item is held overnight, with this flag being set to NO or left empty, then the *DISPO.ITEMS* record will be reset to the first *DISPO.OFFICER* as per the parameters for Precedence processing, routing for unavailable *DISPO.OFFICER*, etc. If this flag is set to YES, then the *DISPO.ITEMS* record will not be altered.

# Tracking updates made to Dispo Items

Each time a *DISPO.ITEMS* record is updated the GEN.COMMENT field is updated with the contents of the COMMENTS field and the following details are appended:

The Dispo Officer that made the update, the User ID of the User that made the update, followed by the time and date that the update was made.

# Approving Dispo Overrides

When the input of a record causes an *OVERRIDE* and that *OVERRIDE* is marked for DISPO then a *DISPO.ITEMS* record is created. The status of each DISPO item on the record must be marked "APPROVED" before the originating record can be fully authorised. Only a *USER* who has a DISPO.OFFICER record with the application and appropriate competence will be able to approve a disco item.

Only after all the items within a *DISPO.ITEMS* record are approved, can the contract record be finally **A**uthorised. The normal rules for a USER's applications and *OVERRIDE.CLASS* apply.

The *DISPO.ITEMS* record may be updated only after all related non-dispo authorisations have taken place on the originating record.

In a multi-company environment it is possible for one of two paths to be followed during authorisation of a Dispo

Dispo can be configured to utilise OFS to perform final authorisation for all transactions that are created in remote Company accounts. The *SYSTEM* record in the *DISPO.PARAMETER* application contains a reference to an *OFS.SOURCE* record that has been set-up to run in BATCH mode. On approval of all Dispo Items within a *DISPO.ITEMS* record, an OFS message with an instruction to authorise the original contract is created.

The second path taken is when *DISPO.PARAMETER* application has not been configured and the original contract requiring authorisation is in a remote company. **T24** displays a message requesting that the user changes company to approve the Dispo.



## DISPO.ITEMS,COMMENTS – AUTH.ROUTINE field

The AUTH.ROUTINE field within the DISPO.ITEMS,COMMENTS version has been updated to action a BASIC subroutine called DISPO.NEXT.VERSION when a record has been committed using the DISPO.ITEMS,COMMENTS version.

The BASIC subroutine called **DISPO.NEXT.VERSION** has been supplied to:

#### For Multi company environments:

- Check if original contract needs to be authorised in a different company.
- If so, is it possible to generate an OFS message to complete the Authorisation?
- If it is not possible to generate an OFS message advise the user to change company to the company where the contract was originally created.

#### For Single company environments:

- Calculate the command required to complete authorisation of the original contract.
- Store the command in R.VERSION(EB.VER.NEXT.VERSION).
- T24 performs the command stored in: R.VERSION(EB.VER.NEXT.VERSION).

If it is not possible to create the OFS message, or the T24 environment is set up for Single Company only, calculate the command required to complete authorisation of the original contract.

The subroutine DISPO.NEXT.VERSION performs the following calculation when calculating the name of the version that is required to complete the authorisation of the original contract.

Can "Application, DISPO" version be found in VERSION table?

No? Can "Application," version be found in VERSION table?

No? Can "Application" version be found in VERSION table?

Once the version name is known, a command is constructed. This command is comprised of:

#### VersionName A OriginalContractId

VersionName The version that performs final authorisation of original contract.

A The Authorise function

*OriginalContractId* The Contract ID of the Original Contract.

A COMMON variable R.VERSION(EB.VER.NEXT.VERSION) is updated with the command to be performed. At this point no updates are made to the *VERSION* table.

Finally, T24 performs any command found in the COMMON variable R.VERSION (EB.VER.NEXT.VERSION).

Final authorisation can then be performed by viewing the original contract displayed, and committing the contract.

If the Application, DISPO VERSION record has the NEXT.VERSION field set to DISPO.ITEMS,COMMENTS, then once the contract has been authorised, the DISPO.ITEMS, COMMENTS window will be displayed ready for the next item.