Alcatel 1000 S12

OAM Documentation
OAM General Description
OD202

215 33267 AAAA TRMS Ed. 01

Status Released

Change Note

Short Title OD202

Contents

Figures

Tables

Preface

Este documento da uma visão global da **administração de acesso e registro** tal como é implementada nas centrais Alcatel 1000 S12.

O documento descreve as características básicas do tratamento de sessões e proteção de acesso para os distintos grupos de usuários.

São listados e descritos os comandos, da maneira mais usada pela administração de acesso e da função de registro.

A administração de acesso inclue tarefas sobre vários níveis de acesso:

- Gerência de senhas,
- Administração de usuários,
- Administração de identidades de usuários e seus perfis,
- Administração de grupos de usuários e seus perfis,
- Gestão do acesso aos comandos,
- Gestão do acesso aos dispositivos.

A administração de registro inclue as seguintes áreas:

- Controle da função de registro com inicialização, começo e fim,
- Manejo dos arquivos com dados de registro,

Objetivo deste Documento

Este tipo de documento proporciona um resumo detalhado das tarefas nos Manuais OAM Alcatel 1000 S12 .A administração de acesso e a administração da função de registro são tarefas que correspondem principalmente aos gerenciadores do sistema. Este documento contém um resumo das tarefas e funções da área:

"Administração de Acesso e Registro"

e dá informação detalhada sobre os comandos e procedimentos associados a esta área.

Cada capítulo esta proporciona exemplos típicos dos comandos pertencentes à área funcional descrita. Estes exemplos ajudam o usuário a familiarizar-se com o manuseio dos comandos e parâmetros associados.

Os exemplos dados neste documento podem diferir dos encontrados em condições reais de operação, pois estes dependem das configurações do equipamento.

Quem deve ler este Documento

Este manual deverá ser lido pelo pessoal responsável pela gestão das tarefas OAM de operação em "Modo-Direto" do Alcatel 1000 S12 .

Documentação Relacionada

Para maiores informações sobre um tópico específico, por favor consultar a seguinte documentação:

- *Guia do Usuário CHM da Documentação do Cliente,*
- *Manual de Informação Suporte de Documentação do Cliente,*
- *Manual de Informes de Saída de Documentação do Cliente.*

Convenções Tipográficas

Courier	Esta fonte é usada para mostrar exemplos de diálogos/monólogos.
negrito	Esta fonte é usada para marcar palavras e frases importantes.
Restrições	As restrições são apresentadas em áreas separadas onde podem ser reconhecidas com facilidade.
Comandos e Parâm.	A Tabela 1 mostra as principais convenções de escrita de comandos e de seus parâmetros que são utilizados neste documento e para entrada em modo-direto.

Tabela 1 Convenções de entrada

Símbolo		**como separador**	**como caractere de controle**
/* ..... */	Barra mais Asterisco	abre comentário .... fecha comentário	abre comentário .... fecha comentário
,	Vírgula	Separacão de parámetros	
:	Dois pontos	Fim do nome do comando	
=	Sinal igual	Atribuir valor a parâmetro	
&	Ampersand	Separação de argumentos dentro de um parâmetro	
&&	Duplo ampersand	Separação de argumentos que formam um intervalo	
-	Travessão	Separação de identificadores de uma característica	

Símbolo		como separador	como caractere de controle
’	Apóstrofe	Separação do indicador de base do valor	
”	Aspas	Límite de uma cadeia de texto (a passar ao usuário)	
()	Parênteses	Limitação (abertura e fechamento) de mnemônicos de substituição de texto	
?	Sinal de Interrogação		Petição de validamento
;	Ponto e vírgula		Verificar, executar, terminar sessão
$	Sinal do Dólar		Ignorar entrada até o caracter de tomada de controle introduzir antes
!	Sinal de exclamação		Verificar, executar, continuar
.	Ponto		Comprovar, executar, continuar, entrada novas características
CAN	Control-X		Cancelar e abortar o diálogo atual
BS	Apagar Caracter (Back Space)		Apagar o caracter anterior

Este ícone indica a **entrada de um comando MMC** dentro de um exemplo

Este ícone indica o **informe de saída** dentro de um exemplo.

1 Conceitos Básicos e Definições

Este capítulo introduz as características básicas do manejo de sessões e administração de acesso. Descreve seus elementos, funções e define os termos chaves.

Os tópicos deste capítulo são:

- o conceito de sessão
- os diferentes tipos de acesso e como são protegidos
- descrição dos grupos de usuários ’operador normal’, ’operador de segurança’, e ’gerência do sistema’
- o procedimento a ser executado no estabelecimento de conexão.

1.1 Tratamento de Sessões

As conexões do operador são das poucas ações de uma **sessão**, que permanece ativa até ser iniciada a desconexão. A sessão é tratada por meio do Tratamento de Sessões: testa e controla a conexão, e também compreende o tratamento dos comandos CHM introduzidos e a desconexão do operador.

1.2 Proteção de Acesso: Características e Implementação

Para prevenir um acesso não autorizado, a central tem uma proteção no sistema:

- Para iniciar uma sessão (’conexão’), o operador deve introduzir sua **identidade de usuário** e **senha.**

  As identidades de usuários acabam sendo bloqueadas quando o sistema recebe de forma repetida um número de conexões não válidas.

  As senhas expiram depois de um tempo (normalmente depois de 28 dias) e devem ser definidas de novo.

Acesso do Usuário

- Cada identidade de usuário têm seu próprio **perfil de usuário**, onde são defidos seus direitos de acesso a uma central do S12. O Alcatel 1000 S12 pode manusear até 999 usuários por vez. Cada usuário tem um número sequencial na categoria 1001a1999, que é usado internamente como um índice e é chamado de **Identificador de senha Lógica (Logical Password Identifier) (LPI).** O LPI está associado ao grupo de usuários.
- Cada identidade de usuário é atribuída a um **grupo de usuários**. Na central pode haver 255 grupos de usuários diferentes, e cada um deles tem seu próprio **perfil de grupo.** O perfil de grupo especifica para seus membros, os direitos de acesso as áreas de comandos.

Acesso por senha

- A **senha** do usuário está relacionada com sua identidade de usuário particular.
- Cada identidade de usuário é atribuída a um **grupo de usuários**. Numa central pode haver 255 grupos de usuários diferentes, e cada um deles tem seu próprio **perfil de grupo.** Este perfil de grupo especifica para seus membros, os direitos de acesso às áreas de comandos.

  Para uso interno, a senha pode ser definida no formato gravado (6 a 12 caracteres) ou não gravado (1 a 8 caracteres) . A senha é verificada com a identidade de usuário atual e a hora de expiração. As senhas não podem ser visualizadas pois elas devem se manter secretas. Para maiores informações sobre os níveis de segurança das senhas consultar o capítulo 1.6 na página 23.

Acesso a Comandos

- Os comandos CHM estão agrupados e atribuídos dinâmicamente a uma das 128 **áreas de comandos.** Um comando pertence somente a uma área de comandos, sendo gerada esta atribuição pelo pessoal da segurança ou o gerenciador do sistema (ver definição no capítulo). Os direitos de acesso podem ser aplicados a uma ou várias áreas de comandos.

Acesso a Dispositivos

- O acesso do usuário às áreas de comandos é controlado pela identidade de usuário (ver também perfil de grupo). Dar o nome do usuário correto e a senha não são suficientes para introduzir com êxito um comando. O dispositivo CHM máquina usado para introduzir o comando deve proporcionar acesso também a essa área de comandos. É chamado de **acesso de dispositivo:** Mas os direitos de acesso atribuídos a dispositivos de entrada individuais são diferentes! Somente é aceito um comando se o usuário e o dispositivo garantirem o acesso à área de comandos envolvidos.

  Portanto, um comando de usuário pode ser aceito pelo sistema no terminal 1 mas não no terminal 2. No primeiro caso, tanto a senha do usuário e o dispositivo proporcionam acesso à área de comandos envolvidos. Entretanto, no terminal 2 o dispositivo não proporciona este acesso.

  Entretanto, um gerenciador do sistema, sempre pode executar qualquer comando a partir de qualquer dispositivo.

  Um dispositivo pode ser definido como de **acesso restrito (barred)**. Neste caso, a conexão é rejeitada, a menos que:

- o usuário seja um gereciador de sistema
- o usuário seja um ”gerente do terminal”
- o usuário seja um “operador de segurança” e especifique a característica ”sem verificação do operador de segurança”.

1.3 Tentativas de Acesso Não Autorizado

As tentativas de acesso ao sistema não autorizado são registrado. Está é uma função do **Registro.** Para maiores informações sobre o registro, ver o capítulo 9.

1.4 Opções de Bloqueio

Um usuário é bloqueado depois de um certo número de acessos inválidos, como é especificado em seu perfil de usuário, a menos que ele/ela seja:

- gerente do sistema
- usuário terminal
- operador de segurança com o indicador de 'bloqueio de operador de segurança' sendo falsa as características de usuário (ver capítulos 3.3 e 3.4)

São definidos quatro opções de bloqueio nas características de usuário:

- Usuário:
  um usuário é bloqueado e o contador de conexões inválidas é colocado em zero a cada 24 horas.
- Dispositivo:
  um dispositivo é posto em 'acesso restrito (barrded)' e o contador de conexões inválidas é colocado em zero a cada 24 horas.
- Conexão de usuário:
  ver opção de bloqueio para o usuário, mas o contador de conexões inválidas é colocado em zero depois de uma conexão bem sucedida.
- Conexão de dispositivo:
  ver opção de bloqueio para o dispositivo, mas o contador de conexões inválidas é colocado em zero depois de uma conexão bem sucedida.

1.5 Detalhes Sobre Grupos de Usuários

Geralmente podem se distinguir **três** tipos de grupos de usuários, cada um complementado com 'variantes':

- **'Operador Normal':**

  Segundo sua função, o operador normal tem somente acesso restringido às diferentes áreas de comandos, por ex. poderia modificar somente sua própria senha.

  Variantes:

  - O operador terminal se conecta ao S12 através de periféricos externos. Recebe um tratamento privilegiado do S12. Podem ser definidos vários usuários terminais.
  - O operador de Grupo de Comunicação de Negócios (Business Communication Group) (BCG) é conectado ao S12 por meio de uma linha RDSI. Ao conectar-se, o usuário BCG está sujeito a um controle específico de acesso ao BCG além da verificação normal.

- **'Operador de Segurança':**

  O operador de segurança é um operador especial, que tem acesso a comandos que não são acessíveis para os operadores normais.

  É responsável pela administração de acesso, pela administração das identidades de usuários, pode liberar senhas bloqueadas, pode modificar o perfil de um usuário e o perfil de um grupo de usuários.

  Podem ser definidos vários operadores de segurança numa central. O operador de segurança não pode acessar o sistema fora da hora permitida.

  Em uma central podem estar definidos vários operadores de segurança. Um operador de segurança somente pode ter acesso ao sistema durante o horário permitido. Um operador de segurança é identificado no **perfil de grupo** por meio do indicador de operador de segurança que deverá estar em ON.

  Existe algumas características especiais para o operador de segurança:

  - ele será bloqueado nos acesso ilegais a não ser que o indicador 'bloqueio do operador de segurança' esteja em OFF.

- ele não terá acesso a um dispositivo excluído não ser que o indicador 'verificação do operador de segurança' esteja em OFF.

Estes indicadores são encontrados nas características de usuário (mais detalhes ver os capítulos 3.4 e 3.5).

- **'Gerenciador de sistema':**

O gerenciador do sistema tem todas responsabilidade pelas operações da central. Nunca pode ser bloqueado e tem acesso a todos os dispositivos a qualquer momento, inclusive os dispositivos restringidos.

O gerente do sistema é responsável pela administração do acesso, das identidades de usuários, pode liberar senhas bloqueadas, modificar o perfil de um usuário e o perfil de um grupo de usuários. Entretanto, não pode trocar seu período de conexão e acesso a vacaciones.

Em uma central podem ser definidos vários gerente do sistema. É reconhecido pelo indicador de 'operador de segurança' no **perfil de usuário** e por 3 indicadores no **perfil de grupo**:

- permissão para modificar o perfil de um usuário
- permissão para modificar o perfil de um grupo de usuários.
- Indica no prefil de grupo

  Quando este indicador está instalado, o gerente do sistema pode adicionar e apagar áreas de comandos do perfil de grupo.

- indicador de operador de segurança.

O indicador 'troca o mapeamento do operador' nas características do usuário (ver capítulo 3.4) tem implicações sobre os seguintes separadores, no próprio perfil de usuário e perfil de grupo do gerenciador do sistema; se ele estiver indicado, o gerenciador do sistema tem permissão para modificar:

- o indicador de bloqueio no perfil de usuário
- o indicador de permissão no perfil de usuário e perfil de grupo
- o indicador de operador de segurança
- o acesso às áreas de comandos.

Resumindo: Se o indicador 'trocar o mapeamento do operador' estiver colocado, o gerente do sistema pode colocar os indicadores e realizar as ações mencionadas anteriormente, a não ser que conceda ao último grupo gerente de sistema. Se o indicador não está instalado, não será possível realizar as ações anteriores.

1.6 Níveis de Segurança das senhas

Há vários níveis de segurança para senhas. Um nível de segurança é atribuído a cada senha. Em ordem ascendente:

- Nenhuma verificação específica
- Verificação simples com
  - todos os caracteres devem ser diferentes
  - os caracteres não devem estar em ordem ascendente
  - os caracteres não devem estar em ordem descendente
- A senha deve incluir ao menos um caractere numérico
- A senha deve incluir ao menos um caractere especial (nem numérico nem alfabético)
- A senha não deve ser uma das cadeias de caracteres pré-definidas como proibido.

O nível superior de segurança mais próximo sempre cobre os níveis inferiores.

1.7 Procedimento de Verificação na Conexão

Verificação na conexão

Durante a conexão do usuário, o SW tratador de sessões contesta a veracidade da identidade do usuário e senhas introduzidas:

1. Existe o usuário?
2. O acesso do usuário está atualmente colocado no bloco negado? (p.ex. devido a demasiadas tentativas não válidas de conexão)
3. O dispositivo de entrada está atualmente excluído ou não? (por meio de um Comando Homem Máquina (Man Machine Command) (CHM))
4. Permite ao usuário a conexão no dia e hora mês?
5. Está o usuário já em uma sessão, o que significa que já está conectado ou não?
6. É permitido ao usuário se direcionar a central destino dada?
7. Concede o dispositivo de entrada acesso à central destino dada?
8. Quando se introduz um comando: Concede ao grupo de usuários - ao que pertence a identidade de usuário - acesso a área de comandos direcionada?

9. Se um gerenciador de BCG se conecta: O sistema verifica se o número de BCG corresponde com o usuário.

São feitas também as seguintes verificações:

- Permitir o dispositivo de entrada ou Manuseio de Sessões? (sim/não)
- É a senha introduzida na mesma entrada válida para a Identidade de Usuário?
- Foi expirado a senha introduzida ou não?
- Dependendo da tarefa dada: Conceda o dispositivo de entrada acesso a área de comandos direcionada?

1.8 FMMs Implicados no Tratamento de Sessões

As FMMs seguintes estão implicadas no tratamento de sessões de uma **sessão local que usa um enlace não binário:**

Ao receber um sinal de ruptura, o Manuseador de Arquivos de VDU (VDU File Handler) (VDUFH) comprovará o tipo de terminal na relação R_DV_CHAR para verificar se o terminal é do tipo ”sessão” ou não.

Se o terminal for do tipo ”sessão”, o VDUFH solicita a cadeia de caracteres do usuário>.

Depois que o usuário for introduzido na identidade de usuário, o VDUFH solicita a cadeia de caracteres PASSWORD>.

Depois que o usuário for introduzido na senha, o VDUFH envia uma mensagem de conexão ao Supervisor de Tratamento de Sessões (FMM SESS).

A FMM SESS leva a cabo algumas verificações básicas, cria uma aplicação, envia uma resposta ao VDUFH indicando seu processo de aplicação, verifica todas as restrições a serem aplicadas na senha e envia uma mensagem FMM Diálogo CHM (FMM MMCD) para informar da sessão de usuário que está a caminho.

A FMM MMCD encabeça o diálogo, enviando uma mensagem à Aplicação do Tratamento de Sessões (FMM SESA), cria um processo de aplicação e informa à FMM SESA que já está na lista para a entrada do comando.

A FMM SESA transfere a mensagem anterior, a resposta textual ao VDUFH. O VDUFH mostra ao operador, pedindo que introduza um comando. Neste momento, o usuário se conecta e o operador pode introduzir comandos CHM, até que inicie sua desconexão.

A VDUFH passa os comandos introduzidos à FMM SESA, junto com a mensagem ”comandos de sessão de usuário”.

Cada vez que a FMM SESA recebe comandos, é iniciada a FMM MMCD como se estivesse estabelecendo uma nova sessão já que a FMM SESA não conhece nada de sessões.

Quando o operador inicia a desconexão VDUFH envia uma mensagem de desconexão à FMM SESA , que a troca e envia um comando que indica ”abortar” à FMM MMCD para força terminar sua aplicação. Logo, a FMM SESA coloca o usuário como ”não conectado” e devolve uma mensagem de reconhecimento ao VDUFH.

1.9 Definições

Acesso a comandos O acesso a comandos resume os direitos de acesso às áreas de comandos; o acesso a comandos atribuídos a um usuário normal é definido pelo perfil do grupo de usuários.

Para que uma área concreta de comandos seja acessível ou não,via um dispositivo dependerá do acesso de dispositivo, que é atribuído ao dispositivo de entrada.

Área de comandos As áreas de comandos são grupos de comandos CHM. Cada comando CHM é atribuído a uma das 128 áreas de comandos.

Acesso de dispositivos O acesso de dispositivo resume os direitos de um dispositivo CHM-Máquina para ter acesso às áreas de comandos. Um dispositivo pode ser colocado como de 'acesso excluído'. Neste caso, já não se aceitarão mais comandos de qualquer usuário normal.

Perfil de grupo O perfil de grupo é o resumo das características que são atribuídas a um grupo de usuários. Também estabelece a que áreas de comandos o grupo de usuários tem acesso.

Registro Esta função registra os eventos da central e as reporta em forma de mensagens escritas nos arquivos do usuário.

MPTMON O MPTMON é a abreviatura de Monitor de testes MultiProcesso, é uma ferramenta de testes usadas para obter acesso e operar uma central Alcatel 1000 S12.

Grupo de usuários Cada usuário é atribuído a um grupo de usuários. Existem 255 grupos de usuários distintos numa central. Os usuários de um grupo de usuários simples tem atribuídas as mesmas características.

Distinguimos três tipos gerais de grupos de usuários:

- operador normal
- operador de segurança
- gerente do sistema

Identidade de usuário A identidade do usuário é uma cadeia de caracteres alfanuméricos, reservada para um usuário. A identidade do usuário é apresentada pelo usuário ao sistema e depois é utilizado pelo sistema para identificá-lo.

Perfil de usuário O perfil de usuário é o resumo das características atribuídas a ele.

2 Gerenciamento de Senhas

Este capítulo mostra o tratamento básico de senhas. Descreve os comandos mais frequentemente utilizados, ilustrados com exemplos. Os comandos selecionados, tratam das seguintes tarefas:

- Exibir e modificar a própria senha
- modificar a senha de outro usuário (somente para operadores de segurança)

O capítulo1 apresenta a informação detalhada sobre os conceitos básicos e definições dos termos especiais.

2.1 Tarefas e Referências

Neste capítulo são descritos os comandos para gerenciar as senhas.

Os exemplos aqui proporcionados não incluem todos os possíveis parâmetros para cada um dos comandos. Consultar o correspondente Procedimento Detalhado se desejar informações completas.

A tabela 2 contêm uma lista de referências dos documentos de manuais de Operação e Manutenção apresentados neste capítulo.

Tabela 2 Comandos, CRN e documentos relacionados com o gerenciamento de senhas

Tarefa	Comando-CHM	CRN	Documento
Modificar a Própria Senha	MODIFY-OWN-PSW	04815	DP04815
Exibir o Próprio Perfil	DISPLAY-OWN-PROFILE	04811	DP04811

2.2 Modificar a Própria Senha

Descrição Depois de um certo tempo, a senha do usuário expira e o usuário deve estabelecer uma nova senha. Também pode desejar estabelecer uma nova senha, mesmo não tendo expirado a senha anterior. A nova senha sustituirá a antiga.

Nota A nova senha introduzida deve ser diferente das três últimas, pois mostrará uma mensagem de erro. A senha é comprovada de acordo com o nível de segurança (especificado nas características do usuário)

Tabela 3 MODIFY-OWN-PASSWORD (CRN 04815)

Comando Introduzido	Significado
<MODIFY-OWN-PSW:	
<OLDPSW="USER900",	senha antiga
<NEWPSW="MART0001",	nova senha
<CONFPSW="MART0001".	confirmar senha (repetir a nova senha)

```
MODIFY-OWN-PSW                                                    COM ÊXITO
-------------------------------------------------------------------------

USUARIO  :  USER900

CLAVE HA SIDO MODIFICADA CON EXITO

ULTIMO INFORME   =    04673
```

2.3 Exibir o Próprio Perfil

Descrição Usar este comando para visualizar o próprio perfil de usuário.

De acordo com o conteúdo das relações da base de dados, o usuário obtêm um informe de saída onde é mostrado uma visão total ou parcial de seu perfil com:

- Usuário
- LPI (índice numérico dado a cada Usuário)
- Grupo de Usuários
- Linguagem de Usuário
- Indicativo de operador de segurança: para gerenciadores do sistema e operadores de segurança.
- Dias que restam para expirar a senha, etc.

Tabela 4 DISPLAY-OWN-PROFILE (CRN 04811)

Comando Introduzido	Significado
<DISPLAY-OWN-PROFILE.	só o comando, não necessita parâmetros adicionais

```
DISPLAY-OWN-PROFILE                                              CON EXITO
------------------------------------------------------------------------

USERID                                  : USER900
LPI                                     : 1901
NUMERO DE GRUPO DE USUARIO              : 32
TIPO DE GRUPO DE USUARIO                : NORMAL
IDIOMA DE USUARIO                       : ESPANOL
DIAS ANTES DE QUE EXPIRE LA CLAVE       : 0
DIAS TOTALES EN QUE LA CLAVE ES VALIDA     : 0
ENTRADAS NO VALIDAS REGISTRADAS         : 0
MAXIMAS ENTRADAS NO VALIDAS PERMITIDAS : 3
ACESSOS NO VALIDOS REGISTRADOS          : 0
MAXIMOS ACCESOS NO VALIDOS PERMITIDOS   : 0
USUARIO ACTIVO                           : NO ENTRADO  AND
                                        : NO BLOQUEADO

ESTE USUARIO ES UN OFICIAL DE SEGURIDAD
```

3 Administração de Usuários

Este capítulo mostra o tratamento básico da administração de usuários. Descreve os comandos mais frequentemente utilizados ilustrados com os exemplos. Os comandos aqui agrupados, tratam as seguintes tarefas:

- exibir os usuários ativos
- exibir e modificar as características dos usuários.

  Estas características definem como são tratados os usuários, como são verificados seus acessos e como são tratados as tentativas ilegais ou não válidas.

Podemos encontrar informações mais detalhadas sobre os conceitos básicos e definições de termos especiais no capítulo 1.

3.1 Tarefas e Referências

Neste capítulo são descritos os comandos para se modificar as características dos usuários.

Os exemplos a seguir não proporcionaram todos os possíveis parâmetros para cada um dos comandos. Consultar o correspondente Procedimento Detalhado se desejar informações mais completas.

A tabela 5 contêm uma lista de referências a outros documentos, úteis nos manuais de Operação e Manutenção representados neste capítulo.

Tabela 5 Comandos, CRN e documentos relacionados com a administração de usuários

Tarefa	Comando-CHM	CRN	Documento
Visualizar Usuários Ativos	DISPLAY-ACTIVE-USERS	05855	DP05855
Visualizar Características de um Usuário	DISPLAY-USER-FEATURES	05875	DP05875
Modificar Características de um Usuário	MODIFY-USER-FEATURES	05876	DP05876

3.2 Exibir Usuários Ativos

Descrição Usa-se este comando para visualizar todos os usuários que estão atualmente conectados. Para cada usuário conectado é mostrado:

- identidade do usuário
- LPI
- grupo de usuários
- identidade do dispositivo físico onde o usuário está atualmente conectado.

Tabela 6 DISPLAY-ACTIVE-USERS (CRN 05855)

Comando Introduzido	Significado
<DISPLAY-ACTIVE-USERS.	não requerer mais parâmetros

```
DISPLAY-ACTIVE-USERS                                          CON EXITO
------------------------------------------------------------------------

LOS USUARIOS SEGUIENTES ESTAN ACTIVOS :

NING

ULTIMO INFORME   =    05568
```

3.3 Exibir Características do Usuário

Descrição: Usa-se este comando para visualizar todas as possíveis características de usuário tais como são definidas na correspondente relação da base de dados. As características definem o tratamento dos usuários, especialmente verificar seus acessos e o tratamento das tentivas de acesso ilegais ou não válidas.

Tabela 7

DISPLAY-USER-FEATURES (CRN 05875)

Comando Introduzido	Significado
<DISPLAY-USER-FEATURES.	não requer nenhum parâmetro

```
DISPLAY-USER-FEATURES                                          CON EXITO
------------------------------------------------------------------------

BLOQUEAR OPCION          : ENTRUSR
CLAVES ENCRIPTADAS       : NO
CHEQUEAR OFICIAL SEGUR   : NO
BLOQUEAR OFICIAL SEGUR   : NO
CAMBIAR MAPA OFICIALES   : SI
INFORME ACCESO ILEGAL    : SI
ENVIAR INFORME AVISO     : NO
VISTA CARACTERIST        : LLENO
PERIODO TIEMPO SALIDA    : 59  M
CLAVE UNICA              : NÃO
GRUPOS DE USR MAXIMO     : 255
TIPO DE CENTRAL          : SKR74
LENGUAJE MMC             : ESPANOL
LONGITUD NIVEL CLAVE     : SI
                CARAC    : SI
                SIMPLE   : SI
                NUMERO   : SI
               ESPECIAL  : NO
                SUB STR  : NO

ULTIMO INFORME   =    05535
```

3.4 Modificar Características de Usuário

Descrição Usa-se este comando para modificar algumas características de usuário do sistema e assim alterar os dados na relação correspondente da base de dados.

Podem ser modificadas uma, várias ou todas as características seguintes:

- Tempo de desconexão

  Especifica o tempo de inatividade antes de desconectar de forma automática um usuário conectado.

- Opção de bloqueio

  Este parâmetro define se o usuário ou o dispositivo que está sendo utilizado poderá ser bloqueado quando o número de tentativas de acessos ilegais superar um limiar.

- Bloqueio do operador de segurança

  Este parâmetro define se o operador de segurança deve ser bloqueado ou não, quando o número de acessos ilegais superar um limiar.

- Possibilidade de modificar o mapa de acesso pelo operador de segurança

  Este parâmetro define se tal modificação é possível ou não.

Tabela 8 MODIFY-USER-FEATURES (CRN 05876)

Comando Introduzido	Significado
<MODIFY-USER-FEATURES:	
<LOGOFTIM=30**.**	tempo de desconexão

```
MODIFY-USER-FEATURES                                              CON EXITO
------------------------------------------------------------------------

     ANTIGUO                              NUEVO

BLOQUEAR OPCION          : ENTRUSR   BLOQUEAR OPCION          : ENTRUSR
CLAVES ENCRIPTADAS       : NO        CLAVES ENCRIPTADAS       : NO
CHEQUEAR OFICIAL SEGUR   : NO        CHEQUEAR OFICIAL SEGUR   : NO
BLOQUEAR OFICIAL SEGUR   : NO        BLOQUEAR OFICIAL SEGUR   : NO
CAMBIAR MAPA OFICIALES   : SI        CAMBIAR MAPA OFICIALES   : SI
INFORME ACCESO ILEGAL    : SI        INFORME ACCESO ILEGAL    : SI
ENVIAR INFORME AVISO     : NO        ENVIAR INFORME AVISO     : NO
VISTA CARACTERIST        : LLENO     VISTA DE CARACTERIST     : LLENO
PERIODO TIEMPO SALIDA    : 59  M     PERIODO TIEMPO SALIDA    : 30  M
CLAVE UNICA              : NO        CLAVE UNICA              : NO
GRUPOS DE USR MAXIMO     : 255       GRUPOS DE USR MAXIMO     : 255
TIPO DE CENTRAL          : SKR74     TIPO DE CENTRAL          : SKR74
LENGUAJE MMC             : ESPANOL   LENGUAJE MMC             : ESPANOL
LONGITUD NIVEL CLAVE     : SI        LONGITUD NIVEL CLAVE     : SI
               CARAC     : SI                         CARAC     : SI
               SIMPLE    : SI                         SIMPLE    : SI
               NUMERO    : SI                         NUMERO    : SI
             ESPECIAL    : NO                       ESPECIAL    : NO
               SUB STR   : NO                         SUB STR   : NO

   ULTIMO INFORME   =    05535
```

4 Administração de Identidades de Usuário e Perfís de Usuário

Este capítulo mostra o tratamento básico da administração das identidades de usuários e perfis de usuários. Descreve os comandos mais frequentemente utilizados, ilustrados com exemplos. Os comandos aqui agrupados, tratam das seguintes tarefas:

- Exibir e modificação das identidades de usuário e os perfis de usuário.

Em geral, só aos operadores de segurança é permitido executar estes comandos.

Podemos encontrar informações mais detalhadas sobre os conceitos básicos e definições de termos especiais no capítulo 1.

4.1 Tarefas e Referências

Neste capítulo são descritos os comandos para administração das identidades de usuário e perfis de usuário.

Os exemplos a seguir não proporcionam todos os possíveis parâmetros para cada um dos comandos. Consultar o correspondente Procedimento Detalhado se desejar informações mais detalhadas.

A tabela 9 contém uma lista de referências a outros documentos úteis nos manuais de Operação e Manutenção apresentados neste capítulo.

Tabela 9 Comandos, CRN e documentos relacionados com a administração de identidades de usuário e perfil de usuário

Tarefa	Comando-CHM	CRN	Documento
Visualizar Perfil de Usuário	DISPLAY-USER-PROFILE	04812	DP04812

4.2 Exibir Perfil de Usuário

Descrição: Usar este comando para visualizar o perfil de um usuário especificado por sua identidade de usuário **ou** identificação de senha lógica (LPI).

Um informe de saída mostra uma visão completa ou parcial de seu perfil.

Tabela 10 DISPLAY-USER-PROFILE (CRN 04812)

Comando Introduzido	Significado
<DISPLAY-USER-PROFILE:	
<USERID="USER900"**.**	identidade do usuário

```
DISPLAY-USER-PROFILE                                          CON EXITO
------------------------------------------------------------------------

USERID    :  USER900

USERID                                  : USER900
LPI                                     : 1901
NUMERO DE GRUPO DE USERID               : 32
TIPO DE GRUPO DE USERID                 : NORMAL
IDIOMA DE USERID                        : ESPANOL
DIAS ANTES DE QUE EXPIRE LA CLAVE       : 0
DIAS TOTALES EN QUE LA CLAVE ES VALIDA  : 0
ENTRADAS NO VALIDAS REGISTRADAS         : 0
MAXIMAS ENTRADAS NO VALIDAS PERMITIDAS  : 3
ACCESOS NO VALIDOS REGISTRADOS          : 0
MAXIMOS ACCESOS NO VALIDOS PERMITIDOS   : 0
USERID ACTIVO                           : NO ENTRADO  AND
                                        : NO BLOQUEADO

ESTE USERID ES UN OFICIAL DE SEGURIDAD

ULTIMO INFORME   =    04672
```

Tabela 11 DISPLAY-USER-PROFILE (CRN 04812)

Comando Introduzido	Significado
<DISPLAY-USER-PROFILE:	
<LPI=1901**.**	identificação de senha lógica

```
DISPLAY-USER-PROFILE                                          CON EXITO
------------------------------------------------------------------------

LPI      :  1901

USERID                                 : USER900
LPI                                    : 1901
NUMERO DE GRUPO DE USERID              : 32
TIPO DE GRUPO DE USERID                : NORMAL
IDIOMA DE USERID                       : ESPANOL
DIAS ANTES DE QUE EXPIRE LA CLAVE      : 0
DIAS TOTALES EN QUE LA CLAVE ES VALIDA : 0
ENTRADAS NO VALIDAS REGISTRADAS        : 0
MAXIMAS ENTRADAS NO VALIDAS PERMITIDAS : 3
ACCESOS NO VALIDOS REGISTRADOS         : 0
MAXIMOS ACCESOS NO VALIDOS PERMITIDOS  : 0
USERID ACTIVO                          : NO ENTRADO  AND
                                       : NO BLOQUEADO

ESTE USERID ES UN OFICIAL DE SEGURIDAD

ULTIMO INFORME   =    04672
```

5 Administração de Grupos de Usuários e Perfil de Usuário

Este capítulo mostra o tratamento básico da administração de grupos de usuários e perfil de usuários. Descreve os comandos mais frequentemente utilizados, ilustrados com os exemplos. Os comandos aqui agrupados tratam das seguintes tarefas:

- Exibição e modificação do perfil de usuário e do grupo de usuários especificado.

O grupo de usuário estabelece,

- que usuários pertencem a um grupo de usuários
- que direitos de acesso são atribuídos ao grupo de usuários
- que áreas de comandos são acessíveis para um grupo de usuários.

Em geral só operadores de segurança são autorizados a executar estes comandos os .

Podemos encontrar informações mais detalhadas sobre os conceitos básicos e definições de termos especiais no capítulo 1.

5.1 Tarefas e Referências

Neste capítulo são descritos os comandos para administração das identidades de usuário e perfil de usuário.

Os exemplos a seguir não proporcionam todos os possíveis parâmetros para cada um dos comandos. Consultar o correspondente Procedimento Detalhado se desejar informações mais detalhadas.

Na tabela 12 contêm uma lista de referências a outros documentos úteis nos manuais de Operação e Manutenção.

Tabela 12 Comandos, CRN e documentos relacionados com a administração de grupos de usuários e perfis de grupo

Tarefa	Comando-CHM	CRN	Documento
Visualizar Perfil de Grupo	DISPLAY-GROUP-PROFILE	04813	DP04813

5.2 Exibir Perfil de Grupo

Descrição: Só para operadores de segurança. Usa-se este comando para visualizar

- o perfil do grupo de usuários especificado
- quais áreas de comandos são acessíveis para o grupo de usuários
- quais usuários pertencem ao grupo de usuários especificado.
- no caso de um grupo de operador de segurança : se o indicativo de operador está instalado ou não.
- no caso de um grupo de gerente do sistema : se o indicativo de operador está instalado, assim como a permissão para modificar perfil do usuário e perfil de grupo.

Tabela 13 DISPLAY-GROUP-PROFILE (CRN 04813)

Comando Introduzido	Significado
<DISPLAY-GROUP-PROFILE:	
<USERGRP=2,	número dol grupo de usuários
<ALLUSERS.	todos os usuários do grupo de usuários

```
DISPLAY-GROUP-PROFILE                                              CON EXITO
------------------------------------------------------------------------------

GRUPO    :  2
TODOS LOS USUARIOS

USUARIOS ASIGNADOS A ESTE GRUPO              :

 USERNBR    USERID       USERNBR    USERID       USERNBR    USERID
------------------------------------------------------------------------
 1021       USER020      1022       USER021      1023       USER022
 1024       USER023      1025       USER024      1026       USER025
 1027       USER026      1028       USER027      1029       USER028
 1030       USER029

ULTIMO INFORME   =    04675
```

Tabela 14 DISPLAY-GROUP-PROFILE (CRN 04813)

Comando IntroduZido	Significado
<DISPLAY-GROUP-PROFILE:	
<USERGRP=2**.**	número do grupo de usuários

```
DISPLAY-GROUP-PROFILE                                              CON EXITO
------------------------------------------------------------------------------

GRUPO   :  2

NOMBRE GRUPO  : GRUPO_002

PERMITIDO ACCESO PERM :
INICIO  HORA, MINUTO    FINAL HORA,MINUTO    PSW DISTR
          7&0                  18&0            ON

PERMITIDO MODIFICAR/ACCEDER Y CARACTERISTICAS

  DOS ATOM     USR-PROF   GRP-PROF   OFFICER   VACAC     TML

      NORMAL      N          N          N      N  (DO)     N

GRUPO USUARIOS PUEDE ACCEDER A LAS AREAS         :

  2    3    4    5    6    7    8    9    10   11
  12   13   14   15   16   17   18   19   20   21
  22   23   24   25   26   27   28   29   30   31
  32

GRUPO USUARIOS PUEDE ACCEDER LAS AREAS         :

  2    3    4    5    6    7    8    9
  10   11   12   13   14   15   16   17
  18   19   20   21   22   23   24   25
  26   27   28   29   30   31   32

ULTIMO INFORME   =    04675
```

6 Gerência do Acesso aos Comandos

Os comandos CHM estão agrupados em áreas de comandos. Este capítulo mostra o tratamento básico, como gerenciar o acesso aos comandos. Descreve os comandos mais frequentemente utilizados, ilustrados com exemplos. Os comandos aqui agrupados tratam das seguintes tarefas:

- visualização de seus próprios comandos CHM e aos de outro usuário
- visualização e modificação da atribuição de comandos CHM às diferentes áreas de comandos.

  Só aos operadores de segurança é permitido executar estes comandos.

Podemos encontrar informações mais detalhadas sobre os conceitos básicos e definições de termos especiais no capítulo 1.

6.1 Tarefas e Referências

Neste capítulo são descritos os comandos para o gerenciamento de acesso aos comandos ORJ.

Os exemplos a seguir não proporcionam todos os possíveis parâmetros para cada um dos comandos. Consultar o correspondente Procedimento Detalhado se desejar informações mais detalhadas.

A tabela 15 contém uma lista de referências aos documentos úteis nos manuais de Operação e Manutenção apresentados neste capítulo.

Tabela 15 Comandos, CRN e documentos relacionados com o gerenciador do acesso aos comandos

Tarefa	Comando-CHM	CRN	Documento
Exibir a Lista Própria de Comandos	DISPLAY-OWNCMD-LIST	05144	DP05144
Exibir Lista de Comandos	DISPLAY-COMMAND-LIST	04852	DP04852
Exibir o acesso aos Comandos	DISPLAY-COMMAND-ACCESS	07612	DP07612
Modificar o acesso aos Comandos	MODIFY-COMMAND-ACCESS	07613	DP07613

6.2 Exibir a Lista Própria de Comandos

Descrição Usa-se este comando para visualizar a lista própria de comandos CHM a que se tem acesso ao usuário. É mostrado o Número de Referência do Comando (Command Reference Number) (CRN) dos comandos CHM.

Tabela 16 DISPLAY-OWNCMD-LIST (CRN 05144)

Comando Introduzido	Significado
<**DISPLAY-OWNCMD-LIST.**	não se requer parâmetros

```
DISPLAY-OWNCMD-LIST                                              CON EXITO
                                              PARTE DE RESULTADO   0001 +
------------------------------------------------------------------------
 USERID : USER900                                 DEV : 00130/070F/00003

 00348 00498 00439 07682 08362 07655 06736 06430 00517 00149 07201
 05847 05905 01616 05767 01574 00128 00025 06597 00101 04224 06204
 01556 01532 01681 06223 05573 00001 05574 01679 01680 01677 01676
 *
 *
 *
 00083 00486 05114 05205 07504 07589 07934 04585 04579 04581 04583
 01547 07660 05580 05649 04382 05230 06549 00393 07281 04820 00793
 07606 05763 05982 05978 05941 06803 06185 00984 05651 08302 00985

SIGUE RESULTADO  =    04717
```

```
DISPLAY-OWNCMD-LIST                                              CON EXITO
                                              PARTE DE RESULTADO   0002 -
------------------------------------------------------------------------
 USERID : USER900                                 DEV : 00130/070F/00003

 06160 05535 04468 06282 04320 06141 00397 04214 04732 06478 04498
 05317 04006 04283 04497 07604 07602 05380 07600 07601 05332 04756
 04871 00226 00234 00249 04285 05184 06280 04787 04786 07735 01670
 *
 *
 *
 00038 00894 05673 00492 00011 06732 05244 01674 01342 04874 04952
 06405 07209 00039 00928 00287 07115 05598 06737 05610 06683 07638
 07637 07997 00412 01533 04938 07652 00014 00163 04220 06444 07199

ULTIMO INFORME   =    04717
```

6.3 Exibir Lista de Comandos

Descrição: Usa-se este comando para visualizar os comandos CHM a que tem acesso um usuário específico e o dispositivo de entrada indicados. Podem ser indicados até três dispositivos de entrada. São mostrados os números de referência de comando (CRN) dos comandos CHM.

Tabela 17 DISPLAY-COMMAND-LIST (CRN 04852)

Comando Introduzido	Significado
<DISPLAY-COMMAND-LIST:	
<USERID="USER900",	identidade do usuário
<DEV=130&H'2D&3**.**	identidade do dispositivo de entrada

```
DISPLAY-COMMAND-LIST                                          CON EXITO
                                              PARTE DE RESULTADO   0001 +
------------------------------------------------------------------------
 USERID : USER900                                DEV : 00130/002D/00003

 USERID PERTENCE A UN OFICIAL DE SEG - ACCESO DEL
 DISPOSITIVO NO CONSIDERADO!

 00348 00498 00439 07682 08362 07655 06736 06430 00517 00149 07201
 05847 05905 01616 05767 01574 00128 00025 06597 00101 04224 06204
 01556 01532 01681 06223 05573 00001 05574 01679 01680 01677 01676
 *
 *
 *
 00083 00486 05114 05205 07504 07589 07934 04585 04579 04581 04583
 01547 07660 05580 05649 04382 05230 06549 00393 07281 04820 00793
 07606 05763 05982 05978 05941 06803 06185 00984 05651 08302 00985

SIGUE RESULTADO  =    04717
```

```
DISPLAY-COMMAND-LIST                                              CON EXITO
                                              PARTE DE RESULTADO   0002 -
------------------------------------------------------------------------
 USERID : USER900                                 DEV : 00130/002D/00003

 06160 05535 04468 06282 04320 06141 00397 04214 04732 06478 04498
 05317 04006 04283 04497 07604 07602 05380 07600 07601 05332 04756
 04871 00226 00234 00249 04285 05184 06280 04787 04786 07735 01670
 *
 *
 *
 00038 00894 05673 00492 00011 06732 05244 01674 01342 04874 04952
 06405 07209 00039 00928 00287 07115 05598 06737 05610 06683 07638
 07637 07997 00412 01533 04938 07652 00014 00163 04220 06444 07199

ULTIMO INFORME   =    04717
```

6.4 Exibir do Acesso aos Comandos

Descrição Só para operadores de segurança. Usar este comando para visualizar a atribuição dos comandos CHM às diferentes áreas de comandos. 'Pode ser visualizado resultados de até 10 comandos CHM.

- número de referência do comando
- mnemônico(s) do decodificador do comando

Tabela 18 DISPLAY-COMMAND-ACCESS (CRN 07612)

Comando Introduzido	Significado
<DISPLAY-COMMAND-ACCESS:	
<COMMAND="DISPLAY-ACTIVE-ALARMS"**.**	comando

```
DISPLAY-COMMAND-ACCESS                                          CON EXITO
-------------------------------------------------------------------------

                                          AREA
 MNEMONICO COMANDO          NR COMANDO    ANTERIOR
-----------------------------------------------------------
 DISPLAY-ACTIVE-ALARMS      19             2

ULTIMO INFORME   =    04257
```

6.5 Modificar o Acesso aos Comandos

Descrição Só para operadores de segurança. Usa-se este comando para modificar a atribuição da área de comandos para acesso ao comando CHM especificado. Podem ser trocadas as áreas de comandos até para 10 comandos CHM de cada vez.

- área atual de comandos para acesso ao comando
- área prévia de comandos para acesso ao comando

Tabela 19 MODIFY-COMMAND-ACCESS (CRN 07613)

Comando Introduzido	Significado
<MODIFY-COMMAND-ACCESS:	
<COMMAND=19,	comando
<ÁREA=2**.**	nova área de comandos que vai ser atribuído o comando anterior

```
MODIFY-COMMAND-ACCESS                                          CON EXITO
-------------------------------------------------------------------------

                                          AREA      AREA
MNEMONICO COMANDO          NR COMANDO     ACTUAL    ANTERIOR
-----------------------------------------------------------
DISPLAY-ACTIVE-ALARMS      19             7          2

ULTIMO INFORME   =    04257
```

7 Gerenciador do Acesso aos Dispositivos

Este capítulo mostra o planejamento básico de como gerenciar o acesso aos dispositivos. Descreve os comandos mais frequentemente utilizados, ilustrados com exemplos. Os comandos aqui agrupados tratam as seguintes tarefas:

- visualização e modificação das áreas de comandos ás quais tem acesso um dispositivo de entrada.
- exclusão e desbloqueio do acesso dos dispositivos às centrais e áreas de comandos.

Podemos encontrar informações mais detalhadas sobre os conceitos básicos e definições de termos especiais no capítulo 1.

7.1 Tarefas e Referências

Neste capítulo são descritos os comandos para gerenciamento do acesso aos dispositivos.

Os exemplos a seguir não proporcionam todos os possíveis parâmetros para cada um dos comandos. Consultar o correspondente Procedimento Detalhado se desejar informações mais completas.

A tabela 20 contém uma lista de referências a outros documentos úteis nos manuais de Operação e Manutenção.

Tabela 20 Comandos, CRN e documentos relacionados para a administração do acesso

Tarefa	Comando-CHM	CRN	Documento
Exibir a Área de Comandos para um Dispositivo	DISPLAY-DEVICE-CMDAREA	04814	DP04814
Modificar a Área de Comandos para um Dispositivo	MODIFY-DEVICE-CMDAREA	04818	DP04818
Excluir a Área de Comandos para um Dispositivo	DELETE-DEVICE-CMDAREA	05993	DP05993
Exibir Dispositivos Excluídos	DISPLAY-BARRED-DEVICES	04970	DP04970
Modificar Dispositivos Excluídos	MODIFY-BARRED-DEVICES	04971	DP04971

7.2 Exibir Área de Comandos para um Dispositivo

Descrição Usar este comando para visualizar quais áreas de comandos e centrais (terminais quando se trata de um Centro de Serviço de Rede (Network Service Center) (NSC) um em particular ou todos os dispositivos de entrada tem autorização de acesso. O informe de saída indica também se o dispositivo está excluído, assim como quantas tentativas de acesso não válido estão permitido.

Tabela 21 DISPLAY-DEVICE-CMDAREA (CRN 04814)

Comando Introduzido	Significado
<DISPLAY-DEVICE-CMDAREA:	
<DEV=5&H'C&1,	dispositivo

```
DISPLAY-DEVICE-CMDAREA                                          CON EXITO
------------------------------------------------------------------------

DISPOSITIVO                    : 00005&000C&00001
INFORME INTENTO ENTRAR         : OFF
ACCESOS NO VALIDOS PERMITIDOS : 4
DISPOSITIVO ES                 : ACESSO NÃO TACHADO
CENTRO DE OPERADOR             : 00000
DISPOSITIVO OPER DENTRO CENTRO: 00000
FICHERO MMC USADO POR CENTRO   : 00002
NUMERO REFERENCIA DISPOSITIVO : 1001

DISP NO TIENE ACCESO A SIG AREAS DE COMANDO  :

  1    2    3    4    5    6    7    8    9    10
  11   12   13   14   15   16   17   18   19   20
  21   22   23   24   25   26   27   28   29   30
  31   32   33   34   35   36   37   38   39   40
  41   42   43   44   45   46   47   48   49   50
  51   52   53   54   55   56   57   58   59   60
  61   62   63   64   65   66   67   68   69   70
  71   72   73   74   75   76   77   78   79   80
  81   82   83   84   85   86   87   88   89   90
  91   92   93   94   95   96   97   98   99   100
  101  102  103  104  105  106  107  108  109  110
  111  112  113  114  115  116  117  118  119  120
  121  122  123  124  125  126  127  128

DISP TIENE ACCESO A SIG AREAS PRE-R7         :

  1    2    3    4    5    6    7    8
  9    10   11   12   13   14   15   16
  17   18   19   20   21   22   23   24
  25   26   27   28   29   30   31   32

DISP TIENE ACCESO A SIGUIENTES CENTRALES     :

SITE-ID       SITE-NAME
------------------------------------------------------------------
1             CPCAEJ

ULTIMO INFORME   =    04674
```

7.3 Modificar Área de Comandos para um Dispositivo

Descrição Usa-se este comando para atribuir autorização de acesso centrais e áreas de comandos para acesso de dispositivos. Todas as modificações realizadas para um NSC são aplicados também de forma automática às centrais.

Tabela 22 MODIFY-DEVICE-CMDAREA (CRN 04818)

Comando Introduzido	Significado
<MODIFY-DEVICE-CMDAREA:	
<DEV=5&H'C&1,	dispositivo
<INITACC=1.	inicializar o contador de violações de acessos

```
MODIFY-DEVICE-CMDAREA                                          CON EXITO
------------------------------------------------------------------------

DISPOSITIVO                    : 00005&000C&00001
INFORME INTENTO ENTRAR         : OFF
ACCESOS NO VALIDOS PERMITIDOS : 1
DISPOSITIVO ES                 : ACCESS NO TACHADO
CENTRO DE OPERADOR             : 00000
DISPOSITIVO OPER DENTRO CENTRO: 00000
FICHERO MMC USADO POR CENTRO   : 00002
NUMERO REFERENCIA DISPOSITIVO : 1001

DISP NO TIENE ACCESO A SIG AREAS DE COMANDO  :
```

```
  1    2    3    4    5    6    7    8    9    10
  11   12   13   14   15   16   17   18   19   20
  21   22   23   24   25   26   27   28   29   30
  31   32   33   34   35   36   37   38   39   40
  41   42   43   44   45   46   47   48   49   50
  51   52   53   54   55   56   57   58   59   60
  61   62   63   64   65   66   67   68   69   70
  71   72   73   74   75   76   77   78   79   80
  81   82   83   84   85   86   87   88   89   90
  91   92   93   94   95   96   97   98   99   100
  101  102  103  104  105  106  107  108  109  110
  111  112  113  114  115  116  117  118  119  120
  121  122  123  124  125  126  127  128

DISP TIENE ACCESO A SIG AREAS PRE-R7         :

  1    2    3    4    5    6    7    8
  9    10   11   12   13   14   15   16
  17   18   19   20   21   22   23   24
  25   26   27   28   29   30   31   32

DISP TIENE ACCESO A SIGUIENTES CENTRALES     :

SITE-ID       SITE-NAME
------------------------------------------------------------------
1             CPCAEJ

ULTIMO INFORME   =    04674
```

7.4 Excluir Área de Comandos para um Dispositivo

Descrição Usar este comando para cancelar o direito de acesso de dispositivo de entrada especificado às centrais e as áreas de comandos.

Tabela 23 DELETE-DEVICE-CMDAREA (CRN 05993)

Comando Introduzido	Significado
<DELETE-DEVICE-CMD ÀREA:	
<DEV=5&H'C&9.	dispositivo

```
DELETE-DEVICE-CMDAREA                                          CON EXITO
------------------------------------------------------------------------

EL SIGUIENTE DISPOSITIVO HA SIDO BORRADO CON EXITO DE
LA RELACION DE ACCESO A DISPOSITIVO:

TIPO /NA  /NUMERO
-----------------
00005/000C/00009

ULTIMO INFORME   =    05598
```

7.5 Exibir Dispositivos Restritos

Descrição Usar este comando para visualizar,

- que dispositivos físicos estão no estado ”acesso restrito”
- se o dispositivo indicado está no estado ”acesso restrito” ou não.

Tabela 24 DISPLAY-BARRED-DEVICES (CRN 04970)

Comando Introduzido	Significado
<DISPLAY-BARRED-DEVICES:	
<ALLDEV.	todos os dispositivos físicos no estado ”acesso excluído”

```
DISPLAY-BARRED-DEVICES                                          CON EXITO
------------------------------------------------------------------------

ALLDEVS

NO DISPOSITIVOS LISTADOS

ULTIMO INFORME   =    04883
```

Comando Introduzido	Significado
<DISPLAY-BARRED-DEVICES:	
<DEV=130&H’2D&3.	identidade do dispositivo físico no estado ”acesso excluído”

```
DISPLAY-BARRED-DEVICES                                          CON EXITO
------------------------------------------------------------------------

DEVICE   :  00130/002D/00003  NO LISTADO

ULTIMO INFORME   =    04883
```

7.6 Modificar Dispositivos Restritos

Descrição Só para operador de segurança. Usa-se este comando para bloquear ou desbloquear o dispositivo de acesso para um dispositivo físico.

Tabela 25 MODIFY-BARRED-DEVICES (CRN 04971)

Comando Introduzido	Significado
<MODIFY-BARRED-DEVICES:	
<DEV=130&H'2D&3,	identidade do dispositivo físico
<BAR=OFF.	dispositivo em estado "excluído" (=on) ou "não excluído" (=off)

```
MODIFY-BARRED-DEVICES                                          CON EXITO
------------------------------------------------------------------------

DEVICE   :  00130/002D/00003  NO LISTADO

ULTIMO INFORME   =    04883
```

8 Modificar Autorização para MPTMON

Este capítulo mostra como pode ser estabelecida e eliminada a autorização para a ferramenta de testes ”Monitor de Testes MultiProcesso (Multiprocess Test Monitor) (MPTMON)”. Descreve como se usa o comando e o ilustra com um exemplo.

8.1 Tarefas e Referências

Neste capítulo são descritos os comandos para o gerenciamento do acesso ao MPTMON.

Os exemplos a seguir não proporcionam todos os possíveis parâmetros para cada um dos comandos.

Consultar o correspondente Procedimento Detalhado se desejar informações mais completas.

A tabela 26 contém uma lista de referências a outros documentos úteis nos manuais de Operação e Manutenção neste capítulo.

Tabela 26 Comandos, CRN e documentos relacionados com a administração do acesso ao MPTMON

Tarefa	Comando-CHM	CRN	Documento
Modificar Autorização MPTMON	MODIFY-MPTMON-AUTH	04006	DP04006

8.2 Modificar Autorização para MPTMON

Descrição Usar este comando para estabelecer a autorização da ferramenta de testes MPTMON. São possíveis as seguintes autorizações:

- só trabalhos locais,
- só leitura ,
- modificação,
- nenhuma autorização.

A nova autorização estabelecida substitue a que já existia.

Tabela 27 MODIFY-MPTMON-AUTH (CRN 04006)

Comando Introduzido	Significado
<MODIFY-MPTMON-AUTH:	
<AUTH=MODIFY.	tipo de autorização que vai ser estabelecida

```
MODIFY-MPTMON-AUTH                                                  CON EXITO
------------------------------------------------------------------------------
FINALIZACION BASE DE DATOS =  H'0000

ULTIMO INFORME    =    04027
```

9 Administração de Registro - Introdução

Este capítulo apresenta a função de registro usada nas centrais Alcatel 1000 S12. Descreve seus elementos, funções e define os termos chaves.

Os tópicos deste capítulo são:

- definição dos tipos de registro e outros termos chave
- descrição das áreas de tarefas, comandos usados suas interrelações.

O subsistema de registro mantém um livro de registro da interface CHM. Suas duas principais funções são:

- Salvar os dados registrados
- Supervisão da interface CHM.

Salvando os Dados Registrados

O subsistema de registro escreve todos os tipos de comandos CHM e/os informes CHM em arquivos pré-definidos dos discos do PLCE ou PBCE se a função de registro estiver ativada previamente.

Tipos de Registro

O subsistema de registro pode gerenciar simultâneamente os seguintes 6 tipos de registro:

- Comandos aceitos (ACCMD)

  Todos os comandos CHM introduzidos que foram aceitos por qualquer manejador de comandos.

- Todos os comandos (ALLCMD)

  Todos os comandos CHM introduzidos, que foram aceitos ou não pelo Sistema de Entrada/Saída ou qualquer manejador de comandos, incluindo os comandos dos Centros de Serviço de Rede.

- Informes Solicitados (REPORT)

  Todos os informes gerados pelos manejadores de comandos em resposta aos Trabalhos Solicitados pelo Operador (Operator Requested Job) (ORJ), incluíndo os solicitados através do NSC.

- Informes não Solicitados (UNSOLREP)

  Todos os informes gerados por quaisquer módulos para atrair a atenção sobre estados específicos ou eventos do sistema, incluíndo os informes não solicitados do NSC.

- Informes de Alarme (ALARM)

  Todos os informes gerados por quaisquer módulos, em resposta à condições de alarme e para informar sobre as trocas de estado essênciais no sistema, incluíndo os informes de alarmes do NSC.

- Informes de Violações (VIOLREP)

  Todos os informes gerados pelo próprio sistema em resposta às violações de acesso, por ex. tentativas ilegais de conexão ou de acesso a comandos/dispositivos.

Supervisão Eficiente da Interface CHM

A função de registro habilita qualquer operador ou FMM usuária para recuperar todos ou certo tipo de elementos CHM registrados

em formato legível/imprimível (ASCII) ou binário. Os critérios de recuperação são:

- tipo de registro
- janela de tempo
- identidade de usuário
- dispositivo de entrada
- mensagem ou número de referência do comando.

Áreas de tarefas A administração de registro compreende as seguintes áreas:

- Controle da função de registro com inicialização, começo e fim.
- Gravação dos dados registrados.
- Salvamento dos dados registrados.

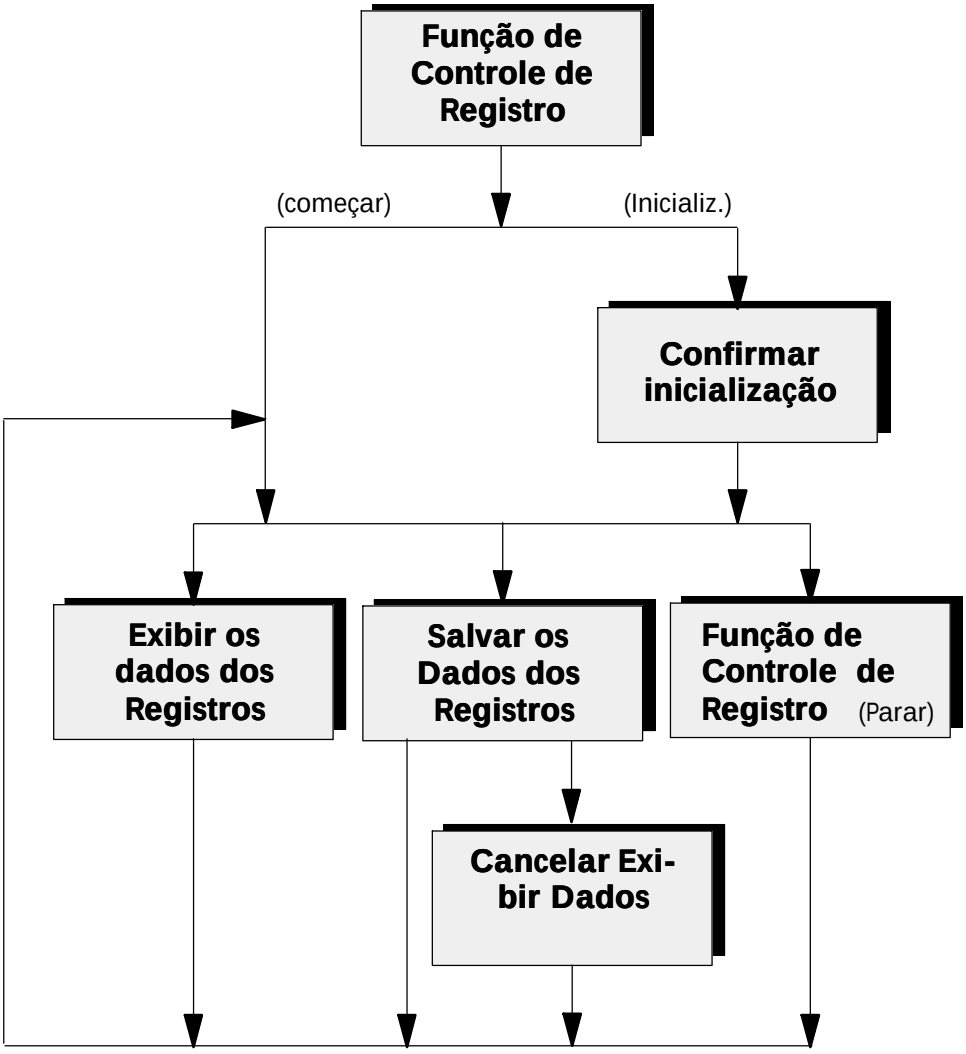

Figura 1 Comandos para a administração da Função de registro

10 Controle da Função de Registro

Este capítulo mostra o manejo básico do controle da função de registro. Descreve os comandos mais frequentemente utilizados, ilustrados com os exemplos:

- visualização da função de registro: Está ou não ativada a função de registro? Quais são os arquivos de registro de comandos e informes? Que estados mostram os tipos de registro?
- inicialização, começo e finalização da função de registro

Podemos encontrar informações mais detalhadas sobre os conceitos básicos e definições de termos especiais no capítulo 9.

10.1 Tarefas e Referências

Neste capítulo sera descrito os comandos para controlar a função de registro.

Os exemplos a seguir não proporcionam todos os possíveis parâmetros para cada um dos comandos.

Consultar o correspondente Procedimento Detalhado se desejar informações mais completas.

A tabela 28 contém uma lista de referências a outros documentos úteis nos manuais de Operação e Manutenção.

Tabela 28 Comandos, CRN e documentos relacionados com o controle da função de registro

Tarefa	Comando-CHM	CRN	Documento
Exibir a Função de Registro	DISPLAY-LOGGING-FUNCTION	04989	DP04989
Controle da Função de Registro	CONTROL-LOGGING-FUNCTION	07966	DP07966
Confirmar inicialização	CONFIRM-INIT	07967	DP07967

10.2 Exibir a Função de Registro

Descrição Usar este comando para

- checar se a função de registro está ativa neste momento,
- visualizar informações sobre os arquivos de registro de comandos e informes
- mostrar o estado atual de todos os tipos de registro.

O comando será executado de forma imediata, a menos que seja planejado para uma hora determinada.

Tabela 29 DISPLAY-LOGGING-FUNCTION (DP 04989)

Comando Introduzido	Significado
<DISPLAY-LOGGING-FUNCTION:	
<LOGTYPE=ALL.	tipo de arquivo de registro (ver também o capítulo 9)

```
DISPLAY-LOGGING-FUNCTION                                          CON EXITO
------------------------------------------------------------------------------
LOGTYPE  = ALL

                    AUTO  ANOTAD   ALARM      ALARM     DESDE ULTI SALV
LOGTYPE    ESTADO  SALVAR  ELEMS    HNDL      UMBRAL    ELEMS   CAPACIDA
------------------------------------------------------------------------------
ACCMD      PASIVO    OFF       0      ON         70 %        0        0 %
ALLCMD     PASIVO    OFF       0      ON         70 %        0        0 %
REPORT     PASIVO    OFF       0      ON         70 %        0        0 %
UNSOREP    PASIVO    OFF       0      ON         70 %        0        0 %
ALARM      PASIVO    OFF       0      ON         70 %        0        0 %
VIOLREP    PASIVO    OFF       0      ON         70 %        0        0 %

ULTIMO INFORME   =    04894
```

10.3 Controle da Função Registro

Descrição Usa-se o comando 'CONTROL-LOGGING-FUNCTION' para:

- Inicializar o subsistema de registro (comando mais parâmetro INIT)

  Inicializar a função de registro para todos os tipos de registro; usar este comando quando não há nenhum registro ativo ou quando foi carregado um novo pacote software.

  Os exemplos a seguir não proporcionam todos os possíveis parâmetros para cada um dos comandos. Consultar o correspondente Procedimento Detalhado se desejar informações mais detalhadas.A tabela 26 contém uma lista de referências a outros documentos úteis nos manuais de Operação e Manutenção usados neste capítulo.

  Se inicializar todos os arquivos de registro e colocar em 'ativo' o estado do registro. O comando deve ir seguido do comando 'CONFIRM-INIT:REPLY=CONFIRM; (ver capítulo 10.4).

- Iniciar a função de registro (comando mais parâmetro START)

  Voltar a iniciar a sessão de registro quando outra sessão ou o mesmo usuário for desativado do registro previamente.

- Deter a função de registro (comando mais parâmetro STOP)

  Deter a função de registro; a função de registro pode ser detida de forma separada para cada tipo de registro.

- Visualizar informação sobre o tipo de registro (comando mais parâmetro DISPLAY)

Tabela 30 CONTROL-LOGGING-FUNCTION (CRN 07966)

Comando Introduzido	Significado
<CONTROL-LOGGING-FUNCTION:	
<LOGTYPE=VIOLREP,	tipo de registro
<INIT.	Inicializar uma nova sessão de registro

```
CONTROL-LOGGING-FUNCTION                          EN ESPERA DE CONFIRMACION
------------------------------------------------------------------------
INICIO
TIPO LOG = VIOLREP

                     AUTO  LOGGED   ALARM     ALARMA    DESDE ULTIMO SAVE
TIPO LOG   ESTADO    SAVE   ITEMS    HNDL     UMBRAL     ITEMS   CAPACIDAD
------------------------------------------------------------------------
VIOLREP    PASIVO    OFF       0     ON         70 %        0       0 %

PARA PROCESSAR LA FUNCION INIT, INTRODUZA COMANDO CONFIRM-INIT
ANTES DE 300 SEGUNDOS CON EL PARAMETRO REPLY=CONFIRM O CANCEL!

EM ESPERA DE CONFIRMACION

SIGUE RESULTADO  =    07918
```

10.4 Confirmar inicialização

Descrição Usa-se este comando para confirmar ou cancelar o comando CONTROL-LOGGING-FUNCTION. O comando será executado imediatamente, a menos que tenha sido programado para uma determinada hora.

Nota A inicialização da função de registro tem que ser confirmada com o comando CONFIRM-INIT:REPLY=CONFIRM.

Tabela 31 CONFIRM-INIT (CRN 07967)

Comando Introduzido	Significado
<CONFIRM-INIT:	
<REPLY=CONFIRM.	resposta (confirmar/cancelar comando)

```
CONFIRM-INIT                                                        CON EXITO
-------------------------------------------------------------------------------
REPLY= CONFIRM

                     AUTO  ANOTAC   ALARM       ALARMA   DESDE ULT  SALV
TIPO LOGIN ESTADO    SALV   ITEMS    HNDL   UMBRAL   ITEMS   CAPACIDAD
-------------------------------------------------------------------------------
VIOLREP    ACTIVO    OFF       0     ON         70 %        0       0 %

ULTIMO INFORME   =    04015
```

11 Manejo de Arquivos com Dados do Registro

Este capítulo mostra o tratamento básico de como gravar os dados registrados. Descreve os comandos mais frequentemente utilizados, ilustrados com exemplos. Os comandos aqui agrupados tratam as seguintes tarefas:

- Exibir os parâmetros chaves dos arquivos de registro de comandos e informes para um ou todos os tipos de registros.
- Exibir os dados que descrevem os arquivos de registro do tipo especificado assim como seu conteúdo.

Podemos encontrar informações mais detalhadas sobre os conceitos básicos e definições de termos especiais no capítulo 9.

11.1 Tarefas e Referências

Neste capítulo serão descritos os comandos para tratar ou gerenciar os dados registrados.

Os exemplos a seguir não proporcionam todos os possíveis parâmetros para cada um dos comandos.

Consultar o correspondente Procedimento Detalhado se desejar informações mais detalhadas.

Na tabela 32 contêm uma lista de referências a outros documentos úteis nos manuais de Operação e Manutenção.

.

Tabela 32 Comandos, CRN e documentos relacionados com a gravação dos dados registrados

Tarefa	Comando-CHM	CRN	Documento
Exibir as Características do arquivo de Registro	DISPLAY-LOGFILE-CHAR	04017	DP04017
Exibir os Dados Registrados	DISPLAY-LOG-DATA	05198	DP05198

11.2 Exibir as Características dos Arquivos de Registro

Descrição Usa-se este comando para visualizar os parâmetros e a chave de acesso dos arquivos de registro de comandos e informes para um ou todos os tipos de registro. Para cada tipo de registro são listados todos os arquivos de registro junto com suas identidades de arquivo de registro, a chave de autorização e o dispositivo.

O comando será executado imediatamente, a menos que esteja programado para uma determinada hora.

Tabela 33 DISPLAY-LOGFILE-CHAR (CRN 04017)

Comando Introduzido	Significado
<DISPLAY-LOGFILE-CHAR:	
<LOGTYPE=VIOLREP.	tipo de arquivo de registro (ver também o capítulo 9)

```
DISPLAY-LOGFILE-CHAR                                              CON EXITO
------------------------------------------------------------------------------
LOGTYPE    = VIOLREP

TIPO DE LOGGIN  ID FICH LOG   CLAVE acCeso        DISPOSITIVO
-------------------------------------------------------------
VIOLREP             1290             SS             DKA1DKB1
VIOLREP             1291             SS             DKA1DKB1
VIOLREP             1292             SS             DKA1DKB1
VIOLREP             1293             SS             DKA1DKB1
VIOLREP             1294             SS             DKA1DKB1
VIOLREP             1295             SS             DKA1DKB1
VIOLREP             1296             SS             DKA1DKB1
VIOLREP             1297             SS             DKA1DKB1
VIOLREP             1298             SS             DKA1DKB1
VIOLREP             1299             SS             DKA1DKB1

ULTIMO INFORME    =    04189
```

11.3 Exibir os Dados Registrados

Descrição Usa-se este comando para visualizar de forma seletiva os dados contidos nos arquivos de registro. Os critérios de seleção são:

- o tipo de registro; conforme definição do capítulo 9
- critério específico de seleção
- período de registro da informação a ser visualizada
- o destino do informe.

O comando será executado imediatamente, a menos que tenha sido planejada para uma determinada hora.

Tabela 34 DISPLAY-LOG-DATA (CRN 05198)

Comando Introduzido	Significado
<DISPLAY-LOG-DATA:	
<LOGTYPE=VIOLREP,	tipo de arquivo de registro (ver também o capítulo 9)
	tipo de registro
<OUTDEV=DKA1.	dispositivo de saída

```
DISPLAY-LOG-DATA                                    ARRANCADO CON EXITO
                                                  RESULTADO INTERMEDIO
------------------------------------------------------------------------

LOGTYP = VIOLREP

FECHA INICIO = 1998/JUL/28     HORA INIC  =  00:00
FECHA FINAL  = 1998/JUL/28     HORA FINAL =  00:17

OUTDEV/LDEV  = DKA1

SIGUE RESULTADO  =    05036
```

```
DISPLAY-LOG-DATA                                                CON EXITO
                                                          RESULTADO FINAL
-------------------------------------------------------------------------

LOGTYP = VIOLREP

FECHA INICIO = 1998/JUL/28     HORA INIC  =  00:00
FECHA FINAL  = 1998/JUL/28     HORA FINAL =  00:17

OUTDEV/LDEV  = DKA1
OUTDEV/FILE  = 1362

DATOS NO ENCONTRADOS

ULTIMO INFORME   =    05036
```

Tabela 35 DISPLAY-LOG-DATA (CRN 05198)

Comando Introduzido	Significado
<DISPLAY-LOG-DATA:	
<LOGTYPE=ACCMD,	tipo de registro
<OUTDEV=DKA1.	dispositivo de saída

```
DISPLAY-LOG-DATA                                  ARRANCADO CON EXITO
                                                  RESULTADO INTERMEDIO
-------------------------------------------------------------------------

LOGTYP = ACCMD

DATA INICIO = 1998/JUL/28     HORA INIC  =  00:00
DATA FINAL  = 1998/JUL/28     HORA FINAL =  00:28

OUTDEV/LDEV  = DKA1

SIGUE RESULTADO  =    05036
```

```
DISPLAY-LOG-DATA                                                CON EXITO
                                                          RESULTADO FINAL
------------------------------------------------------------------------

LOGTYP = ACCMD

DATA INICIO = 1998/JUL/28     HORA INIC  =  00:00
DATA FINAL  = 1998/JUL/28     HORA FINAL =  00:28

OUTDEV/LDEV  = DKA1
OUTDEV/FILE  = 1362

DATOS NO ENCONTRADOS

ULTIMO INFORME   =    05036
```

12 Salvando os Dados de Registro

Este capítulo mostra o tratamento básico de como salvar os dados registrados. Descreve os comandos mais frequentemente utilizados, ilustrados com exemplos. Os comandos aqui agrupados tratam as seguintes tarefas :

- carregados os dados armazenados em arquivos de registro a disco óptico ou fita magnética
- detenção do comando de salvar.

Podemos encontrar informações mais detalhadas sobre os conceitos básicos e definições de termos especiais no capítulo 9

12.1 Tarefas e Referências

Neste capítulo serão descritos os comandos para controlar e salvar os dados registrados.

Os exemplos a seguir não proporcionam todos os possíveis parâmetros para cada um dos comandos.

Consultar o correspondente Procedimento Detalhado se desejar informações mais detalhadas.

A tabela 36 contém uma lista de referências a documentos úteis nos manuais de Operação e Manutenção acrescentados neste capítulo.

Tabela 36 Comandos, CRN e documentos relacionados com o salvamento dos dados registrados

Tarefa	Comando-CHM	CRN	Documento
Salvar Dados Registrados	SAVE-LOG-DATA	05200	DP 05200
Deter Visualização de Dados	STOP-DISPLAY-DATA	05199	DP 05199

12.2 Salvar os Dados Registrados

Descrição Um alarme ou uma mensagem não solicitada informa ao operador que os arquivos de registro estão já quase cheios. O operador tem que transferir os dados registrados para um disco óptico ou numa fia magnética trnasmiti-los a um centro remoto ou através do FTAM.

Usa-se este comando para carregar dados que estão armazenados em arquivos de registro, em um disco óptico ou uma fita magnética. São carregados todos os dados pertencentes aos tipos de registro selecionados e que foram acumulados desde o último carregamento.

O comando será executado imediatamente, a menos que tenha sido programado para uma determinada hora.

Tabela 37 SAVE-LOG-DATA (CRN 05200)

Comando Introduzido	Significado
<SAVE-LOG-DATA:	
<LOGTYPE=ACCMD.	tipo de arquivo de registro (ver também o capítulo 9)
<OUTDEV=DKA1.	dispositivo de salída

```
SAVE-LOG-DATA                                          ARRANCADO CON EXITO
                                                      RESULTADO INTERMEDIO
-------------------------------------------------------------------------

LOGTYP = ACCMD

OUTDEV/LDEV  = DKA1

SIGUE RESULTADO  =    05038
```

```
SAVE-LOG-DATA                                                    CON EXITO
                                                          RESULTADO FINAL
------------------------------------------------------------------------

LOGTYP = ACCMD

DATA INICIO = 1998/JUL/28     HORA INICIO=  00:35
DATA PARADA = 1998/JUL/28     HORA FINAL=  00:42

OUTDEV/LDEV  = DKA1
OUTDEV/FILE  = 1372

ULTIMO INFORME   =    05038
```

12.3 Cancelar a Exibição dos Dados

Descrição Este comando permite ao usuário cancela a execução dos comandos:

- DISPLAY-CMD-LOG, DP 06025 (dar DISPLAY)
- SAVE-LOG-DATA, DP 05200 (dar SAVE).

Tabela 38 STOP-DISPLAY-DATA (CRN 05199)

Comando Introduzido	Significado
<STOP-DISPLAY-DATA:	
<TASK=SAVE.	tarefa que vai ser cancelada

```
SAVE-LOG-DATA                                                    AVISO
                                                    RESULTADO FINAL
-------------------------------------------------------------------------

LOGTYP = ACCMD

OUTDEV/LDEV  = DKA1
OUTDEV/FILE  = 1372

PARADA SOLICITADA POR OPERADOR

ULTIMO INFORME   =
05038
```

Abbreviations

BCG	Grupo de Comunicação de Negócios (Business Communication Group)
CHM	Comando Homem Máquina (Man Machine Command)
CRN	Número de Referência do Comando (Command Reference Number)
LPI	Identificador de senha Lógica (Logical Password Identifier)
MPTMON	Monitor de Testes MultiProcesso (Multiprocess Test Monitor)
NSC	Centro de Serviço de Rede (Network Service Center)
ORJ	Trabalhos Solicitados pelo Operador (Operator Requested Job)
VDUFH	Manuseador de Arquivos de VDU (VDU File Handler)

Index

Espaços

A

C

D

E

F

G

I

J

M

O

P

R

S

T

U

V