



Sun™ Mainframe Security Facility Release Notes for AIX Platforms

Release 1.1.0

Sun Microsystems, Inc.
www.sun.com

Part No. 819-6570-10
May 2006, Revision A

Submit comments about this document at: <http://www.sun.com/hwdocs/feedback>

Copyright 2006 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, California 95054, U.S.A. All rights reserved.

Sun Microsystems, Inc. has intellectual property rights relating to technology that is described in this document. In particular, and without limitation, these intellectual property rights may include one or more of the U.S. patents listed at <http://www.sun.com/patents> and one or more additional patents or pending patent applications in the U.S. and in other countries.

This document and the product to which it pertains are distributed under licenses restricting their use, copying, distribution, and decompilation. No part of the product or of this document may be reproduced in any form by any means without prior written authorization of Sun and its licensors, if any.

Third-party software, including font technology, is copyrighted and licensed from Sun suppliers.

Parts of the product may be derived from Berkeley BSD systems, licensed from the University of California. UNIX is a registered trademark in the U.S. and in other countries, exclusively licensed through X/Open Company, Ltd.

Sun, Sun Microsystems, the Sun logo, Java, AnswerBook2, docs.sun.com, and Solaris are trademarks or registered trademarks of Sun Microsystems, Inc. in the U.S. and in other countries.

All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. in the U.S. and in other countries. Products bearing SPARC trademarks are based upon an architecture developed by Sun Microsystems, Inc. ORACLE is a registered trademark of Oracle Corporation.

The OPEN LOOK and Sun™ Graphical User Interface was developed by Sun Microsystems, Inc. for its users and licensees. Sun acknowledges the pioneering efforts of Xerox in researching and developing the concept of visual or graphical user interfaces for the computer industry. Sun holds a non-exclusive license from Xerox to the Xerox Graphical User Interface, which license also covers Sun's licensees who implement OPEN LOOK GUIs and otherwise comply with Sun's written license agreements.

U.S. Government Rights—Commercial use. Government users are subject to the Sun Microsystems, Inc. standard license agreement and applicable provisions of the FAR and its supplements.

DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID.

Copyright 2006 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, Californie 95054, États-Unis. Tous droits réservés.

Sun Microsystems, Inc. possède les droits de propriété intellectuels relatifs à la technologie décrite dans ce document. En particulier, et sans limitation, ces droits de propriété intellectuels peuvent inclure un ou plusieurs brevets américains listés sur le site <http://www.sun.com/patents>, un ou les plusieurs brevets supplémentaires ainsi que les demandes de brevet en attente aux États-Unis et dans d'autres pays.

Ce document et le produit auquel il se rapporte sont protégés par un copyright et distribués sous licences, celles-ci en restreignent l'utilisation, la copie, la distribution, et la décompilation. Aucune partie de ce produit ou document ne peut être reproduite sous aucune forme, par quelque moyen que ce soit, sans l'autorisation préalable et écrite de Sun et de ses bailleurs de licence, s'il y en a.

Tout logiciel tiers, sa technologie relative aux polices de caractères, comprise, est protégé par un copyright et licencié par des fournisseurs de Sun.

Des parties de ce produit peuvent dériver des systèmes Berkeley BSD licenciés par l'Université de Californie. UNIX est une marque déposée aux États-Unis et dans d'autres pays, licenciée exclusivement par X/Open Company, Ltd.

Sun, Sun Microsystems, le logo Sun, Java, AnswerBook2, docs.sun.com, et Solaris sont des marques de fabrique ou des marques déposées de Sun Microsystems, Inc. aux États-Unis et dans d'autres pays.

Toutes les marques SPARC sont utilisées sous licence et sont des marques de fabrique ou des marques déposées de SPARC International, Inc. aux États-Unis et dans d'autres pays. Les produits portant les marques SPARC sont basés sur une architecture développée par Sun Microsystems, Inc. ORACLE est une marque déposée registre de Oracle Corporation.

L'interface utilisateur graphique OPEN LOOK et Sun™ a été développée par Sun Microsystems, Inc. pour ses utilisateurs et licenciés. Sun reconnaît les efforts de pionniers de Xerox dans la recherche et le développement du concept des interfaces utilisateur visuelles ou graphiques pour l'industrie informatique. Sun détient une licence non exclusive de Xerox sur l'interface utilisateur graphique Xerox, cette licence couvrant également les licenciés de Sun implémentant les interfaces utilisateur graphiques OPEN LOOK et se conforment en outre aux licences écrites de Sun.

LA DOCUMENTATION EST FOURNIE "EN L'ÉTAT" ET TOUTES AUTRES CONDITIONS, DÉCLARATIONS ET GARANTIES EXPRESSES OU TACITES SONT FORMELLEMENT EXCLUES DANS LA LIMITE DE LA LOI APPLICABLE, Y COMPRIS NOTAMMENT TOUTE GARANTIE IMPLICITE RELATIVE À LA QUALITÉ MARCHANDE, À L'APTITUDE À UNE UTILISATION PARTICULIÈRE OU À L'ABSENCE DE CONTREFAÇON.



Adobe PostScript

Contents

Preface v

Sun Mainframe Security Facility Release 1.1.0 1

General Installation Information 1

Documentation Advisory 2

Important Operating Information 2

Deploying Behind a Firewall 2

Upgrading Sun MSF 2

Shutting Down the Security Server 3

Enhancements 3

Configuration Utility 3

“No Prompt” Option for Administering the Security Server 3

New Utility for Updating Repository Passwords 3

User-Defined Resource Types 4

Changes from Previous Releases 4

Command Names Changed 4

Password Encryption 4

New Error Messages 5

Known Problems and Limitations 5

Documentation 7

Documentation Errata	7
Refreshing Users' Security Rules	7
Security Server Statistics	8
Log Message Levels	10

Preface

This document describes the enhancements and changes to the Sun™ Mainframe Security Facility (Sun MSF) for Release 1.1.0 on AIX operating system platforms.

Using UNIX Commands

This document might not contain information on basic UNIX® commands and procedures such as shutting down the system, booting the system, and configuring devices. Refer to the software documentation that you received with your system.

Shell Prompts

Shell	Prompt
C shell	<i>machine-name%</i>
C shell superuser	<i>machine-name#</i>
Bourne shell and Korn shell	\$
Bourne shell and Korn shell superuser	#

Typographic Conventions

Typeface*	Meaning	Examples
AaBbCc123	The names of commands, files, and directories; on-screen computer output	Edit your <code>.login</code> file. Use <code>ls -a</code> to list all files. % You have mail.
AaBbCc123	What you type, when contrasted with on-screen computer output	% su Password:
<i>AaBbCc123</i>	Book titles, new words or terms, words to be emphasized. Replace command-line variables with real names or values.	Read Chapter 6 in the <i>User's Guide</i> . These are called <i>class</i> options. You <i>must</i> be superuser to do this. To delete a file, type <code>rm filename</code> .

* The settings on your browser might differ from these settings.

Related Documentation

Product	Title	Part Number
Sun Mainframe Security Facility	<i>Sun Mainframe Security Facility Administrator's Guide</i>	817-7448-10
Sun Mainframe Transaction Processing software	<i>Sun Mainframe Transaction Processing Software Administrator's Guide</i>	817-7431-10
	<i>Sun Mainframe Transaction Processing Software Configuration Guide</i>	817-7433-10
	<i>Sun Mainframe Transaction Processing Software Developer's Guide</i>	817-7432-10
	<i>Sun Mainframe Transaction Processing Software Installation Guide</i>	817-7434-10
	<i>Sun Mainframe Transaction Processing Software Message Guide</i>	817-7435-10
	<i>Sun Mainframe Transaction Processing Software Reference Guide</i>	817-7436-10
	<i>Sun Mainframe Transaction Processing Software Troubleshooting and Tuning Guide</i>	817-7437-10
	<i>Sun Mainframe Transaction Processing Software Release Notes for AIX Platforms</i>	819-5727-10

Documentation, Support, and Training

Sun Function	URL
Documentation	http://www.sun.com/documentation/
Support	http://www.sun.com/support/
Training	http://www.sun.com/training/

Sun Welcomes Your Comments

Sun is interested in improving its documentation and welcomes your comments and suggestions. You can submit your comments by going to:

<http://www.sun.com/hwdocs/feedback>

Please include the title and part number of your document with your feedback:

Sun Mainframe Security Facility Release Notes for AIX Platforms, part number 819-6570-10

Sun Mainframe Security Facility Release 1.1.0

This document contains information about Release 1.1.0 of the Sun Mainframe Security Facility (Sun MSF) for AIX platforms. It contains the following topics:

- [“General Installation Information” on page 1](#)
- [“Documentation Advisory” on page 2](#)
- [“Important Operating Information” on page 2](#)
- [“Enhancements” on page 3](#)
- [“Changes from Previous Releases” on page 4](#)
- [“Known Problems and Limitations” on page 5](#)
- [“Documentation” on page 7](#)
- [“Documentation Errata” on page 7](#)

General Installation Information

Sun MSF Release 1.1.0 has been qualified on the AIX operating system, Release 5.2.

Sun MSF requires that Java™ release 1.4 with the latest patches, or release 1.5 (JDK 5.0) be installed.

The following relational databases have been qualified as the security repository:

- Oracle® relational database, Version 9.2
- IBM DB2 UDB, Version 8.1

Documentation Advisory

The *Sun Mainframe Security Facility Administrator's Guide* for this release contains information that does not apply to AIX platforms. Most of this information relates to functionality that is not qualified on the AIX platform. Other information is specific to the use of the product on Solaris™ platforms.

These release notes contain information that is applicable to AIX environments. Therefore, refer to this document if you are in doubt about whether a feature operates on AIX platforms.

Important Operating Information

This section contains information related to the operation of Sun MSF.

Deploying Behind a Firewall

To avoid possible data compromise when using Sun MTP with Sun MSF, you must deploy all components of Sun MSF, such as the security server and repository, and the Sun MTP regions behind a common firewall. You must also maintain sufficient internal safeguards to avoid exposure on the socket connections used. This precludes a socket port “sniffing” on an unprotected network.

Upgrading Sun MSF

If you are upgrading from Sun MSF 1.0.0 or 1.0.1, you must run the `msfconvdb` utility in order to use the existing repository database with the current release.

Shutting Down the Security Server

When shutting down the security system, the security server must be shut down before attempting to shut down the security loggers. If you try to shut down the security loggers first, the following warning message is issued:

```
[SecurityLogs]:WARNING:Security Loggers not terminated, Security  
Server still active
```

Enhancements

This section describes enhancements that have been made to Sun MSF since Release 1.0.1.

Configuration Utility

The Sun MSF configuration utility makes the task of configuring the Sun MSF environment easier. The configuration utility is invoked with the `msfconfig` command. Refer to the chapter “Configuring Sun MSF” in the *Sun Mainframe Security Facility Administrator’s Guide*.

“No Prompt” Option for Administering the Security Server

The `msfserver` administrative command has a new “no prompt” option that uses the UNIX user ID of the user executing the command. To use this new option, the Sun MSF repository must contain a principal entry for that UNIX user ID, with read and execute permission to the `ObjectReference` resource for the security server. Refer to the *Sun Mainframe Security Facility Administrator’s Guide* for more information.

New Utility for Updating Repository Passwords

This release of Sun MSF introduces the `msfupdkey` utility, which updates the `adapterAdmin` and `adapterUser` passwords on the Sun MSF key file. Use this utility when your site’s database administrator changes the passwords to the

database that serves as the Sun MSF security repository. Refer to the section “Updating Repository Passwords” in the *Sun Mainframe Security Facility Administrator’s Guide*.

User-Defined Resource Types

Sun MSF now fully supports user-defined resource types. Refer to the *Sun Mainframe Security Facility Administrator’s Guide*.

Changes from Previous Releases

Command Names Changed

Several of the Sun MSF command names have changed.

Old Name	New Name
ConvertDBP1toP2	msfconvdb
SecAdmin	msfadmin
MakeAnAdministrator	msfinitr
SecurityServer	msfserver
SecurityLogs	msflog

Password Encryption

As a result of password encryption changes, an open brace ({) cannot be the first character of any password. If you try to use the open brace in the commands `createPrincipal` or `resetPassword`, the password is rejected with the following message:

```
ERROR: Password format is not acceptable for principal:
principalname
```

New Error Messages

(SecSvc_017) Principal {0} account has expired.

Description: The named principal could not be authenticated because its account has expired.

Solution: Contact the Sun MSF administrator about having the account reactivated. A user cannot change the state of an account.

There is also a new Sun MTP error message that corresponds to this failure condition (KIX0542E). Refer to the *Sun Mainframe Transaction Processing Software Release Notes for AIX Platforms*.

Known Problems and Limitations

Check the SunSolveSM web site at <http://sunsolve.sun.com> on a regular basis for any Sun MSF patches that are available, and apply the recommended patches. The base number for patches to Release 1.1.0 is 122267.

Wildcard resources not documented in the Sun MSF documentation (ID 6262262)

Updated documentation will be provided in a future patch release.

KIX_PROGRAM ACCT04 in MTPprimerQueryTransactions, should be in MTPprimerQueryPrograms (ID 6285277)

When using the Sun MTP Primer sample application with Sun MSF, the `primerLoadFile.txt` file adds the ACCT04 program to the MTPprimerQueryTransactions resource domain instead of adding it to the MTPprimerQueryPrograms resource domain.

Change the following line in `primerLoadFile.txt` to correct this error:

```
ard,KIX_PROGRAM,ACCT04,MTPprimerQueryTransactions
```

to:

```
ard,KIX_PROGRAM,ACCT04,MTPprimerQueryPrograms
```

MSF samples are missing required permissions to run the MQ and/or JMS sample applications with MSF (ID 6286231)

- When using the Sun MTP MQ sample application with Sun MSF, the MQJV transaction must have read permission. The MQJV transaction is in the MTPadminTransactions resource domain. However, `suppliedLoadFile.txt` only adds execute and write permissions to the adminMTP role.

Change the following line in `suppliedLoadFile.txt` to correct this error:

```
arp,adminMTP,MTPadminTransactions,EXECUTE,WRITE
```

to:

```
arp,adminMTP,MTPadminTransactions,EXECUTE,WRITE,READ
```

- When using the Sun MTP MQ sample application with Sun MSF, the `suppliedLoadfile.txt` file does not assign any role permissions for `MTPadminPrograms`. The `adminMTP` role needs execute permissions to `MTPadminPrograms`. Add the following line in `suppliedLoadFile.txt` to correct this error:

```
arp,adminMTP,MTPadminPrograms,EXECUTE
```

Note – MQ applications are supported on AIX platforms, however, the MQ-JMS Bridge feature is not.

msfconfig does not configure a DB2 repository correctly. Wrong drivers are assigned. (ID 6427526)

The following procedure enables you to configure a DB2 UDB repository.

1. **Temporarily set the DB2 UDB environment variable `INSTHOME` to `$INSTHOME/sqlllib`.**
`$INSTHOME` normally identifies the DB2 UDB installation directory.
2. **Run the `msfconfig` utility and select a DB2 UDB repository.**
3. **When the `msfconfig` utility is complete, edit the file `$MSF_HOME/config/java.policy` and change the following line from:**

```
grant codebase "file:/database/db2inst1/sqlllib/java/db2java.zip"
{ permission java.security.AllPermission; };
```

to:

```
grant codebase "file:/database/db2inst1/sqlllib/java/db2jcc.jar"
{ permission java.security.AllPermission; };
```
4. **Edit the following values in the `MSFconfig.properties` file:**
 - a. **Change `com.sun.emp.security.adapterDriver=COM.ibm.db2.jdbc.app.DB2Driver` to `com.sun.emp.security.adapterDriver=com.ibm.db2.jcc.DB2Driver`**
 - b. **Change the file name in the `com.sun.emp.security.adapterPath` property from `db2java.zip` to `db2jcc.jar`.**

5. Reset the DB2 UDB `INSTHOME` environment variable to the original installation directory.

Documentation

The Sun MSF documentation has been removed from the *Sun Mainframe Transaction Processing Software Administrator's Guide*. The documentation for Sun MSF is the *Sun Mainframe Security Facility Administrator's Guide* (817-7448-10).

Documentation Errata

This section contains corrections and additions to the *Sun Mainframe Security Facility Administrator's Guide*.

Refreshing Users' Security Rules

The *Sun Mainframe Security Facility Administrator's Guide* contains incorrect information about refreshing users' security rules. It is not true that users rules are discarded when they log out; all rules are retained until a "refresh" is requested. Be aware that Sun MTP and Sun MSF have two distinct caches of rule information. The Sun MTP cache is a per-transaction server local cache, accumulated as each external security manager (ESM) request is made; and this cache is only discarded when a `CEMT PERFORM SECURITY REBUILD` command is executed. The Sun MSF cache is global to the security server, and is also accumulated as each user logs in and makes resource access requests.

The following paragraph replaces the first paragraph under "To Refresh Security Rules" in Chapter 6 of the *Sun Mainframe Security Facility Administrator's Guide*:

Sun MSF maintains its security rules in the security repository. The security server loads each user's access rules at login into a system-wide area of memory in the security server. These security rules stay in memory even after users have logged out. When the security rules change, this area of memory is not automatically updated, so the administrator must use the refresh command (`msfserver -r`) to instruct the security server to update this area of memory.

Security Server Statistics

The *Sun Mainframe Security Facility Administrator's Guide* does not provide information about the security server statistics that are the output of the `msfserver -p` command. A description of the output is provided below.

Output	Description
DumpEntries: global activity counters =====	
login: 1599	Total number of login requests received
logout: 1596	Total number of logout requests received
checkAccess: 2002	Total number of resource permission check requests received
hostUser: 17	Total number of pre-authenticated (UNIX) user ID notifications received
trustedServer: 11	Total number of trusted partner (for example, Sun MTP) handshake messages received
refresh: 1	Total number of refresh (<code>msfserver -r</code>) requests received
dump: 1	Total number of print statistics (<code>msfserver -p</code>) requests received
getEncryptionInfo: 1599	Total number of requests for user's password encryption specifics
invalidRequest: 0	Total number of unrecognized or illegal requests
exception: 0	Total number of times request resulted in a Java Exception response
=====	
DumpEntries: userSessionList contents =====	Summary of all current active users
UserSession: kadmin(null) sessionCount = 1	Total number of active sessions (logins) for this user
UserSession: kixadm(null) sessionCount = 9	Total number of active sessions (logins) for this user
=====	
DumpEntries: trustedServerList contents =====	Summary of all "trusted" partners and their users
TrustedServer: DirectSecurityServer	Name of trusted partner (this <code>msfserver -p</code> command)

Output	Description
serverCount = 1	Single partner process associated
TrustedUser: kadmin(null) sessionCount = 1	Number of active sessions for this user within this trusted partner
TrustedServer: /mfr/rehost/msf	Name of the group of trusted partner processes (Sun MTP region)
serverCount = 9	Current number of processes associated
TrustedUser: kixadm(null) sessionCount = 9	Number of active sessions for this user within this group of trusted partner processes
=====	

Note – The TrustedServer information is a useful summary of the active Sun MTP region’s users. There is also a 1-to-1 association of the number of transaction server processes in that region with the TrustedUser sessionCount for that region’s “default user.” In this example, “kixadm” is the region’s default user, and there is a match between the serverCount and that TrustedUser’s sessionCount.

Log Message Levels

The *Sun Mainframe Security Facility Administrator's Guide* lacked detailed information on log message levels. The log message level is set in the `MSFconfig.properties` file. The values are:

- 0 - Shows only FATAL level messages
- 1 - Shows ERROR, as well as FATAL, level messages
- 2 - Shows WARNING, as well as FATAL and ERROR, level messages
- 3 - Shows all levels of messages including INFO

Running with the `logMessageLevel` property set to 2 provides all access denials (FATAL), login failures (ERROR), and successful accesses and logins. It also includes any `msfadmin` updates completed (WARNING). It is typically not necessary to run with the `logMessageLevel` property set to 3, because INFO level messages include a detailed record of everything Sun MSF is seeing.