Oracle® Fusion Middleware

Troubleshooting Guide for Oracle Mobile Security Suite

Release 3.0.1

E51929-03

September 2014

This guide describes diagnostic tools and troubleshooting tips for Oracle Mobile Security Suite.

Oracle Fusion Middleware Troubleshooting Guide for Oracle Mobile Security Suite, Release 3.0.1

E51929-03

Primary Author: Ellen Desmond

Contributing Author: Vinaye Misra

Contributors: John Boyer, Mitch Frazier, Nicki Lee

Contents

6 Tips for Troubleshooting Kerberos-Enabled Applications

7 Microsoft SQL Server Troubleshooting Tips

8 Certificate Troubleshooting

9 Mobile Device Troubleshooting Tips

10 Mobile Security Administrative Console IIS Configuration

11 Mobile Security Notification Server

12 Troubleshooting Mobile Security Administrative Console LDAP Sync

13 Mobile Security Administrative Console Database Replication

Preface

Oracle Mobile Security Suite enables organizations to provide employees access to corporate data and applications from their mobile devices, to address the growing security needs created by the bring your own device (BYOD) movement.

Audience

This document is intended for administrators who manage Oracle Mobile Security Suite.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc`.

Access to Oracle Support

Oracle customers have access to electronic support through My Oracle Support. For information, visit `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info` or visit `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs` if you are hearing impaired.

Related Documents

For more information, see the following documents in the Oracle Mobile Security Suite documentation set:

- *Oracle Mobile Security Suite Administrative Console Guide*
- *Oracle Mobile Security Suite Application Containerization Tool Guide*
- *Oracle Mobile Security Suite Customization and Branding Guide*
- *Oracle Mobile Security Suite Installation Guide*
- *Oracle Mobile Security Suite Troubleshooting Guide*

Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

1

Introduction to Troubleshooting Oracle Mobile Security Suite

This chapter introduces diagnostic tools and troubleshooting tips for Oracle Mobile Security Suite.

This document contains chapters on the following topics:

- Oracle Mobile Security Suite Diagnostic Tool
- Gathering Server Logs for Support
- Mobile Security Access Server Troubleshooting Tips
- Tips for Troubleshooting Kerberos-Enabled Applications
- Microsoft SQL Server Troubleshooting Tips
- Certificate Troubleshooting
- Mobile Device Troubleshooting Tips
- Troubleshooting Mobile Security Administrative Console LDAP Sync
- Mobile Security Administrative Console Database Replication

The instructions in this document refer to file system paths on Microsoft Windows. The paths on Oracle Linux are slightly different. For example, the `/gateway` directory on Windows corresponds to the `/msas` directory on Linux and the `/acp` directory on Windows corresponds to the `/msac` directory on Linux. However, the troubleshooting techniques described in this document are equally relevant to Microsoft Windows and Oracle Linux installations.

2

Oracle Mobile Security Suite Diagnostic Tool

This chapter describes the Oracle Mobile Security Suite Diagnostic tool.

The Oracle Mobile Security Suite installation on Windows includes the diagnostic tool for troubleshooting the most common issues with the suite. After installation, this tool can be found in the distribution at:

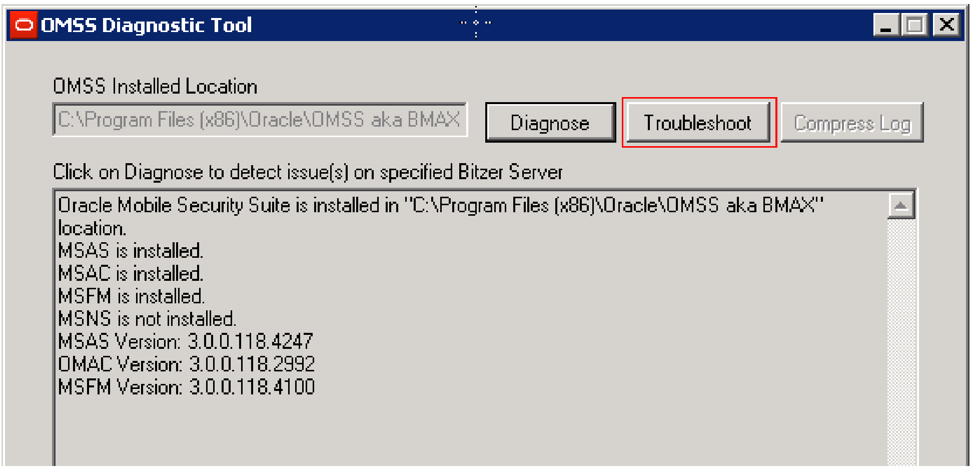
```
install_directory\omss\tools\OMSSDiagnosticTool.exe
```

This chapter contains the following sections:

- Section 2.1, "Installation Location Screen"
- Section 2.2, "Sample Output from the Diagnostic Tool"
- Section 2.3, "Tests for Installation Summary"
- Section 2.4, "Tests for Mobile Security Access Server"
- Section 2.5, "Tests for Mobile Security Administrative Console"
- Section 2.6, "Tests for Mobile Security File Manager and Notification Server"

2.1 Installation Location Screen

After starting the Diagnostic Tool, the Oracle Mobile Security Suite installation location is shown. Click the Diagnose button. The results can be copied and pasted into the clipboard.



OMSS Installed Location

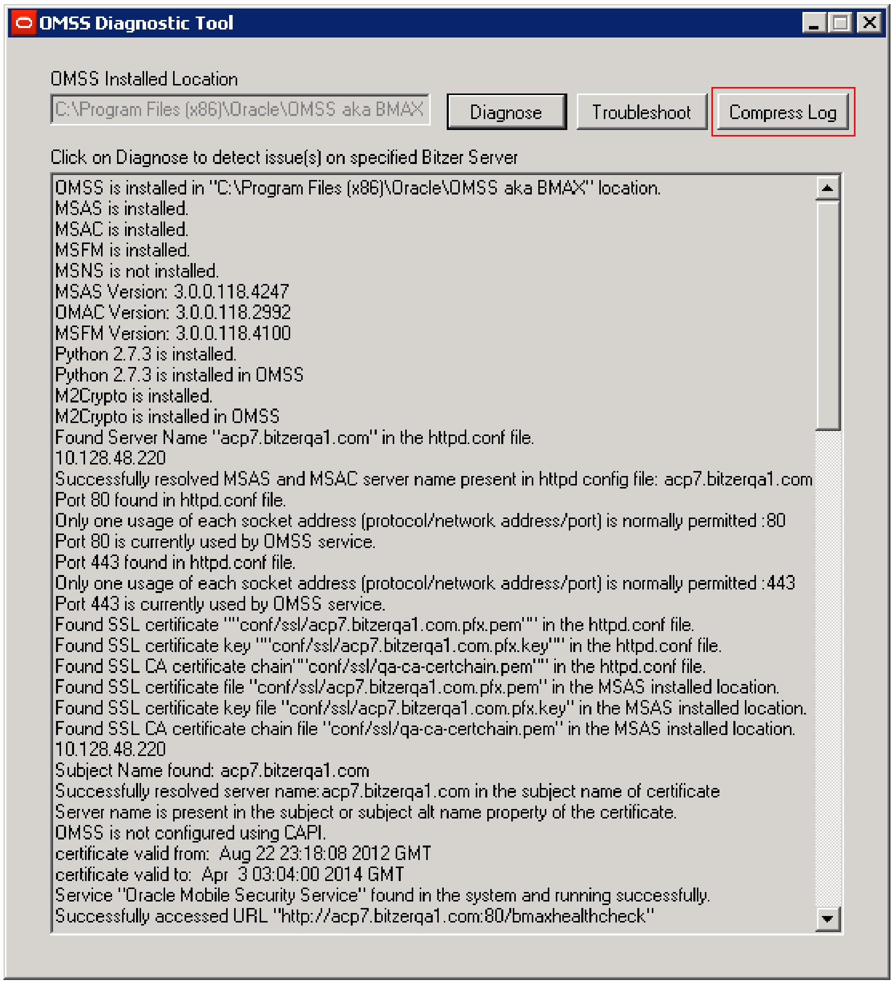
C:\Program Files (x86)\Oracle\OMSS aka BMAX

Click on Diagnose to detect issue(s) on specified Bitzer Server

```
Oracle Mobile Security Suite is installed in "C:\Program Files (x86)\Oracle\OMSS aka BMAX"
location.
MSAS is installed.
MSAC is installed.
MSFM is installed.
MSNS is not installed.
MSAS Version: 3.0.0.118.4247
OMAC Version: 3.0.0.118.2992
MSFM Version: 3.0.0.118.4100
```

2.2 Sample Output from the Diagnostic Tool

The following is an example of the output produced by the diagnostic tool for an operational Oracle Mobile Security Suite. In this example Mobile Security Access Server, Mobile Security Administrative Console, Mobile Security File Server, and Mobile Security Notification Server were installed on the same machine.


OMSS Diagnostic Tool
OMSS Installed Location
C:\Program Files (x86)\Oracle\OMSS aka BMAX
Diagnose
Troubleshoot
Compress Log
Click on Diagnose to detect issue(s) on specified Bitzer Server

```
OMSS is installed in "C:\Program Files (x86)\Oracle\OMSS aka BMAX" location.
MSAS is installed.
MSAC is installed.
MSFM is installed.
MSNS is not installed.
MSAS Version: 3.0.0.118.4247
OMAC Version: 3.0.0.118.2992
MSFM Version: 3.0.0.118.4100
Python 2.7.3 is installed.
Python 2.7.3 is installed in OMSS
M2Crypto is installed.
M2Crypto is installed in OMSS
Found Server Name "acp7.bitzerqa1.com" in the httpd.conf file.
10.128.48.220
Successfully resolved MSAS and MSAC server name present in httpd config file: acp7.bitzerqa1.com
Port 80 found in httpd.conf file.
Only one usage of each socket address (protocol/network address/port) is normally permitted :80
Port 80 is currently used by OMSS service.
Port 443 found in httpd.conf file.
Only one usage of each socket address (protocol/network address/port) is normally permitted :443
Port 443 is currently used by OMSS service.
Found SSL certificate ""conf/ssl/acp7.bitzerqa1.com.pfx.pem"" in the httpd.conf file.
Found SSL certificate key ""conf/ssl/acp7.bitzerqa1.com.pfx.key"" in the httpd.conf file.
Found SSL CA certificate chain""conf/ssl/qa-ca-certchain.pem"" in the httpd.conf file.
Found SSL certificate file "conf/ssl/acp7.bitzerqa1.com.pfx.pem" in the MSAS installed location.
Found SSL certificate key file "conf/ssl/acp7.bitzerqa1.com.pfx.key" in the MSAS installed location.
Found SSL CA certificate chain file "conf/ssl/qa-ca-certchain.pem" in the MSAS installed location.
10.128.48.220
Subject Name found: acp7.bitzerqa1.com
Successfully resolved server name:acp7.bitzerqa1.com in the subject name of certificate
Server name is present in the subject or subject alt name property of the certificate.
OMSS is not configured using CAPI.
certificate valid from:  Aug 22 23:18:08 2012 GMT
certificate valid to:  Apr  3 03:04:00 2014 GMT
Service "Oracle Mobile Security Service" found in the system and running successfully.
Successfully accessed URL "http://acp7.bitzerqa1.com:80/bmaxhealthcheck"
```

2.3 Tests for Installation Summary

The results are displayed in the window. The following tests summarize what is installed:

Test Name	Output/Description
Locate where Oracle Mobile Security Suite is installed	`Oracle Mobile Security Suite is installed in C:\Program Files (x86)\Oracle\OMSS.`
Mobile Security Access Server Version	`The version of Mobile Security Access Server installed 3.0.0.n.n`
Mobile Security Administrative Console (MSAC) Version	`The version of Mobile Security Administrative Console installed 3.0.0.n.n`

Test Name	Output/Description
Mobile Security File Manager Version	`The version of Mobile Security File Manager installed 3.0.0.n.n`
Mobile Security Notification Server Version	`The version of Mobile Security Notification Server installed 3.0.0.n.n`

Verifies components and supporting components installed	`Python 2.7.3 is installed.`
	`Python 2.7.3 is installed in Mobile Security Access Server`
	`M2Crypto is installed.`
	`M2Crypto is installed in Mobile Security Access Server`

2.4 Tests for Mobile Security Access Server

The following tests are performed for Mobile Security Access Server:

Name	Output/Description

Verify Server Name is in DNS:	`Found Server Name "bmaxdev.test.example.com" in httpd.conf file.`
	`Successfully resolved server name present in httpd config file bmaxdev.test.example.com`

Identify ports used by Mobile Security Access Server:	`Port 80 found in httpd.conf file.`
	`Port 80 is currently used by Mobile Security Access Server.`
	`Port 443 found in httpd.conf file.`
	`Port 443 is currently used by Mobile Security Access Server.`

Identify server certificates:	`Found SSL certificate "conf/ssl/bmaxdev.test.example.com-2k.pfx.pem" in the httpd.conf file.`
	`Found SSL certificate key "conf/ssl/bmaxdev.test.example.com-2k.pfx.key" in the httpd.conf file.`
	`Found SSL CA certificate chain "conf/ssl/devCA-FULL-Chain.cer" in the httpd.conf file.`
	`Found SSL certificate file "conf/ssl/bmaxdev.test.example.com-2k.pfx.pem" in the Mobile Security Access Server installed location.`
	`Found SSL certificate key file "conf/ssl/bmaxdev.test.example.com-2k.pfx.key" in the Mobile Security Access Server installed location.`
	`Found SSL CA certificate chain file "conf/ssl/devCA-FULL-Chain.cer" in the BMAX installed location.`

Identify Subject Alternative Names in certificate:	`Subject Name found: bmaxdev.test.example.com`
	`Subject Alternative Name found: bmaxdev.test.example.com`
	`Subject Alternative Name found: *.example.prod`
	`Subject Alternative Name found: *.example.dev`
	`Subject Alternative Name found: *.cod.example.dev`
	`Subject Alternative Name found: *.mw3.example.dev`

Validate the subject name in the certificate is in DNS	`Successfully resolved server name present in the subject property of certificate: bmaxdev.test.example.com`

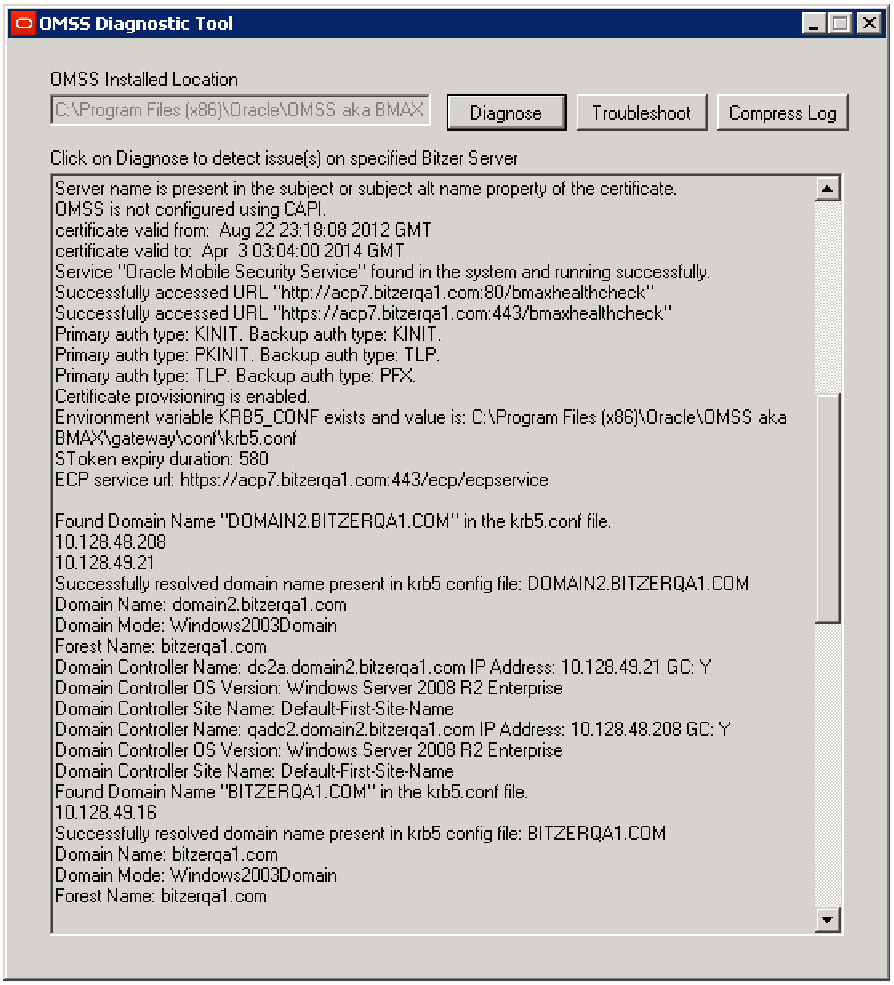
Name	Output/Description
Match Server Name with certificate used by Mobile Security Access Server:	Successfully resolved server name:bmaxdev.test.example.com in the subject name and alternative subject name of certificate Server name is present in the subject or subject alt name property of the certificate.
Displays if certificate is in Windows Certificate store	Mobile Security Access Server is not configured using CAPI
Show Certificate validation dates:	certificate valid from: May 28 06:45:45 2012 GMT certificate valid to: May 28 06:45:45 2014 GMT
Verify that Mobile Security Access Server is running	Service "OMSS" found in the system and running successfully
Test Mobile Security Access Server:	Server name is present in the subject or subject alt name property of the certificate. Service "OMSS" found in the system and running successfully. Successfully accessed URL "http://bmaxdev.test.example.com/bmaxhealthcheck" Successfully accessed URL "https://bmaxdev.test.example.com/bmaxhealthcheck" Successfully accessed URL "https://bmaxdev.test.example.com:443/bmaxhealthcheck"
Report authentication configuration:	Primary auth type: KINIT. Backup auth type: KINIT Primary auth type: OTP. Backup auth type: KINIT Primary auth type: PKINIT. Backup auth type: TLP Primary auth type: OAM. Backup auth type: OAM
Verify that KRB5 environment: Environment variable KRB5_CONF exists and value is: C:\Program Files (x86)\Oracle\OMSS	\Program Files (x86)\Oracle\OMSS\gateway\conf\krb5.conf
Display the secure token expiration duration in minutes.	SToken expiry duration: 580
Verify Kerberos Realm/Active Directory domain, Forest and domain functional levels of each controller in the domain. Indicates if the domain controller is a Global Catalog for Active Directory. The version of Windows for the domain controller, and the Active Directory site Mobile Security Access Server will access:	Found Domain Name " bitzermobile.dev" in the krb5.conf file. 192.168.100.61 192.168.100.60 Successfully resolved domain name present krb5 config file: bitzermobile.dev Domain Mode: Windows2003Domain Forest Name: bitzermobile.dev Domain Controller Name: b-devdc1.bitzermobile.dev IP Address: 192.168.100.60 GC: Y Domain Controller OS Version: Windows Server 2008 R2 Standard Domain Controller Site Name: Default-First-Site-Name Domain Controller Name: b-devdc2.bitzermobile.dev IP Address: 192.168.100.61 GC: Y Domain Controller OS Version: Windows Server 2008 R2 Standard Domain Controller Site Name: Default-First-Site-Name

Name	Output/Description

Display the Radius servers when Radius is configured in Mobile Security Access Server:	`RADIUS Authentication server: win-rsa`
	`Default realm:`

Displays information on the integration between Mobile Security Access Server and Mobile Security Administrative Console:	`Cron job bmax_updater summary: bmax_updater 7/30/2013 4:49:00 PM Ready`
	`ECP service url: https://bmaxdev.test.example.com:443/ecp/ecpservice`

Sample output is as follows:


OMSS Diagnostic Tool
OMSS Installed Location
C:\Program Files (x86)\Oracle\OMSS aka BMAX
Diagnose
Troubleshoot
Compress Log
Click on Diagnose to detect issue(s) on specified Bitzer Server

```
Server name is present in the subject or subject alt name property of the certificate.
OMSS is not configured using CAPI.
certificate valid from:  Aug 22 23:18:08 2012 GMT
certificate valid to:  Apr  3 03:04:00 2014 GMT
Service "Oracle Mobile Security Service" found in the system and running successfully.
Successfully accessed URL "http://acp7.bitzerqa1.com:80/bmaxhealthcheck"
Successfully accessed URL "https://acp7.bitzerqa1.com:443/bmaxhealthcheck"
Primary auth type: KINIT. Backup auth type: KINIT.
Primary auth type: PKINIT. Backup auth type: TLP.
Primary auth type: TLP. Backup auth type: PFX.
Certificate provisioning is enabled.
Environment variable KRB5_CONF exists and value is: C:\Program Files (x86)\Oracle\OMSS aka
BMAX\gateway\conf\krb5.conf
SToken expiry duration: 580
ECP service url: https://acp7.bitzerqa1.com:443/ecp/ecpservice

Found Domain Name "DOMAIN2.BITZERQA1.COM" in the krb5.conf file.
10.128.48.208
10.128.49.21
Successfully resolved domain name present in krb5 config file: DOMAIN2.BITZERQA1.COM
Domain Name: domain2.bitzerqa1.com
Domain Mode: Windows2003Domain
Forest Name: bitzerqa1.com
Domain Controller Name: dc2a.domain2.bitzerqa1.com IP Address: 10.128.49.21 GC: Y
Domain Controller OS Version: Windows Server 2008 R2 Enterprise
Domain Controller Site Name: Default-First-Site-Name
Domain Controller Name: qadc2.domain2.bitzerqa1.com IP Address: 10.128.48.208 GC: Y
Domain Controller OS Version: Windows Server 2008 R2 Enterprise
Domain Controller Site Name: Default-First-Site-Name
Found Domain Name "BITZERQA1.COM" in the krb5.conf file.
10.128.49.16
Successfully resolved domain name present in krb5 config file: BITZERQA1.COM
Domain Name: bitzerqa1.com
Domain Mode: Windows2003Domain
Forest Name: bitzerqa1.com
```

2.5 Tests for Mobile Security Administrative Console

The following test are performed for the Mobile Security Administrative Console:

Name	Output/Description
Database used by Mobile Security Administrative Console	`Microsoft SQL server is used in this example: The mssql database is used for Mobile Security Administrative Console.`

Name	Output/Description

Company Name and ID assigned by Oracle:	`Company Name: Your Company`
	`Company ID: 2308481841`

SQL Server information:	`SQL Server host name: devsql.bitzermobile.dev\sql1`
	`SQL Server schema name: dbo`
	`SQL Server instance name: sql1`
	`SQL Server port number:`
	`Note: No port means default port used (1443)`
	`SQL service authentication type: win`

Mobile Security Administrative Console Admin application database name	`lattice_bmaxdev_24_107`
Mobile Security Administrative Console reporting application database name	`reporting_bmaxdev_24_107`
Mobile Security Administrative Console audit application database name	`audit_bmaxdev_24_107`

SQL service authentication method used by Mobile Security Administrative Console:	`In this example windows authentication was used:`
	`SQL service authentication type: win`

Reports on scheduled tasks that run and their status:	`Cron job dashboard_summary summary: dashboard_summary 7/30/2013 5:28:00 PM Ready`
	`Cron job map_latlong summary: map_latlong 7/30/2013 5:33:00 PM Ready`
	`Cron job container_inactivity_action summary: container_inactivity_action 7/30/2013 5:13:00 PM Ready`

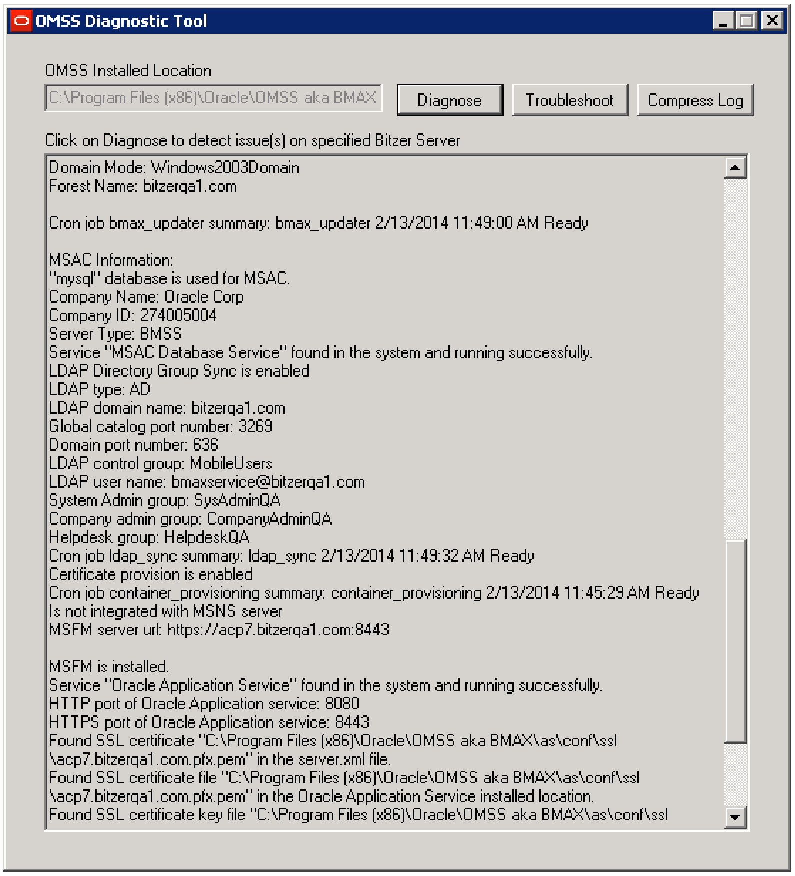
Indicates if LDAP mapping to Mobile Security Administrative Console groups is enabled:	`LDAP Group Sync is enabled`
	`LDAP domain name: bitzermobile.dev`

Specifies the Control Group used to register devices when LDAP Sync is enabled	`LDAP control group: Mobile Users`
Displays the credentials that are used to access LDAP when LDAP Sync is enabled.	`LDAP user name: user1@example.dev`

Displays the Mobile Security Administrative Console access groups:	`System Admin group: Bitzer_system_admin`
	`Company admin group: Bitzer_company_admin`
	`Helpdesk group: Bitzer_helpdesk`

Display background tasks and status:	`Cron job ad_sync summary: ad_sync 7/30/2013 4:40:00 PM Ready`
	`Certificate provision is enabled`
	`Cron job container_provisioning summary: container_provisioning 7/30/2013 4:39:00 PM Ready`

Here is sample output for the Mobile Security Administrative Console from the diagnostic tool:



OMSS Installed Location

C:\Program Files (x86)\Oracle\OMSS aka BMAX

Click on Diagnose to detect issue(s) on specified Bitzer Server

```
Domain Mode: Windows2003Domain
Forest Name: bitzerqa1.com

Cron job bmax_updater summary: bmax_updater 2/13/2014 11:49:00 AM Ready

MSAC Information:
"mysql" database is used for MSAC.
Company Name: Oracle Corp
Company ID: 274005004
Server Type: BMSS
Service "MSAC Database Service" found in the system and running successfully.
LDAP Directory Group Sync is enabled
LDAP type: AD
LDAP domain name: bitzerqa1.com
Global catalog port number: 3269
Domain port number: 636
LDAP control group: MobileUsers
LDAP user name: bmaxservice@bitzerqa1.com
System Admin group: SysAdminQA
Company admin group: CompanyAdminQA
Helpdesk group: HelpdeskQA
Cron job ldap_sync summary: ldap_sync 2/13/2014 11:49:32 AM Ready
Certificate provision is enabled
Cron job container_provisioning summary: container_provisioning 2/13/2014 11:45:29 AM Ready
Is not integrated with MSNS server
MSFM server url: https://acp7.bitzerqa1.com:8443

MSFM is installed.
Service "Oracle Application Service" found in the system and running successfully.
HTTP port of Oracle Application service: 8080
HTTPS port of Oracle Application service: 8443
Found SSL certificate "C:\Program Files (x86)\Oracle\OMSS aka BMAX\as\conf\ssl
\acp7.bitzerqa1.com.pfx.pem" in the server.xml file.
Found SSL certificate file "C:\Program Files (x86)\Oracle\OMSS aka BMAX\as\conf\ssl
\acp7.bitzerqa1.com.pfx.pem" in the Oracle Application Service installed location.
Found SSL certificate key file "C:\Program Files (x86)\Oracle\OMSS aka BMAX\as\conf\ssl
```

2.6 Tests for Mobile Security File Manager and Notification Server

The following tests are performed for Mobile Security File Manager and Mobile Security Notification Server:

Name	Output/Description

Mobile Security Notification Server and Mobile Security File Manager configuration:	`Mobile Security Notification Server url: https://bmaxdev.test.example.com:8443/bns`
	`Mobile Security Notification Server uid: bmaxservice@bitzermobile.dev`
	`Mobile Security File Manager server url: https://bmaxdev.test.example.com:8443`
	`Mobile Security File Manager is installed.`
	`Mobile Security Notification Server is installed.`

State of servers running or stopped	`Service "Oracle Application Server" found in the system and running successfully`

Ports used by servers	`HTTP port of Oracle Application Server:8080`
	`HTTPS port of Oracle Application Server: 8443`

Name	Output/Description
Public Certificates used for SSL operations	Found SSL certificate "C:\Program Files (x86)\Oracle\OMSS\as\conf\ssl\bmax3-dev-gateway-cert.pfx.pem" in the server.xml file. Found SSL certificate file "C:\Program Files (x86)\Oracle\OMSS\as\conf\ssl\bmax3-dev-gateway-cert.pfx.pem" in the Oracle Application Server installed location. Found SSL certificate key file
Private Keys used for SSL operations	"C:\Program Files (x86)\Oracle\OMSS\as\conf\ssl\bmax3-dev-gateway-cert.pfx.key" in the server.xml file. Found SSL certificate key file "C:\Program Files (x86)\Oracle\OMSS\as\conf\ssl\bmax3-dev-gateway-cert.pfx.key" in the Oracle Application Server installed location
Certificate chain used for server	Found SSL CA chain certificate file "C:\Program Files (x86)\Oracle\OMSS\as\conf\ssl\bitzerdev-CAchain.pem" in the Oracle Application Server installed location Found SSL CA chain certificate file "C:\Example\OMSS\as\conf\ssl\bitzerdev-CAchain.pem" in the server.xml file.
Database used for Mobile Security Notification Server is MSSQL	Microsoft SQL server is used in this example: "mssql" database is used for Mobile Security Notification Server
Mobile Security Notification Server SQL Server information	Database is used for Mobile Security Notification Server: MSSQL Database host name: devsql.example.dev Database port number: Database name: bns_bmaxdev_24_107 Database instance name: sql1 Note: No port means default port used (1443) Windows authentication was selected
Mobile Security Notification Server service account	Mobile Security Notification Server Service user name: bmaxservice@bitzermobile.dev

3

Gathering Server Logs for Support

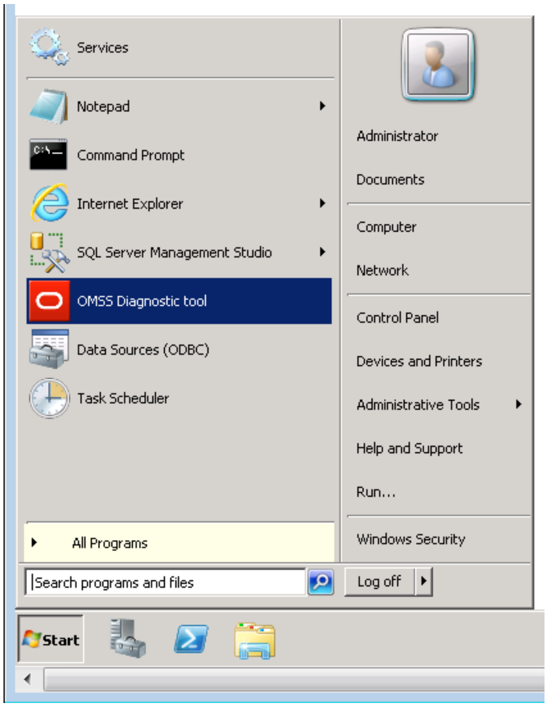
This chapter describes how to gather server logs for Windows installations for troubleshooting Oracle Mobile Security Suite.

This chapter contains the following sections:

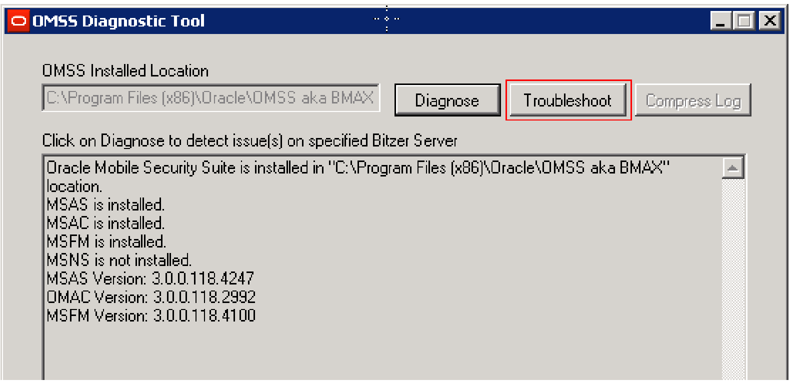
- Section 3.1, "Turn on Debug Level Logging"
- Section 3.2, "Collect Logs"
- Section 3.3, "About Mobile Security Access Server Logs"
- Section 3.4, "About Mobile Security Administrative Console Logs"
- Section 3.5, "About Mobile Security Container Logs"

3.1 Turn on Debug Level Logging

To turn on debug level logging, you use the Oracle Mobile Security Suite Diagnostic Tool.



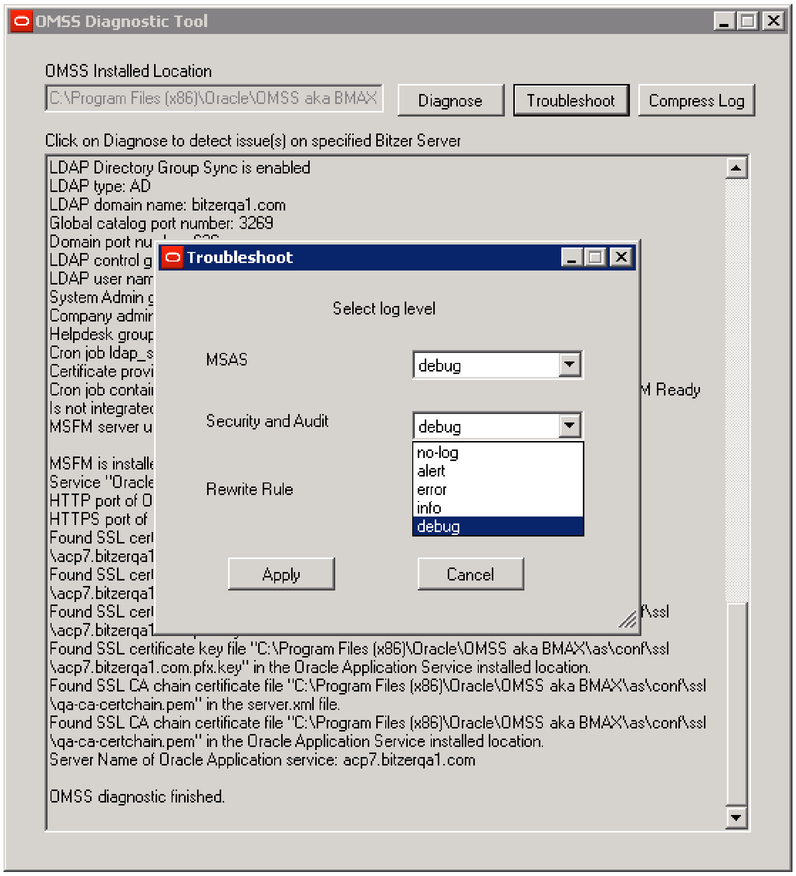
Click **Troubleshoot**.



OMSS Installed Location: C:\Program Files (x86)\Oracle\OMSS aka BMAX

Click on Diagnose to detect issue(s) on specified Bitzer Server

```
Oracle Mobile Security Suite is installed in "C:\Program Files (x86)\Oracle\OMSS aka BMAX"
location.
MSAS is installed.
MSAC is installed.
MSFM is installed.
MSNS is not installed.
MSAS Version: 3.0.0.118.4247
OMAC Version: 3.0.0.118.2992
MSFM Version: 3.0.0.118.4100
```



OMSS Installed Location: C:\Program Files (x86)\Oracle\OMSS aka BMAX

Click on Diagnose to detect issue(s) on specified Bitzer Server

```
LDAP Directory Group Sync is enabled
LDAP type: AD
LDAP domain name: bitzerqa1.com
Global catalog port number: 3269
Domain port nu
LDAP control g
LDAP user nam
System Admin g
Company admir
Helpdesk group
Cron job ldap_s
Certificate provi
Cron job contai
Is not integrated
MSFM server u

MSFM is installe
Service "Oracle
HTTP port of O
HTTPS port of
Found SSL cert
\acp7.bitzerqa1
Found SSL cert
\acp7.bitzerqa1
Found SSL cert
\acp7.bitzerqa1
Found SSL certificate key file "C:\Program Files (x86)\Oracle\OMSS aka BMAX\as\conf\ssl
\acp7.bitzerqa1.com.pfx.key" in the Oracle Application Service installed location.
Found SSL CA chain certificate file "C:\Program Files (x86)\Oracle\OMSS aka BMAX\as\conf\ssl
\qa-ca-certchain.pem" in the server.xml file.
Found SSL CA chain certificate file "C:\Program Files (x86)\Oracle\OMSS aka BMAX\as\conf\ssl
\qa-ca-certchain.pem" in the Oracle Application Service installed location.
Server Name of Oracle Application service: acp7.bitzerqa1.com

OMSS diagnostic finished.
```

Select log level

MSAS: debug

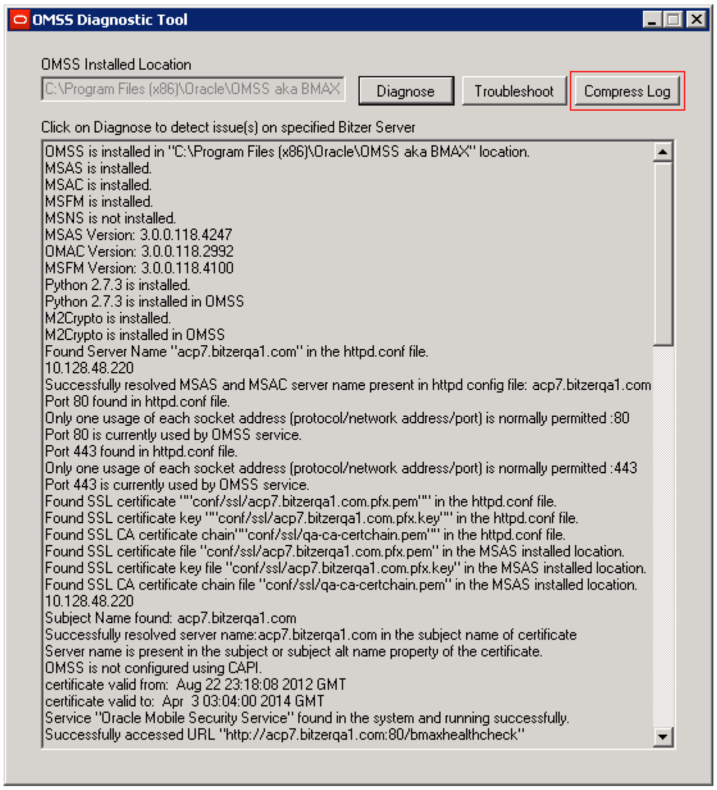
Security and Audit: debug
- no-log
- alert
- error
- info
- debug

Rewrite Rule

After reproducing the issue you have encountered, reduce the log level to its previous setting in a production environment, unless instructed otherwise by Oracle.

3.2 Collect Logs

To collect logs, click **Compress Log**.

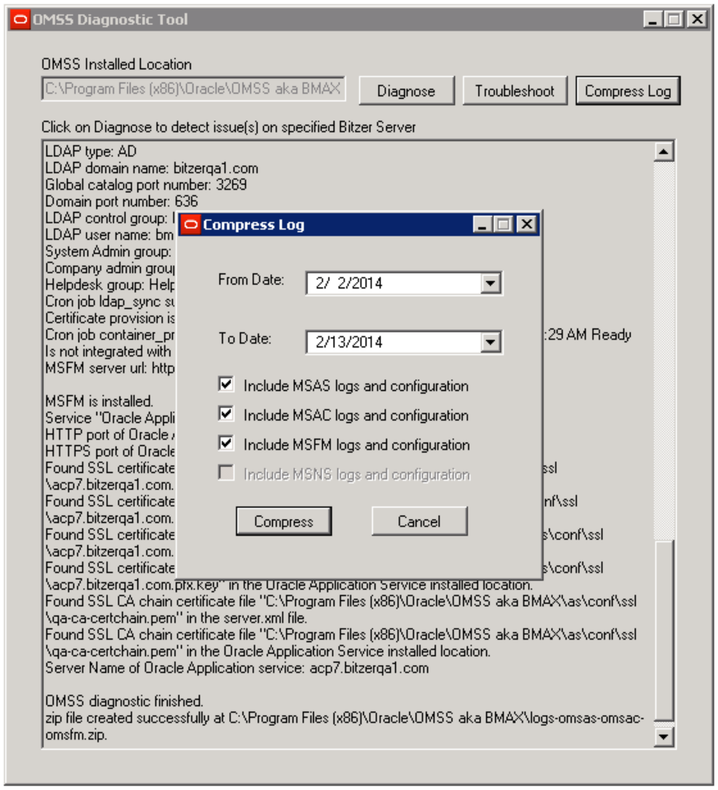


OMSS Installed Location: C:\Program Files (x86)\Oracle\OMSS aka BMAX

Click on Diagnose to detect issue(s) on specified Bitzer Server

```
OMSS is installed in "C:\Program Files (x86)\Oracle\OMSS aka BMAX" location.
MSAS is installed.
MSAC is installed.
MSFM is installed.
MSNS is not installed.
MSAS Version: 3.0.0.118.4247
OMAC Version: 3.0.0.118.2992
MSFM Version: 3.0.0.118.4100
Python 2.7.3 is installed.
Python 2.7.3 is installed in OMSS
M2Crypto is installed.
M2Crypto is installed in OMSS
Found Server Name "acp7.bitzerqa1.com" in the httpd.conf file.
10.128.48.220
Successfully resolved MSAS and MSAC server name present in httpd config file: acp7.bitzerqa1.com
Port 80 found in httpd.conf file.
Only one usage of each socket address (protocol/network address/port) is normally permitted :80
Port 80 is currently used by OMSS service.
Port 443 found in httpd.conf file.
Only one usage of each socket address (protocol/network address/port) is normally permitted :443
Port 443 is currently used by OMSS service.
Found SSL certificate ""conf/ssl/acp7.bitzerqa1.com.pfx.pem"" in the httpd.conf file.
Found SSL certificate key ""conf/ssl/acp7.bitzerqa1.com.pfx.key"" in the httpd.conf file.
Found SSL CA certificate chain""conf/ssl/qa-ca-certchain.pem"" in the httpd.conf file.
Found SSL certificate file "conf/ssl/acp7.bitzerqa1.com.pfx.pem" in the MSAS installed location.
Found SSL certificate key file "conf/ssl/acp7.bitzerqa1.com.pfx.key" in the MSAS installed location.
Found SSL CA certificate chain file "conf/ssl/qa-ca-certchain.pem" in the MSAS installed location.
10.128.48.220
Subject Name found: acp7.bitzerqa1.com
Successfully resolved server name:acp7.bitzerqa1.com in the subject name of certificate
Server name is present in the subject or subject alt name property of the certificate.
OMSS is not configured using CAPI.
certificate valid from:  Aug 22 23:18:08 2012 GMT
certificate valid to:  Apr  3 03:04:00 2014 GMT
Service "Oracle Mobile Security Service" found in the system and running successfully.
Successfully accessed URL "http://acp7.bitzerqa1.com:80/bmaxhealthcheck"
```

The following dialog is shown:



OMSS Installed Location: C:\Program Files (x86)\Oracle\OMSS aka BMAX

Click on Diagnose to detect issue(s) on specified Bitzer Server

```
LDAP type: AD
LDAP domain name: bitzerqa1.com
Global catalog port number: 3269
Domain port number: 636
LDAP control group: l
LDAP user name: bm
System Admin group:
Company admin grou
Helpdesk group: Help
Cron job ldap_sync su
Certificate provision is
Cron job container_pr                                       :29 AM Ready
Is not integrated with
MSFM server url: http

MSFM is installed.
Service "Oracle Appli
HTTP port of Oracle /
HTTPS port of Oracle
Found SSL certificate                                       ssl
\acp7.bitzerqa1.com.
Found SSL certificate                                       nf\ssl
\acp7.bitzerqa1.com.
Found SSL certificate                                       s\conf\ssl
\acp7.bitzerqa1.com.
Found SSL certificate                                       s\conf\ssl
\acp7.bitzerqa1.com.pfx.key" in the Oracle Application Service installed location.
Found SSL CA chain certificate file "C:\Program Files (x86)\Oracle\OMSS aka BMAX\as\conf\ssl
\qa-ca-certchain.pem" in the server.xml file.
Found SSL CA chain certificate file "C:\Program Files (x86)\Oracle\OMSS aka BMAX\as\conf\ssl
\qa-ca-certchain.pem" in the Oracle Application Service installed location.
Server Name of Oracle Application service: acp7.bitzerqa1.com

OMSS diagnostic finished.
zip file created successfully at C:\Program Files (x86)\Oracle\OMSS aka BMAX\logs-omsas-omsac-
omsfm.zip.
```

From Date: 2/ 2/2014

To Date: 2/13/2014

☑ Include MSAS logs and configuration

☑ Include MSAC logs and configuration

☑ Include MSFM logs and configuration

☐ Include MSNS logs and configuration

This dialog is used to easily collect information for each component, with the corresponding configuration. Depending on the size of the logs, this might take some time. After the collection is complete a zip file containing the logs and configuration files can be found in `installation_directory\OMSS`, for example: `C:\Program Files (x86)\Oracle\OMSS`.

3.3 About Mobile Security Access Server Logs

By default, Mobile Security Access Server logs are found in:

install directory`\OMSS\gateway\logs`

For example:

`C:\Program Files (x86)\Oracle\OMSS\gateway\logs`

The following logs are created:

- `access.log`
- `error.log`
- `rewrite.log`

Logs are rolled over once a day, and are time-stamped with the date.

3.3.1 The Access Log

`access.log` contains one line per request that is made to the Mobile Security Access Server.

The following table shows the format of access.log:

Field	Format	Example	Direct Request	Proxy Request
Remote IP Address	IPv4 or IPv6 address	`201.255.17.230`	Present	Present
Remote log name	-	-	-	-
User Identifier	User principal name	`jdoe@example.com`	Present for authenticated requests	Present for authenticated requests
Time of Request	[*DD*/*Mmm*/*YYYY*:*HH*:*MM*:*SS* -*GMT*]	`[18/Sep/2013:05:27:36 -0500]`	Present	Present
Request line	"*HTTPCMD PATH* HTTP/1.1"	`"GET / HTTP/1.1"`	Present	Present, path is always "/"
Proxy Request Scheme	http or https	`http`	-	Present
Proxy Request URL	URL encoding of hostname/path	`host.example.com%2Fsites%2Fsearch%2FPages%2Fdefault.aspx`	-	Present
HTTP Status Response	HTTP Status Code	`200`	Present	Present
Connection Status	X means connection aborted + means connection kept alive - means connection closed	`+`	Present	Present
Size of Response	Size of Response in bytes	`15645`	Present	Present
Request Processing Time	Time to process request in microseconds	`1060827`	Present	Present
Request Thread ID	Thread ID	`3448`	Present	Present

3.3.2 The Error Log

`error.log` contains detailed information, depending on the configured level:

- Default log level is `info`, sufficient to diagnose common problems.
- Log level can be increased to `debug` in the Diagnostic Tool to investigate complex problems.

3.4 About Mobile Security Administrative Console Logs

The following table shows the locations of Mobile Security Administrative Console logs:

Log Type	Location of Log
Installation	*install directory*\install.log
Mobile Security Administrative Console	*install directory*\ACP\logs
User Interface (UI)	*install directory*\ACP\logs\acp-console\
Web service	*install directory*\ACP\logs\ecpservice\
LDAP sync	*install directory*\ACP\logs\ldap-sync\
Scheduled task	*install directory*\ACP\logs\scheduled-tasks\

Logs are rolled over once a day, and are time-stamped with the date.

By default the logs do not contain much detail. Increase the log level to `debug` in Mobile Security Administrative Console for troubleshooting.

3.5 About Mobile Security Container Logs

Client logs can be e-mailed using the "Send logs" function – this will package all necessary client logs.

The log level can be set to "verbose" in the Container app settings to gather detailed logs for troubleshooting.

4 Common Troubleshooting Tips

This chapter describes how to address common issues with Oracle Mobile Security Suite.

The following is a list of common troubleshooting issues that are observed in actual deployments:

- Ports not opened (incoming and outgoing from Access Server)
- Ports blocked either by an external firewall, an application firewall, or `iptables` configuration
- Host names not resolving, DNS problems
- Users do not know how to get server certificates
- Access Server cert not trusted on mobile device
- The clock on the Mobile Security Access Server and the Windows domain controller are out of sync
- Users type in UID, not full UPN
- Back end applications do not have Kerberos SPNs properly defined
- Container and containerized apps signed with different certificates
- When building container static library project, selecting a build target of simulator or a connected device instead of generic iOS device
- Trying to do PKINIT with older Windows version, prior to Win2k8R2
- Incorrect user certificate templates
- Incorrect web settings that send everything direct, or block everything
- When running servers with a domain account, insufficient privileges
  - Missing batch logon or run as service privilege
  - Missing LDAP logon privilege
  - Missing privilege to issue certificate template for users
  - Missing privilege to revoke certificates on the CA
- Missing LDAP groups to map admin groups when starting installation
- Missing trust relationships in multi-domain environments
- Use of alternate UPN suffixes with KINIT (requires configuration change)
- Some back end servers running very old SSL stacks that cannot handle newer ciphers reported by the Access Server (requires configuration change)

- Old or low-end Android devices

5 Mobile Security Access Server Troubleshooting Tips

This chapter describes troubleshooting tips for Oracle Mobile Security Access Server.

This chapter contains the following sections:

- Section 5.1, "SSL Troubleshooting"
- Section 5.2, "Connection Error Troubleshooting"

5.1 SSL Troubleshooting

- Ensure that Mobile Security Access Server certificate is in PEM format (base 64).
- Ensure that Mobile Security Access Server certificate and certificate chain are not revoked.
- If the Mobile Security Access Server certificate contains a Subject Alternate Name, ensure that the server certificate subject name is also in the Subject Alternate Name (SAN) attribute of the certificate.
- Ensure that all Subject Names/Subject Alternative Names are resolved by DNS.
- Ensure that certificate chain file is built with Issuing CA, followed by Intermediate CA(s) and then the Root CA in PEM format if there are multiple CAs in the chain.

5.2 Connection Error Troubleshooting

- Ensure that the mobile device is online/connected to the Internet.
- Ensure that the Mobile Security Access Server is running. Depending on your configuration, the site may have up to three Windows services running:
  - `OMSS`, if Mobile Security Access Server or Administrative Console are installed;
  - `Oracle Application Server`, if Mobile Security Notification Server or File Manager are installed;
  - `OMSS Database Service`, if Mobile Security Administrative Console with MySQL is installed.
- Ensure that all necessary Mobile Security Access Server ports are open on the host firewall or other firewalls in the route from the mobile device to the Mobile Security Access Server.
- Ensure that no other services are using the configured Mobile Security Access Server ports. The Oracle Mobile Security Suite Diagnostics Tool performs this task, but the following command lines can also be helpful.

1. Stop the OMSS Windows service.
2. Open command line and type:

   ```
   netstat -a -n -o
   ```

   to verify that nothing is listening on Mobile Security Access Server ports (defaults 80 and 443)
3. Start the OMSS Windows service.
4. Type:

   ```
   netstat -a -n -o
   ```

   to verify that Mobile Security Access Server is listening on ports (defaults 80, 443, and 7443)

- Ensure that the applications behind Mobile Security Access Server are accessible from Mobile Security Access Server.
- Ensure that Mobile Security Access Server can resolve in DNS the host names of the applications behind Mobile Security Access Server.
- If the connection error occurs for only a single application behind Mobile Security Access Server, ensure that the application is running.
- Ensure that the Mobile Security Administrative Console service account credentials match between the Mobile Security Access Server and the Mobile Security Administrative Console server.
- Ensure that there are no systems in the network blocking proxy traffic (if a firewall or reverse proxy is configured).

6

Tips for Troubleshooting Kerberos-Enabled Applications

This chapter lists tips for troubleshooting Kerberos-enabled applications

The tips are as follows:

1. Web applications that are accessed through the Mobile Security Access Server must be configured for Kerberos with a Service Principal Name (SPN) for each application server that is accessed by an alias instead of its host name.

   For example, if `hostname` is `bmax1.oracle.internal` but is accessed as `http://sharepoint.oracle.internal`, the SPN must be `http://sharepoint.` Additional certificate requirements apply for the Mobile Security Access Server certificate.

   From a machine within the domain of the application server (Mobile Security Access Server can be used if it is joined to the same domain):

   a. Open a command window.

   b. At the command-line prompt, type:

      ```
      setspn  -l customer_application_hostname
      ```

   c. Verify that there is an SPN for the URL the device is trying to access

   d. If the SPN is missing, then type:

      ```
      setspn -a customer_application_hostname
      ```

   e. Verify the SPN by typing:

      ```
      setspn  -l customer_application_hostname
      ```

2. IIS applications such as SharePoint must be configured for Negotiate authentication, which can be followed by NTLM authentication if desired.

3. IIS applications use an application pool with an application-pool identity. This pool cannot be a local account on the web server. Typically, it can be set to a built-in account of `NETWORK` that has permission to access the Active Directory for authentication. When a service account is used for the pool identity, ensure that the account has permission to access and authenticate to Active Directory.

   a. Ensure that the authentication provider is set to `Negotiate`.

   b. Ensure that Windows authentication is set.

   c. Ensure that Anonymous User is NOT set.

Note: The following commands are useful to debug network issues with Wireshark:

1. In display filter, type:

   ```
   kerberos
   ```

2. In display filter, type:

   ```
   ntlmssp
   ```

3. In display filter, type:

   ```
   http
   ```

7

Microsoft SQL Server Troubleshooting Tips

This chapter describes troubleshooting tips for Microsoft SQL Server.

During installation of Mobile Security Administrative Console, Microsoft SQL Server may be chosen as a database and depending on the SQL configuration multiple authentication and connection errors can occur.

Open a command line window and enter a `runas` command using the service account. When a new command window opens, enter:

```
sqlcmd /?
```

In this example, the Mobile Security Administrative Console did not launch due to a database error. Mobile Security Administrative Console tries to access the SQL instance based upon what was entered in the installer for the MS SQL Server.

Execute the `runas` command, which opens a new command line window, as follows:

```
runas /env /user:yourserviceaccount@example.com cmd

sqlcmd -S devsql\sql2,1433
Msg 18456, Level 14, State 1, Server DEVSQL, Line 1
Login failed for user 'BITZERDEV\acpservice'.
sqlcmd -S devsql\sql2,1433 -d lattice
Msg 18456, Level 14, State 1, Server DEVSQL, Line 1
Login failed for user 'BITZERDEV\acpservice'.
```

To increase security, the error message that is returned to the client by SQL Server deliberately hides the nature of the authentication error. However, in the SQL Server error log the correct reason can be found. In this type of error, check the instance logs first. If the error is not found then check the default or base SQL management logs to find the error. Here is an example log.

```
08/12/2012 13:08:54,Logon,Unknown,Error: 18456<c/> Severity: 14<c/> State: 11.
08/12/2012 13:08:38,Logon,Unknown,Login failed for user 'BITZERDEV\acpservice'.
Reason: Token-based server access validation failed with an infrastructure error.
Check for previous errors. [CLIENT: 192.168.100.73]
```

The key to the message is the State which the server will accurately set to reflect the source of the problem. In the example above, State 11 indicates the wrong port is used to access the database, which was caused by the wrong port being specified during setup.

The common error states and their descriptions are provided in the following table:

Error State	Description
1	Error information is not available. This state usually means you do not have permission to receive the error details
2 and 5	Invalid userid
6	Attempt to use a Windows login name with SQL Authentication
7	Login disabled and password mismatch
8	Password mismatch
9	Invalid password
11 and 12	Valid login but server access failure
13	SQL Server service paused
18	Change password required

8

Certificate Troubleshooting

This chapter describes how to troubleshoot the Windows certificate store API.

This chapter contains the following sections:

8.1 Windows CryptoAPI Certificate Store Issues

If the Microsoft Windows CryptoAPI (CAPI) certificate store is mis-configured or is missing a certificate, use the following hints and initialization messages in the log file for troubleshooting:

```
Server should be SSL-aware but has no certificate from windows CAPI configured
[Hint: SSLCAPIEngine requires SSLCertificateCN]

Init: Check that your certificate template is correct and can support your
configured SSL protocol
Init: Private key not found
SSL Library Error: error:89067067:lib(137):CAPI_GET_KEY:cryptacquirecontext error
(Error code= 0x0)
SSL Library Error: error:26096080:engine routines:ENGINE_load_private_key:failed
loading private key
```

8.2 Service Account Not Installed

If the service account that is used to start Mobile Security Access Server or Mobile Security Administrative Console is not installed with IIS, proceed as follows:

1. Verify the certificate is in the service account's certificate store
2. Verify the certificate is in the computer certificate store and the service account has permission to access the private key.
   a. In some versions of Windows, admin privileges are required.
   b. Use the MMC console with certificate snap-in. Give permissions by right clicking and selecting **manage private key** to give permission to the service account.
3. Verify that the subject name of the certificate matches what was specified in the installation. In `httpd.conf`, check the following lines:

```
AuthBMAXSSLCertificateKeyFile nofips p11 capi MY "" <CERT_COMMON_NAME:> cn
```

```
SSLCertificateFile <CERT_COMMON_NAME:>
```

4. Verify that Microsoft Enhanced RSA and AES Cryptographic Provider is being used. This is required when certificates are stored in the Windows certificate store. Microsoft Web server templates can be modified to include the Microsoft Enhanced RSA and AES Cryptographic Provider.

If none of the above suggestions resolve the issue, un-comment the following line in the `httpd.conf` file and send the error logs generated as a result to Oracle support:

```
#SSLCAPIEngineLog "C:/Program Files (x86)\Oracle\OMSS/gateway/logs/openssl_
capi.log"
```

9 Mobile Device Troubleshooting Tips

This chapter describes how to troubleshoot mobile devices.

It contains the following sections:

- Section 9.1, "General Troubleshooting."
- Section 9.2, "SSL Troubleshooting."
- Section 9.3, "Turning on Client Debug Logs."
- Section 9.4, "Normal Sequence of Request for Registration and Authentication."

9.1 General Troubleshooting

The following are some general tips for troubleshooting mobile devices:

1. Ensure that the Mobile Security Access Server host name can be resolved by the mobile device.
2. Ensure that the PAC files are accessible from the URL location specified in the mobile configuration.
3. Ensure that the Mobile Security Access Server host name as specified in the PAC files can be resolved by DNS.
4. Ensure that the Mobile Security Access Server name matches the PROXY statement in the PAC file on the OMSAS.
5. If the Mobile Security Administrative Console server is deployed behind the Mobile Security Access Server, ensure that there is a PROXY statement for the Mobile Security Administrative Console server in the PAC files.
6. If the mobile device is configured for WIFI, ensure that the proxy with the URL of the `bmax.pac` file is specified.
7. If the mobile device is configured for VPN, ensure that the proxy with the URL of `bmax.pac` file is specified on the VPN and is not needed in the WIFI configuration.
8. Ensure that the Mobile Security Access Server configuration files, named `bmax_config.json` or `bmconfig_*.json`, are correctly configured in the Mobile Security Container application settings.
9. If the Mobile Security Access Server is configured for PKINIT or KINIT authentication, ensure that the user account being used is not locked in Active Directory.
10. If the Mobile Security Access Server is configured for Oracle Access Manager authentication, ensure that the user account is not locked.

11. If the Mobile Security Access Server is configured for PKINIT authentication, ensure that client certificates have the correct attributes for mutual authentication and smart-card login.
12. If the Mobile Security Access Server is configured for PKINIT authentication, ensure that the CA certificate chain for the Mobile Security Access Server certificate is installed in the mobile device key chain (network profiles).

9.2 SSL Troubleshooting

See Section 5.1, "SSL Troubleshooting."

9.3 Turning on Client Debug Logs

Navigate to the Mobile Security Container application settings. Turn on Log Mode and set Log Level to Debug.

9.4 Normal Sequence of Request for Registration and Authentication

During the normal registration process for a Mobile Security Container, the following sequence of requests should appear in the `access.log` file of the Mobile Security Access Server:

1. A sequence of requests to an authentication URL, with the expected response of HTTP 407. The number of requests may be different depending on the authentication method being used. The UPN or user ID of the authenticating user should appear at the beginning of the line associated with the authentication request. These requests occur every authentication.
2. A final request to an authentication URL, with the expected response of HTTP 200 or HTTP 302. A response of HTTP 200 means that the authentication was initiated directly within the Mobile Security Container, while a response of HTTP 302 means that the authentication was initiated by a redirect from an external application such as the Safari web browser or a containerized app. If an HTTP 403 is returned in response to any authentication request, it means that the authentication failed. This request occurs every authentication.
3. A request to `/action`. This request sets up the container for offline authentication and PIN/Password reset. This request only occurs during registration and PIN/Password resets.
4. A request to `/ecp/ecpservice/registercontainer.` This request registers the container with the Mobile Security Administrative Console server. The expected response is HTTP 200. This request only occurs during registration.
5. A request to `/ecp/ecpservice/policy/get`. This is a request to retrieve the policies associated with the container. The expected response is HTTP 200. This request occurs every authentication.
6. A request to `/ecp/ecpservice/settings/get`. This is a request to retrieve the company settings. The expected response is HTTP 200. This request occurs every authentication.
7. A request to `/ecp/ecpservice/getcommands`. This is a request to retrieve pending commands for the container. The expected response is HTTP 200. This request occurs periodically after registration.

Depending on the deployment configuration, there will also be a number of requests to the `bmax.pac` file and stunnel.pac. If there are no requests to the `stunnel.pac` or `bmax.pac` it likely means that the Mobile Security Access Server is not accessible from the mobile device.

10
Mobile Security Administrative Console IIS Configuration

This chapter describes errors related to, and configuration of, the Mobile Security Administrative Console with Windows Internet Information Services (IIS).

This chapter contains the following sections:

- Section 10.1, "Troubleshooting Errors Related to IIS Configuration"
- Section 10.2, "Configuring Mobile Security Administrative Console with IIS"

10.1 Troubleshooting Errors Related to IIS Configuration

The following errors are related to IIS configuration:

10.1.1 Database Connection Error

When a database connection error occurs, the following steps might help to resolve it:

- Ensure the identity is able to log in to IIS and do a WinAuth to the SQL database.
- Reboot IIS

10.1.2 File Not Found When Accessing Mobile Security Administrative Console

If you get the error:

```
File not found http://acp1.bitzermobile.dev/acp/lauth
```

verify the following:

- The IIS URL Rewrite mobile is present
- IIS is configured for PHP requests using FastCGI and not CGI
- PHP MIME Type
- PHP Default page
- Application Pool was created assigning the Mobile Security Administrative Console service account as the identity
- The Mobile Security Administrative Console service account has access to the database and has sufficient rights on the machine.
- The web site was created if the default web site was not chosen

- Mobile Security Administrative Console virtual directory was created and has Mobile Security Administrative Console application pool assigned to the Mobile Security Administrative Console virtual site
- Mobile Security Administrative Console Web service virtual directory was created and has Mobile Security Administrative Console application pool assigned to the Mobile Security Administrative Console virtual site
- If a new web site was created then all authentication methods can be disabled
- Mobile Security Administrative Console virtual directory enable only Windows Authentication and disable other authentication methods
- Mobile Security Administrative Console Web service virtual directory enable only Anonymous Authentication and disable other authentication methods
- Port 443 is configured and a web server certificate is installed at the IIS web site level
- The Application virtual directory test passes. It fails unless Basic Settings are set to the app pool id

10.2 Configuring Mobile Security Administrative Console with IIS

As an alternative to having the Oracle Mobile Security Suite installer automatically configure IIS, you can perform that configuration manually.

Use Server Manager to add the Web Server role.

Configure IIS with the following settings:

1. Enable CGI.
2. Enable Windows Authentication.
3. Configure IIS to handle PHP requests using FastCGI.
4. Add PHP MIME Type.
5. Add PHP as Default Document.
6. Add an application pool for the Mobile Security Administrative Console.
7. Create Web Site and Virtual Directories for the Mobile Security Administrative Console and Mobile Security Administrative Console Web services.
8. Enable Windows Authentication and disable Anonymous Authentication.
9. Configure for SSL
10. Install Microsoft Rewrite Module.

Use your Web browser to start Web Service.

11

Mobile Security Notification Server

This chapter describes troubleshooting tips for the Mobile Security Notification Server.

If notifications are not being sent to clients, verify the following:

- The Exchange configuration matches the version of Exchange.
- The permission of the proxy account to act on behalf of users is configured in exchange. This permission is different for Exchange 2007 than for Exchange 2010.

Details for the two versions are described in the following sections:

- Section 11.1, "Exchange Impersonation on Exchange 2007"
- Section 11.2, "Exchange Impersonation on Exchange 2010"

11.1 Exchange Impersonation on Exchange 2007

Exchange 2007 requires two rights to be able to get Exchange Impersonation working:

- `*ms-Exch-EPI-Impersonation`: This right is applied to the Client Access Server and grants the Service Account permission to function as an Exchange Impersonation account on that CAS.
- `oms-Exch-EPI-May-Impersonate`: This right is applied on either a user-by-user basis for each of the users that require impersonation to be enabled, or it can be applied on a mailbox database.

For example, Joe Client is a user with a device, and EWS Proxy is the account used to impersonate the user for notification. To add these rights:

```
Add-ADPermission
   -Identity (Get-ExchangeServer
   -IdentityYOUR_   CAS).DistinguishedName
   -User (Get-User -Identity "EWS Proxy").Identity
   -extendedRight ms-Exch-EPI-Impersonation

Add-ADPermission
   -Identity (Get-User -Identity "Joe Client").DistinguishedName
   -User (Get-User -Identity "EWS Proxy").Identity
   -extendedRight ms-Exch-EPI-May-Impersonate
```

11.2 Exchange Impersonation on Exchange 2010

Exchange 2010 requires the rights to be able to get Exchange Impersonation working:

- The AD users are placed in a group (for example; Notification Users), and the service account has the Management scope of the AD group that exchange is recognized. For example:

  ```
   New-ManagementScope -Name:"ExchImpersonationScope" -RecipientRestrictionFilter
  {memberofgroup -eq "CN=BNS Users,OU=QA,DC=bitzermobile,DC=com"}
  ```

- Define Assign Role:

  ```
  New-ManagementRoleAssignment -Name:"ExchImpersonationRole"
  -Role:ApplicationImpersonation -User:"ewsproxy@example.com"
  -CustomRecipientWriteScope:"ExchImpersonationScope
  ```

- If you receive this message:

  ```
  microsoft.exchange.webservices.data.ServiceVersionException: Method
  SubscribeToPushNotificationsOnAllFolders is only valid for Exchange Server
  version Exchange2010 or later
  ```

  This means that an incorrect exchange version was selected when installing Mobile Security Notification Server.

- If there are no errors it may be caused by Apple Push Notification server, as it does not guarantee for delivery. Verify your Apple credentials provided are valid.

12

Troubleshooting Mobile Security Administrative Console LDAP Sync

This chapter describes troubleshooting tips for LDAP (Oracle Unified Directory and Active Directory) sync with the Mobile Security Administrative Console.

This chapter contains the following topics:

12.1 AD Sync Job Error

When you click **Sync** on the Mobile Security Administrative Console **Settings->LDAP Settings** tab, you see this message:

```
Error while executing LDAP sync Job! Please check the server".
```

This can happen when the scheduled AD sync task is disabled or deleted on the Mobile Security Administrative Console Server. Proceed as follows:

1. Go to the Mobile Security Administrative Console server and open **Task Scheduler**. Check whether the **ldap_sync** task scheduler is disabled under the Task scheduler Library listing.
2. If disabled enable it back.
3. Try to sync again.

12.2 Job is Already Running

When you click a **Sync** button on the Mobile Security Administrative Console **Settings->LDAP Settings** tab you see the message:

```
LDAP sync Job is already running.
```

This message indicates that the LDAP sync task is already running or the LDAP sync scheduled task is stopped during execution. Proceed as follows:

1. Try to sync again after a few minutes.
2. If the error message still appears, go to the Mobile Security Administrative Console server and delete the file:

   ```
   install-dir\OMSS\ACP\config\*_sync_cron_running.log
   ```

3. Try to sync again.

12.3 Group Not Showing

If the LDAP User/Group is not showing on Mobile Security Administrative Console, proceed as follows:

1. Make sure the user/group is member of control group or role mapping groups.
2. Trigger a full sync by clicking **Full Sync** on Mobile Security Administrative Console **Console Settings->LDAP Settings** tab.

12.4 Deleted or Disabled Users Still Appearing

If deleted/Disabled users are still showing up on Mobile Security Administrative Console, trigger a full sync by clicking **Sync Now**

12.5 User Role Mapped to End User

User role is mapped to end user role. Proceed as follows:

1. Make sure user is part of respective role mapping group.
2. Trigger full sync by clicking **Full Sync** on the Mobile Security Administrative Console **Console Settings->LDAP settings** tab.

12.6 Cannot Log In to Console

If you cannot log in to the Mobile Security Administrative Console:

1. Make sure LDAP sync schedule task is complete. You can check the status of the sync in one of these log files:

   ```
   install-dir\OMSS\ACP\logs\ldap-sync\ldap_sync_job_scheduler.log
   ```

   or

   ```
   install-dir\OMSS\ACP\logs\ad-sync\ad_sync_job_scheduler.log
   ```

2. If another admin user is allowed to log in, check for the failed user on Mobile Security Administrative Console console.
3. If the user does not show up on Mobile Security Administrative Console console, trigger a sync by clicking **Full Sync** on the Mobile Security Administrative Console's **Settings->LDAP settings** tab.

12.7 Invalid Username

If you cannot register a Mobile Security Container and get the error:

```
Invalid username
```

Make sure the user is appearing on Mobile Security Administrative Console console and is part of the control group.

13

Mobile Security Administrative Console Database Replication

This chapters describes troubleshooting tips for Mobile Security Administrative Console (OMSAC) Database Replication.

Containerized apps must be loaded onto each OMSAC. If the App's icon is missing from the replicated (Subscriber) Mobile Security Administrative Console server, but it appears on the server where it was uploaded, proceed as follows:

1. In the replicated environment, upload the app binary on all the Mobile Security Administrative Console servers.
2. After uploading the app binary on one server, the DB entry replicates on all servers.
3. Log in to the other Mobile Security Administrative Console server's console and re-upload the binary for each of the corresponding uploaded app entry.