Oracle® Fusion Middleware

Installation Guide for Oracle Mobile Security Suite

Release 3.0.1

E51930-03

March 2014

This book describes how to install Oracle Mobile Security Suite.

ORACLE

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

E51930-03

Primary Author: Ellen Desmond

Contributing Author: Vinaye Misra

Contributor: John Boyer

Contents

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 Identity and Access Management administrators who install the 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 Release Notes*
- *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

This guide describes how to install Oracle Mobile Security Suite.

Oracle Mobile Security Suite enhances employee productivity by allowing secure access to corporate applications and data from mobile devices while preserving a rich user experience. The Mobile Security Container creates an enterprise workspace on any mobile device, corporate owned or personal, and for all mobile platforms. Employees get seamless access to intranet resources, corporate data and mobile apps with enterprise-grade security and deep integration with Oracle Access Manager and Microsoft Active Directory authentication for true Single Sign-On.

2

Installation Requirements

This chapter describes the requirements for installing Oracle Mobile Security Suite.

It contains the following sections:

2.1 Server Requirements

The minimum server requirements for installing any of the Oracle Mobile Security Suite servers are as follows:

- Windows 2008 R2 or Oracle Linux 6 Update 1+
- Latest service pack and security updates
- 4 GB memory
- 2.2 GHZ processor with 4 cores
- 30GB hard drive

2.2 Deployment Configurations

The Oracle Mobile Security Suite installer can be used to install the Mobile Security Access Server (formerly BMAX), Mobile Security Administrative Console (formerly ACP), Mobile Security File Manager (formally m/Drive), and Mobile Security Notification Server (formerly BNS). Depending on the intended use, the components can be installed on the same or different physical server (or virtual server) machines. The following table summarizes five common deployment configurations.

Option	Machine 1	Machine 2	Machine 3	Machine 4	Comments
1	Access Server Administrative Console File Manager Notification Server Database				Lab Administrative Console not on IIS

Option	Machine 1	Machine 2	Machine 3	Machine 4	Comments
2	Access Server	Administrative Console File Manager Notification Server Database			Lab or Production
3	Access Server	Administrative Console File Manager Notification Server	Database		Lab or Production
4	Access Server	Administrative Console	Database	File Manager Notification Server	Lab or Production
5	Access Server	Administrative Console Notification Server	Database	File Manager	Lab or Production

2.3 Installation Program Requirements

This section contains the following topics:

2.3.1 LDAP, Database, and Authentication Server Requirements

When connecting the Oracle Mobile Security Suite to external LDAP, Database and Authentication servers the following prerequisites are required:

- If you are using Oracle Access Manager for authentication, you must have least at Oracle Access Manager (OAM) with Mobile and Social (OAMMS) version 11g R2 PS2 with Patch 18325631.
- If you are using Microsoft Active Directory for authentication, you must have at least version Windows 2008 domain controllers and a domain functional level of at least Windows 2003.
- If you are using Oracle Unified Directory for LDAP user and group synchronization, you must have at least version 11g R2 PS2 with patch 18165497.
- If you are using Microsoft Active Directory for LDAP user and group synchronization, you must have at least version Windows 2003.
- If you are using Oracle Database as a repository then you must have at least version 11g R2.

- If you are using Microsoft SQL Server as a repository then you must have at least version 2008.

  Note: Microsoft SQL Server support has been deprecated and might not be supported in future releases. It is not recommended for new installs.

- If you are using Oracle Web Services Manager to protect web services with OAuth, you must have at least version 11gR1 PS6 with Patch 17278807.

2.3.2 Mobile Security Access Server Requirements

The following prerequisites are required to install the Mobile Security Access Server:

- Internet Information Services must NOT be installed
- Ports 80 and 443 must be available for the Mobile Security Access Server application on the server.
- Ports 80 and 443 must be open for incoming HTTP traffic on the firewall. These ports must be accessible from mobile devices.
- Port 53 must be open between the Mobile Security Access Server and the Domain Name System (DNS) server(s).
- Port 123 must be open between the Mobile Security Access Server and the Network Time Protocol (NTP) server.
- Port 88 must be open between the Mobile Security Access Server and Active Directory for Kerberos authentication and negotiation.
- Ports 80 and/or 443 must be open between the Mobile Security Access Server and Oracle Access Manager for OAM authentication and OAuth/OAM token management.
- SharePoint and other web applications that will be accessed must be accessible from the Mobile Security Access Server, for example: port 80 for HTTP and port 443 for HTTPS.
- Certificate for Mobile Security Access Server

  If you are using a Microsoft Certificate Authority, the Microsoft Enhanced RSA and AES Cryptographic Provider is required when certificates are stored in the Windows certificate store (CAPI). Microsoft web server templates can be modified to include the Microsoft Enhanced RSA and AES Cryptographic Provider.

  When using non-Microsoft Certificate Authorities, make sure that the Mobile Security Access Server certificate has the right to log in to Windows on the Mobile Security Access Server system. The size of the key should be no less than 1024 bits, and 2048 bits is recommended. If the certificate is stored using Windows CAPI (Windows certificate store) then refer to the Microsoft Enhanced RSA and AES Cryptographic Provider template for attributes to be configured for the non-Microsoft certificate request.

  Certificates / keys can be stored in CAPI with a non-exportable key. Otherwise certificates / keys can be stored in PEM format on the file system.

- If you are installing the Mobile Security Access Server on Windows with CAPI, Windows credentials are required to access the Microsoft cryptographic store. The account (service account) will require:

- Windows Active Directory account with rights to login to the Mobile Security Access Server machine.
- The right to start the Mobile Security Access Server Windows service.

2.3.3 Mobile Security Administrative Console Requirements

The following prerequisites are required to install the Mobile Security Administrative Console server:

Note: A logo in `jpeg`, `png`, or `bmp` format is optional.

- If you are installing the Mobile Security Administrative Console using Oracle Database, you must use an account with the necessary permissions to read and write the selected schemas.
- If you are installing the Mobile Security Administrative Console using Microsoft SQL Server using Windows authentication for a SQL account, the Windows SQL account must be created prior to running setup. The account (service account) will require the following:
  - Ports 389 and/or 636 must be open between the Mobile Security Administrative Console and Oracle Unified Directory for LDAP synchronization.
  - Ports 389, 636, 3268, and/or 3269 must be open between the Mobile Security Administrative Console and Active Directory for LDAP synchronization. For more information, refer to `http://support.microsoft.com`.
  - Windows Active Directory account with rights to login to the Mobile Security Administrative Console machine.
  - Defining the windows account to the desired SQL instance as a SQL account.
  - The right to start the Mobile Security Administrative Console windows service. The easiest way to accomplish this is by giving that account the same rights as `Local System`, or adding the account to the local Administrators group.
  - Port 1443 or custom port defined for Microsoft SQL Server
- If you are installing the Mobile Security Administrative Console with Active Directory group synchronization, Windows credentials are required to authenticate to Active Directory. The credentials only require read access to Active Directory. If using Windows authentication for Microsoft SQL Server, then those credentials can be used as previously entered.
- If you are installing the Mobile Security Administrative Console with Oracle Unified Directory group synchronization, LDAP credentials are required to authenticate to Oracle Unified Directory. The credentials only require read access to Oracle Unified Directory.
- If you are installing Mobile Security Administrative Console on Internet Information Services:
  - Mobile Security Administrative Console must be installed on a separate server than the Mobile Security Access Server Gateway server.
  - Internet Information Services must be installed and configured before the Mobile Security Administrative Console installation.

        * Internet Information Services 7.5 and above
        * Add the `webserver` role using Windows server manager with the following features:

          Application Development: CGI

          Security: Basic Authentication and Windows Authentication

          Management Tools: Internet Information Services Management Scripts and Tools, IIS 6 Metabase Compatibility, IIS 6 WMI Compatibility, IIS 6 Scripting Tools
        * SSL certificate must be assigned after installation.
    - Certificate for Mobile Security Administrative Console server. The Administrative Console server certificate can be your standard SSL server certificate.

2.3.4 Mobile Security File Manager Requirements

The following prerequisites are required to install the Mobile Security File Manager server:

- The Oracle Mobile Security Suite is configured to use Windows Kerberos authentication.
- Existing file shares with network permissions for users.
- File servers can be either Windows or UNIX servers; there is no restriction if the servers allow Kerberos or NTLM authentication based on the Windows user account.
- Ports 8080 and 8443 must be available for the Mobile Security File Manager application on the server.
- Certificate for Mobile Security File Manager server if installed separately from Mobile Security Access Server and Mobile Security Administrative Console.

2.3.5 User Certificate Provisioning Requirements

The following prerequisites are required for user authentication certificate provisioning:

- The Mobile Security Administrative Console must be installed on Windows.
- Mobile Security Administrative Console must be installed with the Windows Active Directory Group Synchronization option selected.
- Kerberos PKINIT must be selected as a primary authentication method. Time Limited Password must be selected as the backup authentication method.
- Microsoft Certificate Authority
    - Configured to allow Subject Alternate Names (SAN) in certificate requests.
    - Configure a Certificate template for smart card login with the private key exportable (clone the smart card login template).
        * Update the template to make the private key exportable.
        * Update the template to allow the subject to be passed in the request.
    - The Active Directory account used to run the Mobile Security Administrative Console service must have the following permissions:

* Read and Enroll the certificate template used (assigned on the security properties or the certificate template)
* Manage certificates at the Certificate Authority level to revoke certificates (assigned on the security properties of the CA)

2.3.6 Mobile Security Notification Server Requirements

The following prerequisites are required to install the Mobile Security Notification Server:

- Ports 8080 and 8443 must be available for the Mobile Security Notification Server. The ports can be shared by Mobile Security File Manager and Notification Server when they are installed on the same server.
- Certificate for Mobile Security Notification Server, if installed separately from Mobile Security Access Server, Administrative Console, and File Manager.
- Exchange Server with EWS Service Enabled for Mobile Security Notification Server to communicate.
- Service Account in Exchange that has impersonation rights to access a group/user's mail boxes.
- Certificate from Apple to authenticate with Apple Push Notification Service (APNS). Refer to `http://developer.apple.com` to find out how to get the certificate.

3

Oracle Mobile Security Suite Installation Options

This chapter describes optional features that can be installed with Oracle Mobile Security Suite.

The following optional features can be installed with the Oracle Mobile Security Suite installer:

- Mobile Security Services: Required for Mobile Security Access Server and the Mobile Security Administrative Console
- Mobile Security Access Server Gateway
  - OAM Password, Kerberos PKINIT, or Kerberos Password or RADIUS One Time Passwords (OTP) for primary authentication
  - OAM Password, Kerberos Password, or Time Limited Password for backup authentication
- Mobile Security Administrative Console
  - Choice of using Oracle Database, Microsoft SQL Server, or embedded MySQL
  - Windows Authentication for Microsoft SQL Server
  - Oracle Unified Directory group synchronization with OUD groups.
  - Windows Active Directory group Synchronization with Mobile Security Administrative Console groups
  - User Authentication Certificate Provisioning using Microsoft Certificate Authority
  - Install on Internet Information Services when installed on a separate server than Mobile Security Access Server to provide Windows Authentication and Authorization to access Mobile Security Administrative Console
- Mobile Security File Manager
- Mobile Security Notification Server

> **Note:** Note that Microsoft SQL Server support has been deprecated and might not be supported in future releases. It is not recommended for new installs.

The installation setup program allows all options to be specified in a new installation as opposed to an upgrade installation from a previous release. In an upgrade, the text field for a value will be disabled (greyed out) if it cannot be changed during an

upgrade. Changing Database types is not supported for upgrades. Changing Mobile Security Administrative Console to use Internet Information Service as a web server is not supported for upgrades.

You must use the following upgrade order when upgrading an existing Oracle Mobile Security Suite deployment:

1. Upgrade the database (if manual database upgrade scripts are used).
2. Upgrade Mobile Security Administrative Console.
3. Upgrade Mobile Security Notification Server.
4. Upgrade Mobile Security File Manager.
5. Upgrade Mobile Security Access Server.
6. Upgrade Mobile Security Containers for iOS and Android.
7. Upgrade containerized apps for iOS and Android.

4

Installing Oracle Mobile Security Suite on Windows

This chapter describes how to install Oracle Mobile Security Suite on Windows.

It contains the following sections:

4.1 Welcome Screen

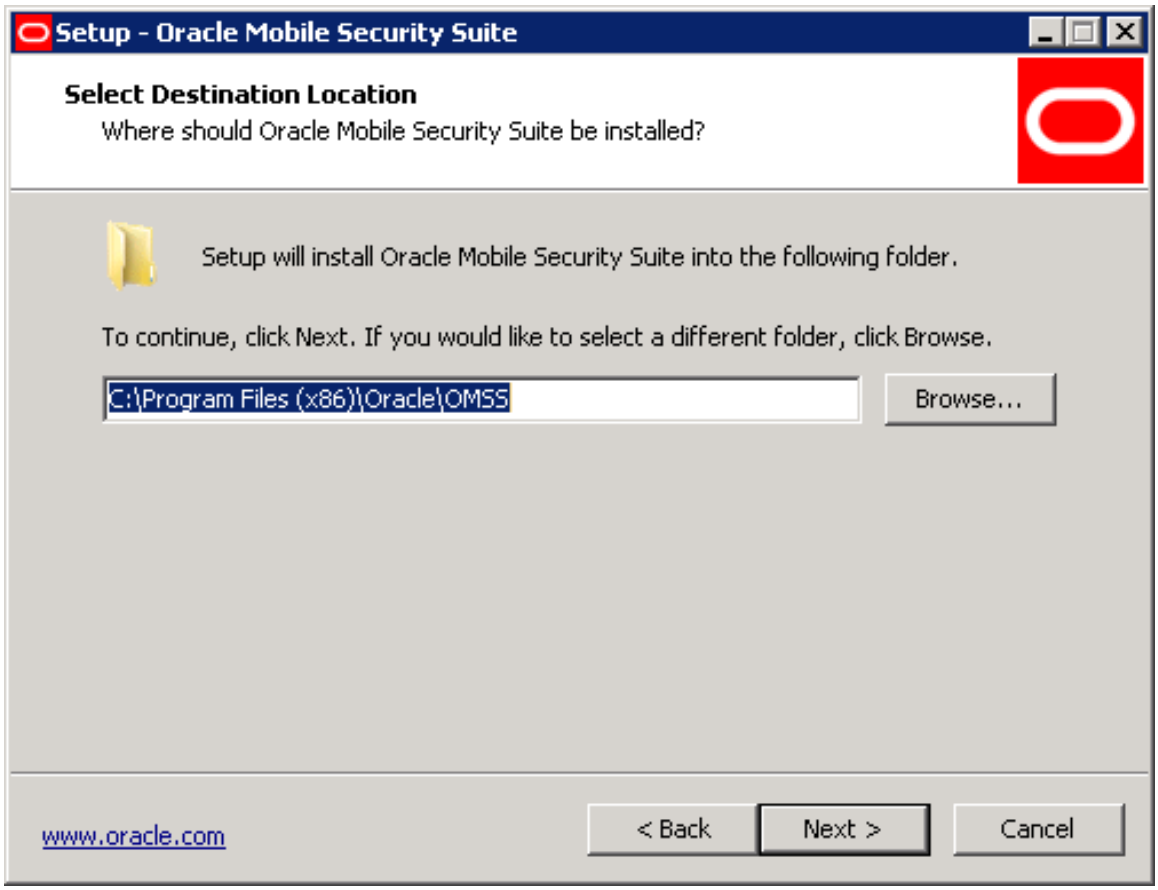
After you execute the Mobile Security Access Server setup program, the Welcome screen appears.

Click **Next**.

4.2 Select Destination Location Screen

Select the destination location where the Mobile Security Access Server will be installed by clicking **Browse** button and selecting the appropriate location.

Click **Next**.

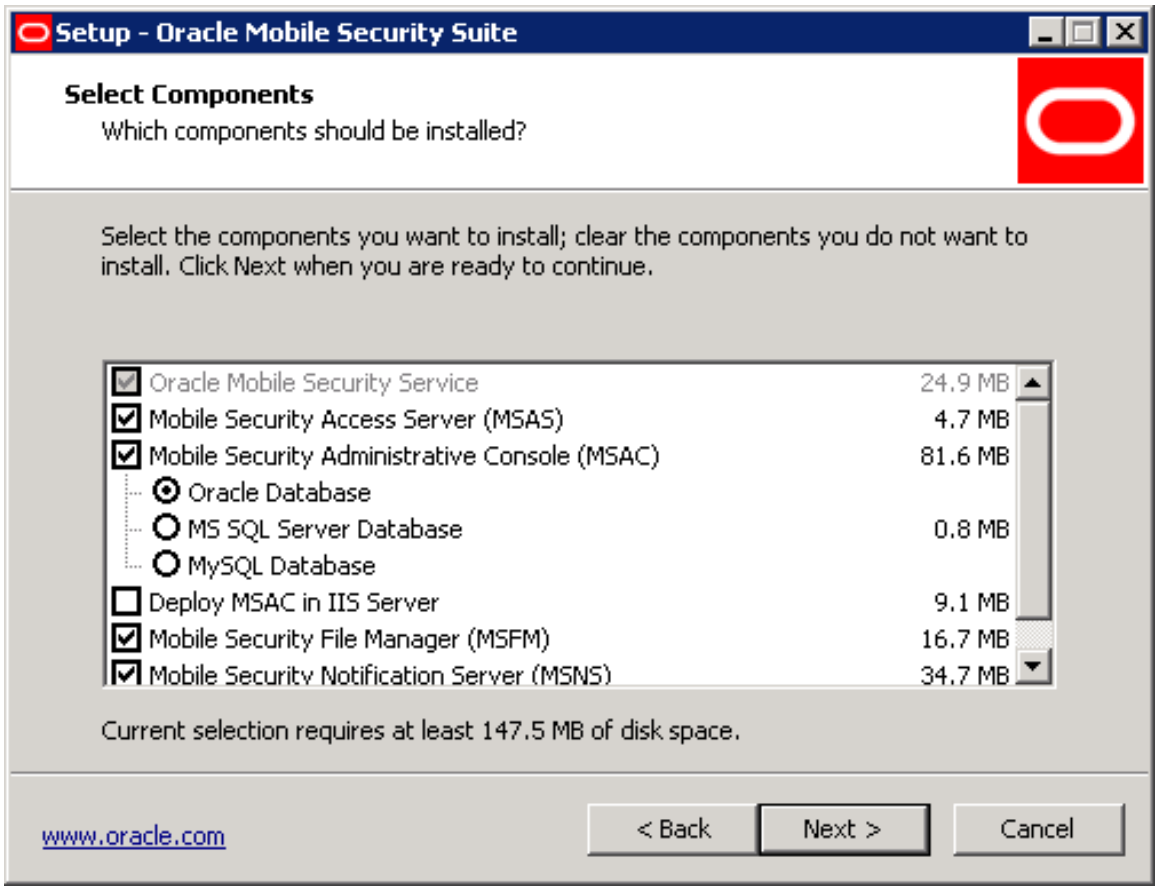


4.3 Select Components Screen

Select the components you want to install. Based upon the components selected, the installer will show further screens.

- Mobile Security Service is required for all of the components.
- Mobile Security Access Server should be installed on a server in the DMZ. It should not be installed for a standalone installation of Mobile Security Administrative Console on a separate server from the Mobile Security Access Server.
- Mobile Security Administrative Console can be installed on the same server as the Mobile Security Access Server, on a different server inside your network, or not at all (in this last case, client containers can point to the Mobile Security-hosted service). When installed on a different server than the Mobile Security Access Server it can optionally be installed using IIS.
- The database for Mobile Security Administrative Console can be either a remote Oracle Database or Microsoft SQL server instance, MYSQL, or Microsoft SQL Server on the same server as the Mobile Security Administrative Console for the embedded MySQL. The Mobile Security Access Server Setup Wizard installs the drivers to connect to Oracle Database or Microsoft SQL Server and creates Mobile Security Administrative Console information in the database but does not install the database server itself.
- Mobile Security File Manager can be installed on the same server as Mobile Security Administrative Console or on a different server inside your network.

- Mobile Security Notification Server can be installed on the same server as Mobile Security Administrative Console or on a different server inside your network.
- Mobile Security Administrative Console can use Oracle Unified Directory or Active Directory groups for access to the Mobile Security Administrative Console console using SSO when deploying Mobile Security Administrative Console.

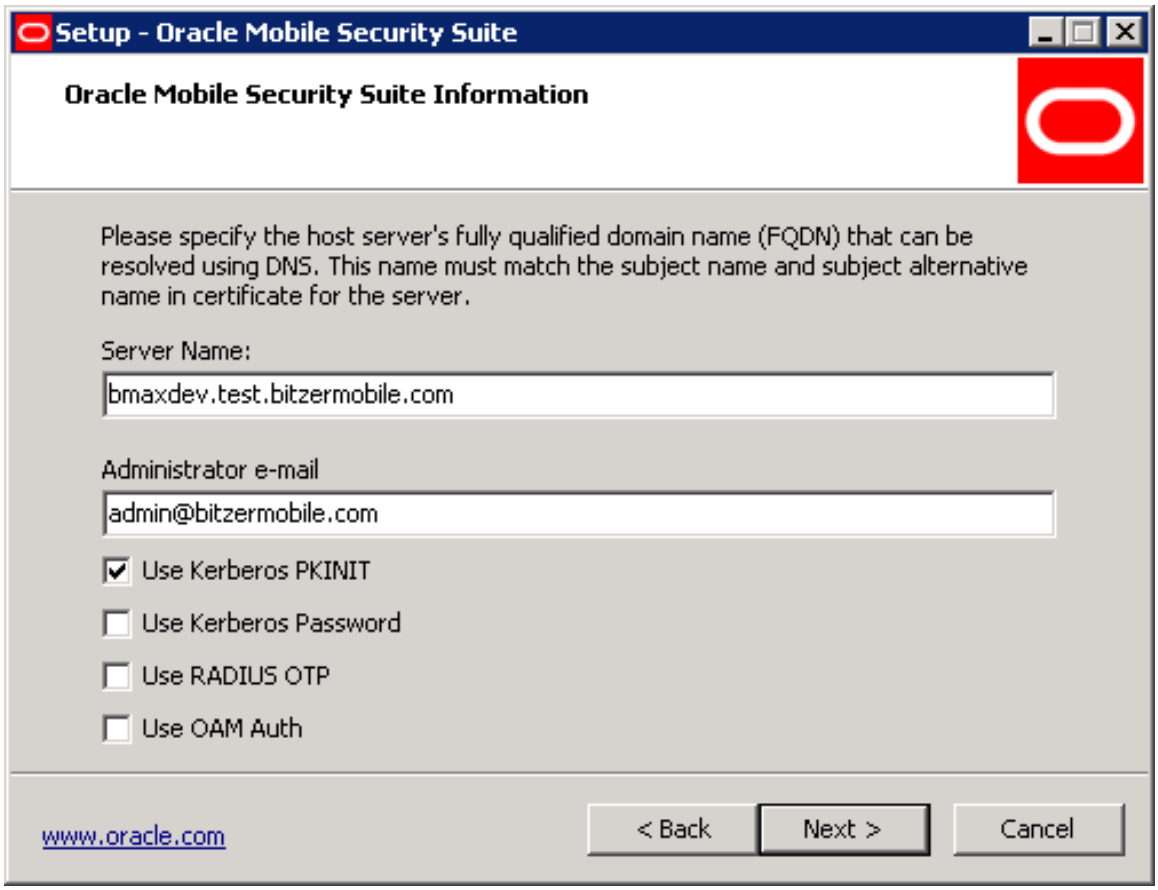


4.4 Mobile Security Access Server Information Screen

Enter the server name and administrator email address. By default, the installer fetches this information from the machine where it is running. If the machine is not part of an Active Directory domain, the domain information will not appear in the server name and email ID information. The server name must match the certificate subject name or subject alternative name present in the Mobile Security Access Server certificate. The server name need not be the host name of the Mobile Security Access Server, but it must be resolvable in DNS by the mobile clients.

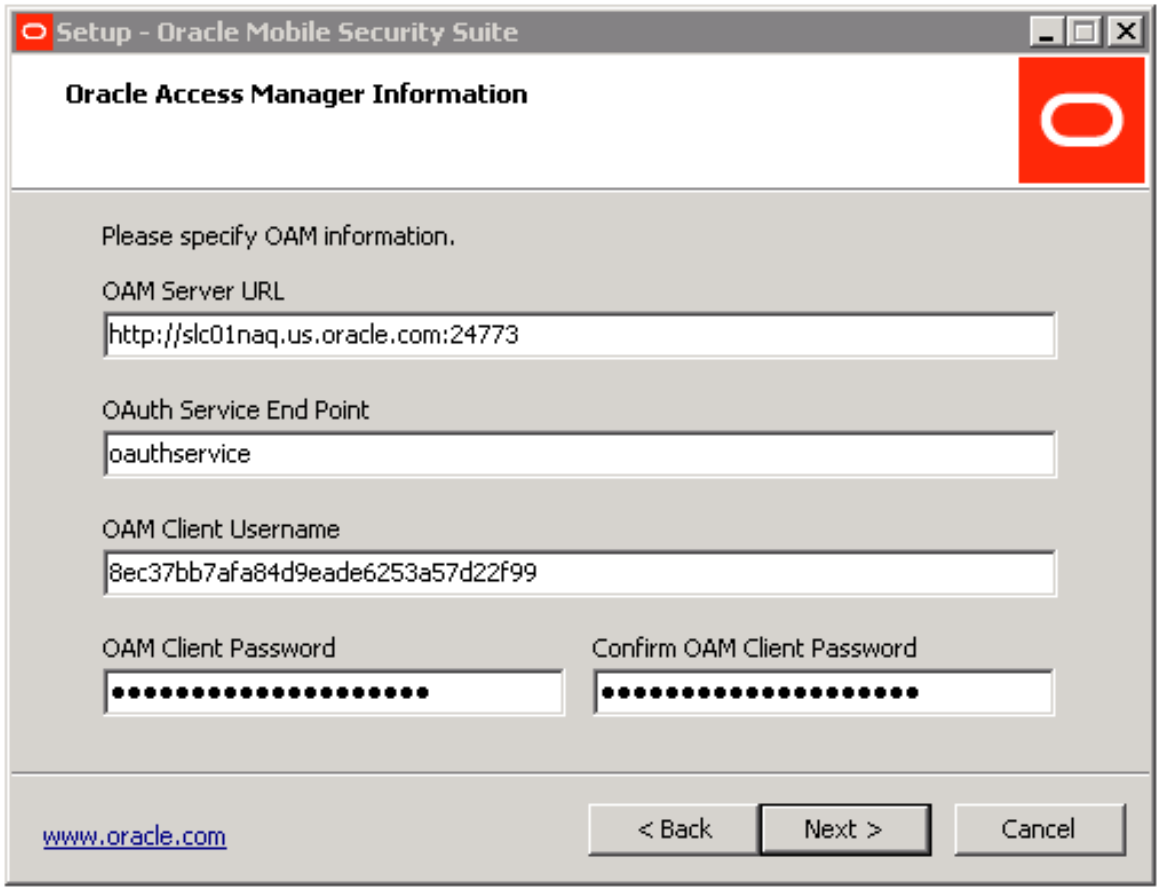
Select the authentication methods that the Mobile Security Access Server will support. Select **OAM Auth** if you are using an Oracle Access Manager user name and password. Select **Kerberos PKINIT** if you are using PKI certificates, **Kerberos Password** if you are using a Windows user name and password, and **RADIUS One Time Password** for OTP tokens as optional primary authentication methods. Each authentication option will generate a Mobile Security Container configuration file that the devices can use during the registration process to be configured for the corresponding authentication method.

Click **Next**.



4.5 Oracle Access Manager Authentication Information Screen

The following screen appears if the Mobile Security Access Server was selected with Oracle Access Manager authentication. Enter the Oracle Access Manager Server URL including scheme (http or https), OAuth Service End Point, and the Username and Password that was previously configured for the Mobile Security Access Server when it was registered as an OAuth Confidential Client with the Oracle Access Manager OAuth Service. Refer to Section A.1 for the associated Oracle Access Manager Configuration:



Click **Next**.

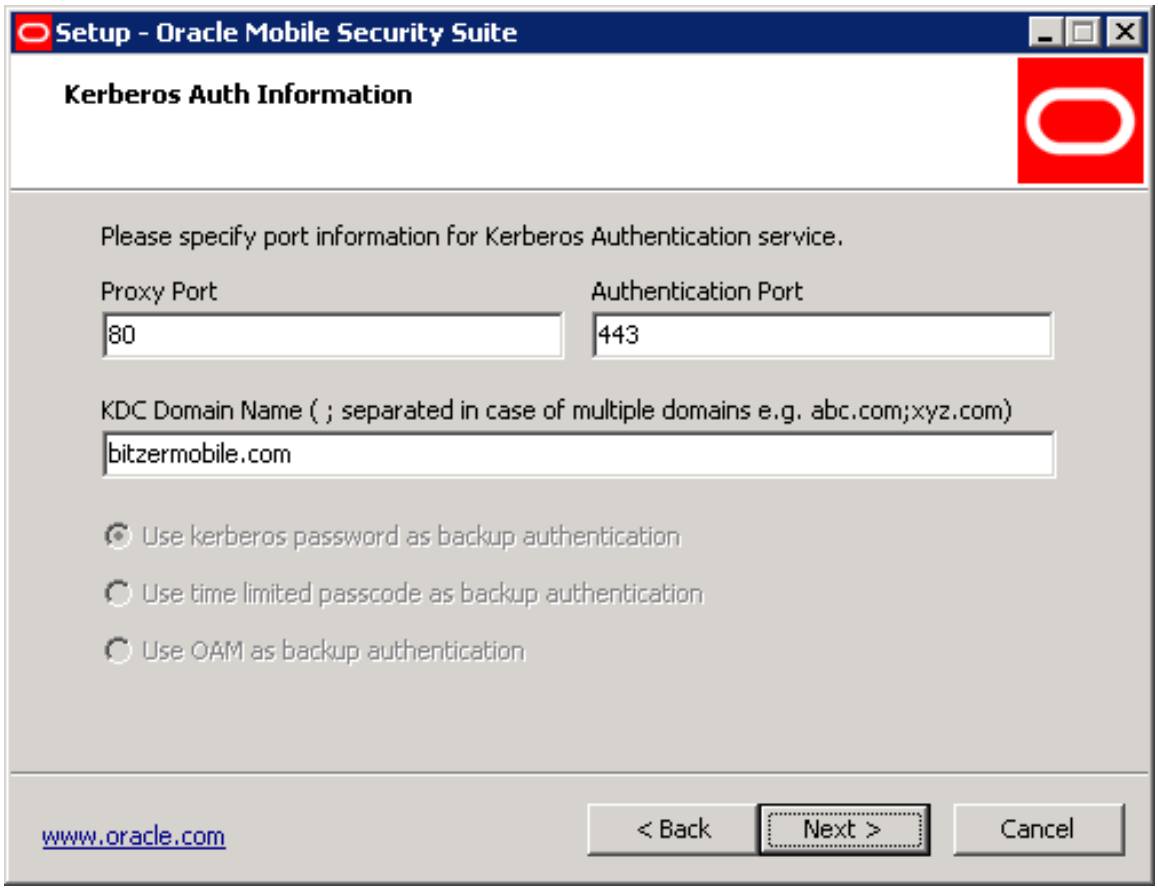
4.6 Kerberos Authentication Information Screen

Enter the **Proxy Port**, **Authentication Port**, and **KDC Domain Names** for user authentication. By default, the proxy port is 80 and the authentication port is 443. If the machine is not part of a domain, it will not show Active Directory domain information in the KDC Domain Name field. You must enter valid Active Directory domain names (Kerberos realms). Multiple domains can be added by separating them with semicolons. After the installation is completed, more domains can be added later to the *`installation_directory`*`/gateway/conf/krb5.conf` file manually.

If you have chosen Kerberos PKINIT as your primary authentication method with user certificate provisioning, then you must choose **Time Limited Passcode** for backup authentication. You can choose either backup authentication method if you have chosen Kerberos PKINIT as your primary authentication method and are using an alternate user certificate provisioning mechanism.

When you click on **Next**, the installer validates the provided information. The installer tests whether the proxy port and authentication port are free, as well as whether the domain name is valid and the Mobile Security Access Server can resolve the domain name in DNS. Click on Next to start the validation. The installer will notify you if an issue is found. Refer to the *Oracle Mobile Security Suite Troubleshooting Guide* if you need help resolving an issue.

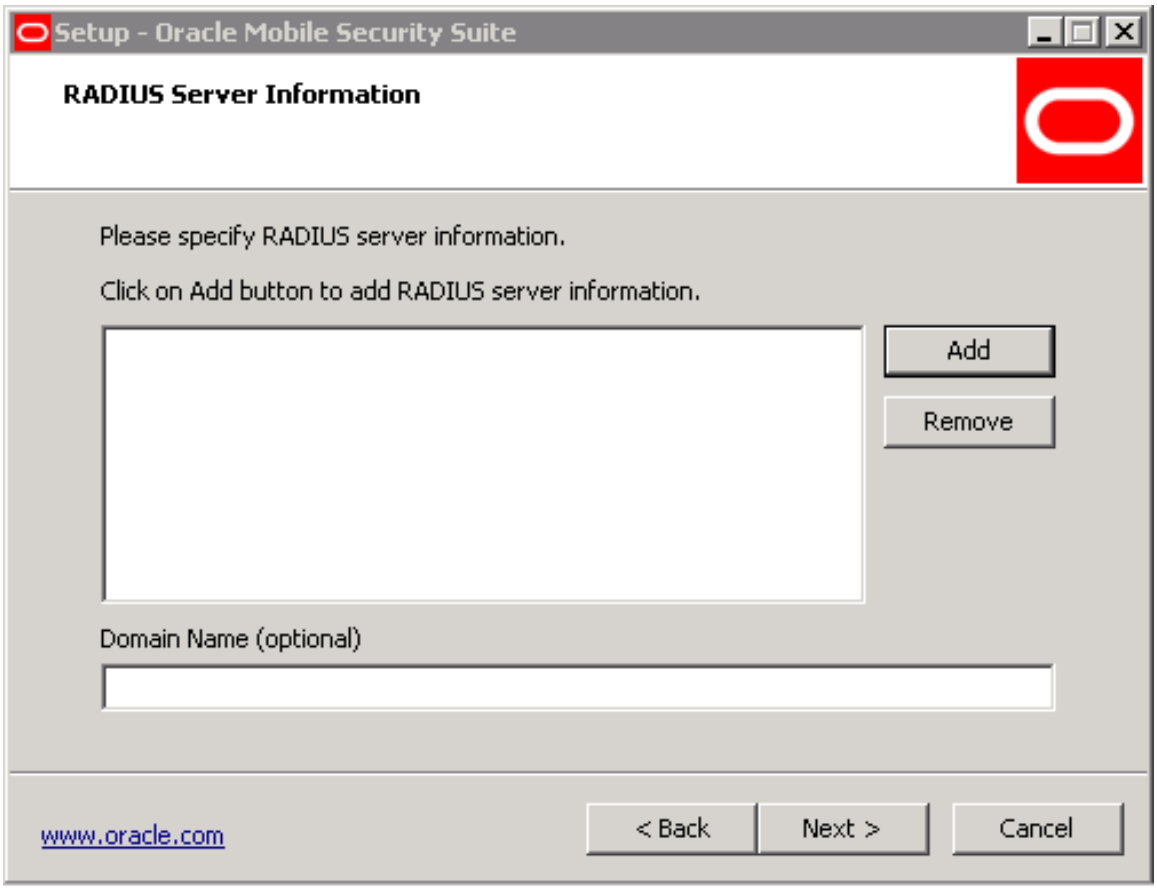
Click **Next**.

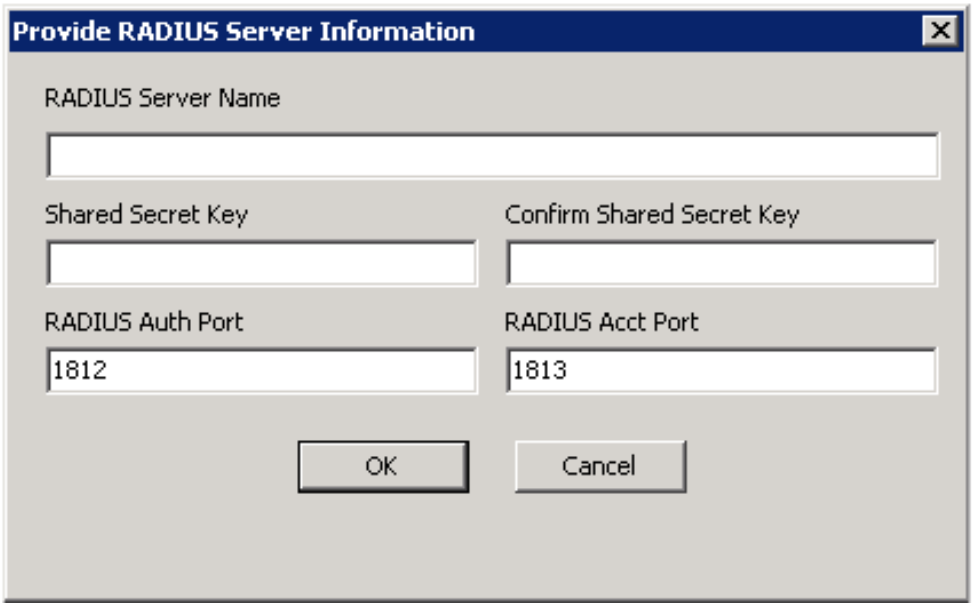


4.7 Radius Server Information Screen

If RADIUS OTP authentication is selected, the following screen will be shown. Mobile Security Access Server supports the standard RADIUS protocol as an addition to Kerberos passwords for two-factor authentication. Enter the **RADIUS Server Name**, optionally specify a default domain depending on the configuration of the RADIUS server, and select the appropriate **Shared Secret Key** for the RADIUS server.

Click **Next**.





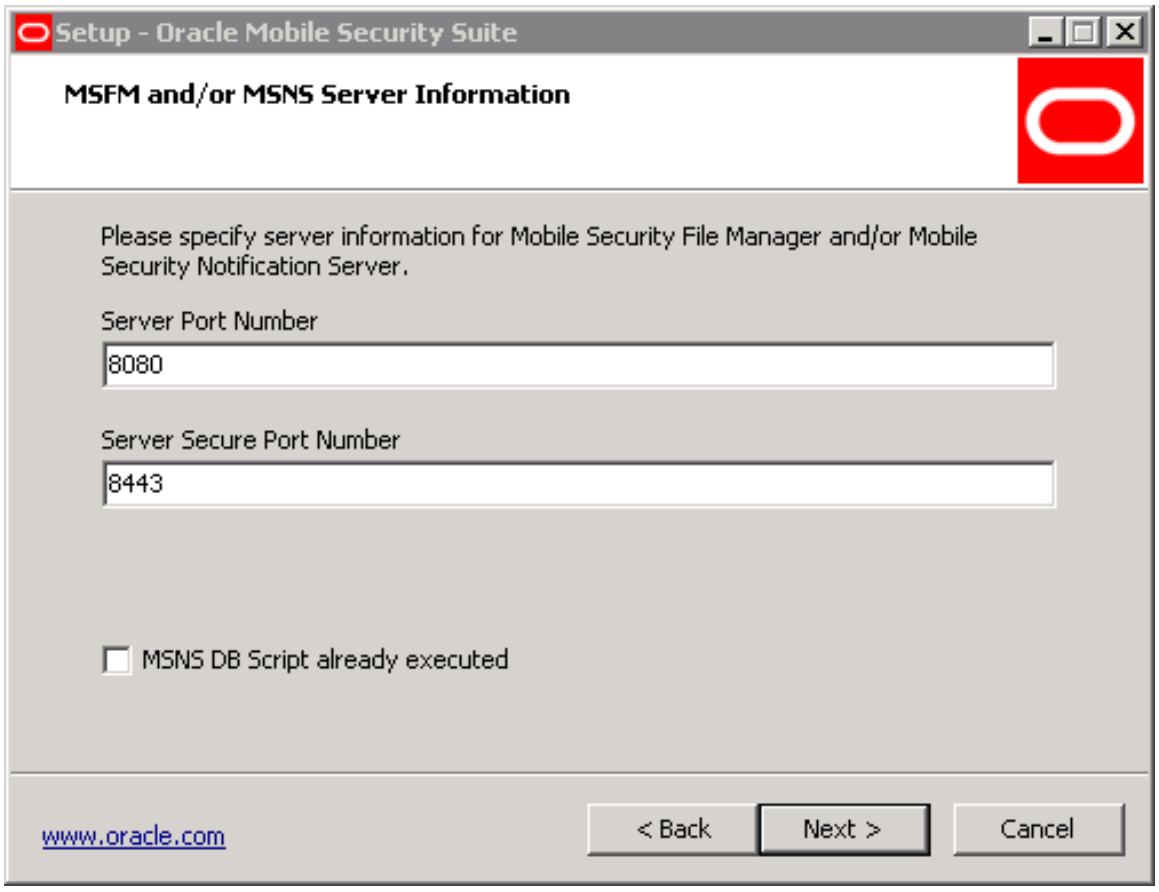
4.8 File Manager and Notification Server Information Screen

If File Manager or Notification Server is chosen then the following screen will be shown. Only the Ports are required to be configured at installation time for Mobile Security File Manager.

If Mobile Security Notification Server is chosen then the additional information shown below must be configured. If the database scripts were run prior to setup, select **MSNS DB Script already executed**.

Refer to the Mobile Security Administrative Console administration guide for configuration. The choice of database does not appear if installed on the same machine as Administrative Console, and the Administrative Console database selection is used instead.

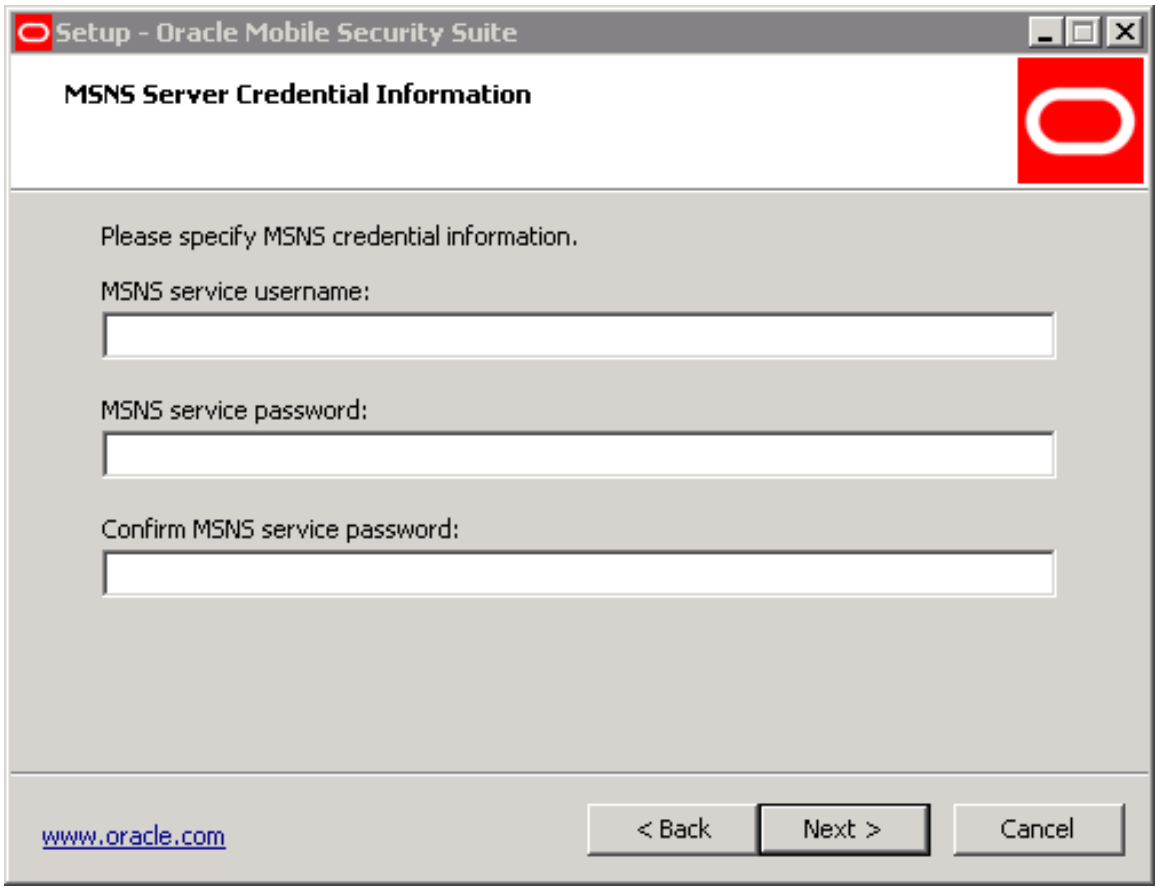
Click **Next**.



4.9 Notification Server Credential Information Screen

If Mobile Security Notification Server is chosen, then the following screen will be shown. Enter a service account that has the rights to run as a service.

Click **Next**.



4.10 Mobile Security Administrative Console Screen

If the Mobile Security Administrative Console component was selected, then the following screen will be shown.

Enter the **Company Name** and browse for a **Company Logo** image. By default, the screen will show Oracle as the company name. If you do not select a company logo image, then Mobile Security Administrative Console will show the Oracle logo in the Mobile Security Administrative Console.

Enter the Product Key that was provided by Oracle, based on your license agreement. In order to receive a Product Key, you must provide Oracle with the exact Company Name that you will use to install the Mobile Security Administrative Console. This Company Name must be entered exactly as it was communicated, including case and white space, for it to match the Product Key.

Select **Use LDAP Directory Group Sync** to map Mobile Security Administrative Console groups to Oracle Unified Directory or Microsoft Active Directory groups. Users or nested groups are supported. When this option is selected, only users with membership in a selected LDAP control group will be allowed to register their mobile device for use with the Mobile Security Suite solution. The frequency with which groups are synchronized can be modified after the installation using Microsoft Tasks Scheduler administration tool. If this option is selected then the Mobile Security Administrative Console LDAP Group Sync screen will be shown.

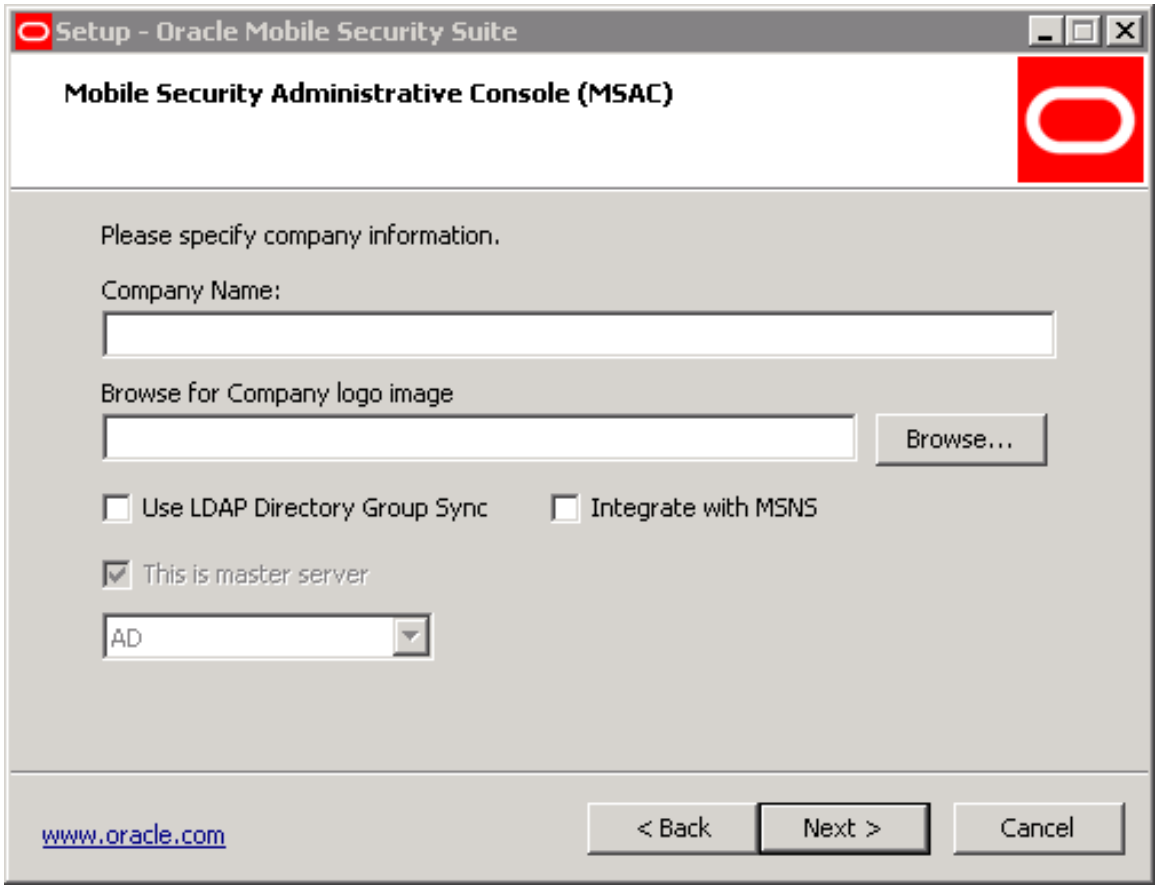
Select **DB Scripts Already Executed** if your database administrator has manually run the database creation or upgrade scripts prior to the installation. The installer will only

run scripts that populate the database with information from the options chosen during installation.

Select **Integrate with MSNS** if the Mobile Security Notification Server is being installed on a separate system.

Select **This is master server** if this is the first Mobile Security Administrative Console server in a replicated configuration of multiple instances of the Administrative Console database.

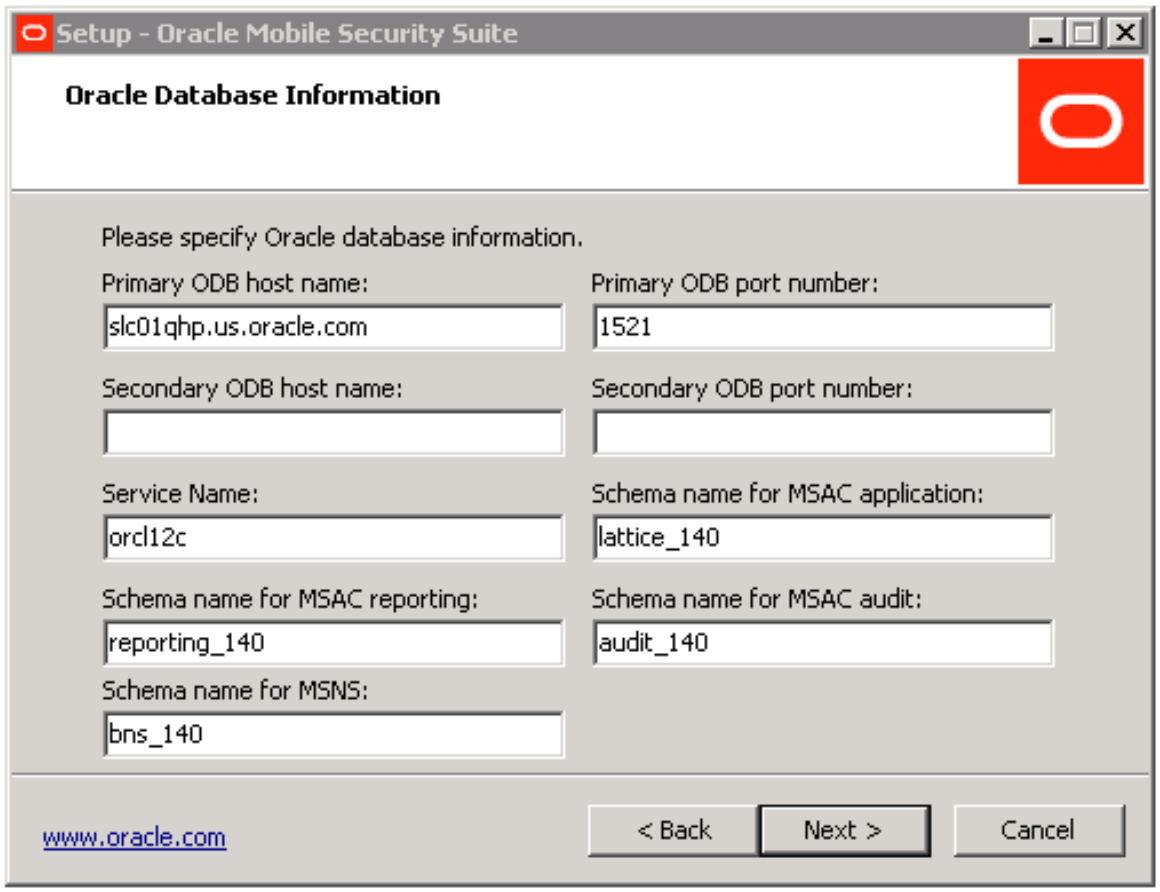
Click **Next**.

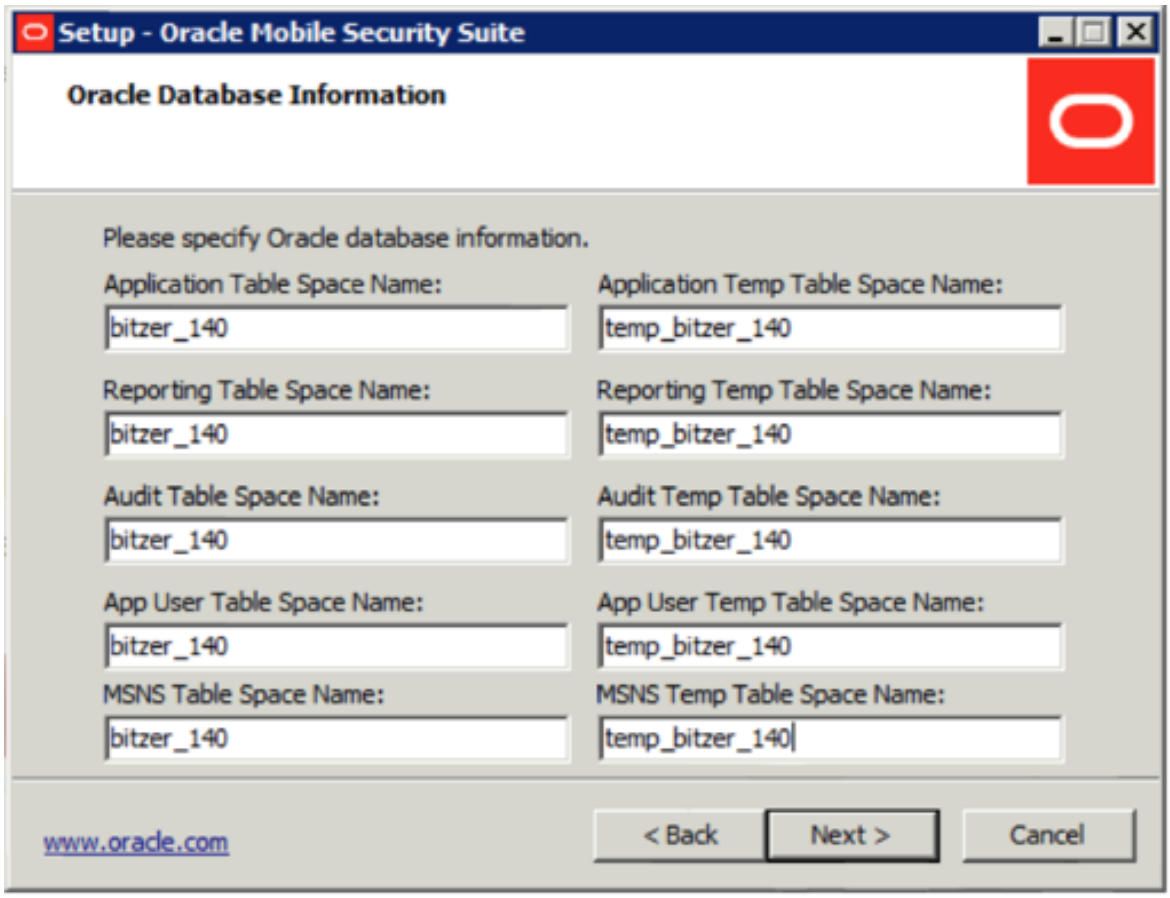


4.11 Oracle Database Screen

the following screen appears if the Mobile Security Administrative Console component was selected with the Oracle Database. Enter the primary, and optionally secondary, Oracle Database host name(s) and port number(s), as well as the chosen service name. The Oracle Database host should be remote from the Mobile Security Administrative Console component and have been previously installed at an accessible location. The selected Oracle Database service name must exist prior to Mobile Security Administrative Console installation.

There is no need to change the database schemas or table space names unless there is a specific business requirement or database naming standard. If the database scripts are modified and run prior to installation, then the corresponding fields should be changed in this dialog. A dialog message will appear if the names do not match what is entered in this dialog box or new schemas are created for the first time. Choose the type of DBA credentials to be used to create the databases.


Setup - Oracle Mobile Security Suite
Oracle Database Information
Please specify Oracle database information.
Primary ODB host name:
slc01qhp.us.oracle.com
Primary ODB port number:
1521
Secondary ODB host name:
Secondary ODB port number:
Service Name:
orcl12c
Schema name for MSAC application:
lattice_140
Schema name for MSAC reporting:
reporting_140
Schema name for MSAC audit:
audit_140
Schema name for MSNS:
bns_140
www.oracle.com
< Back
Next >
Cancel

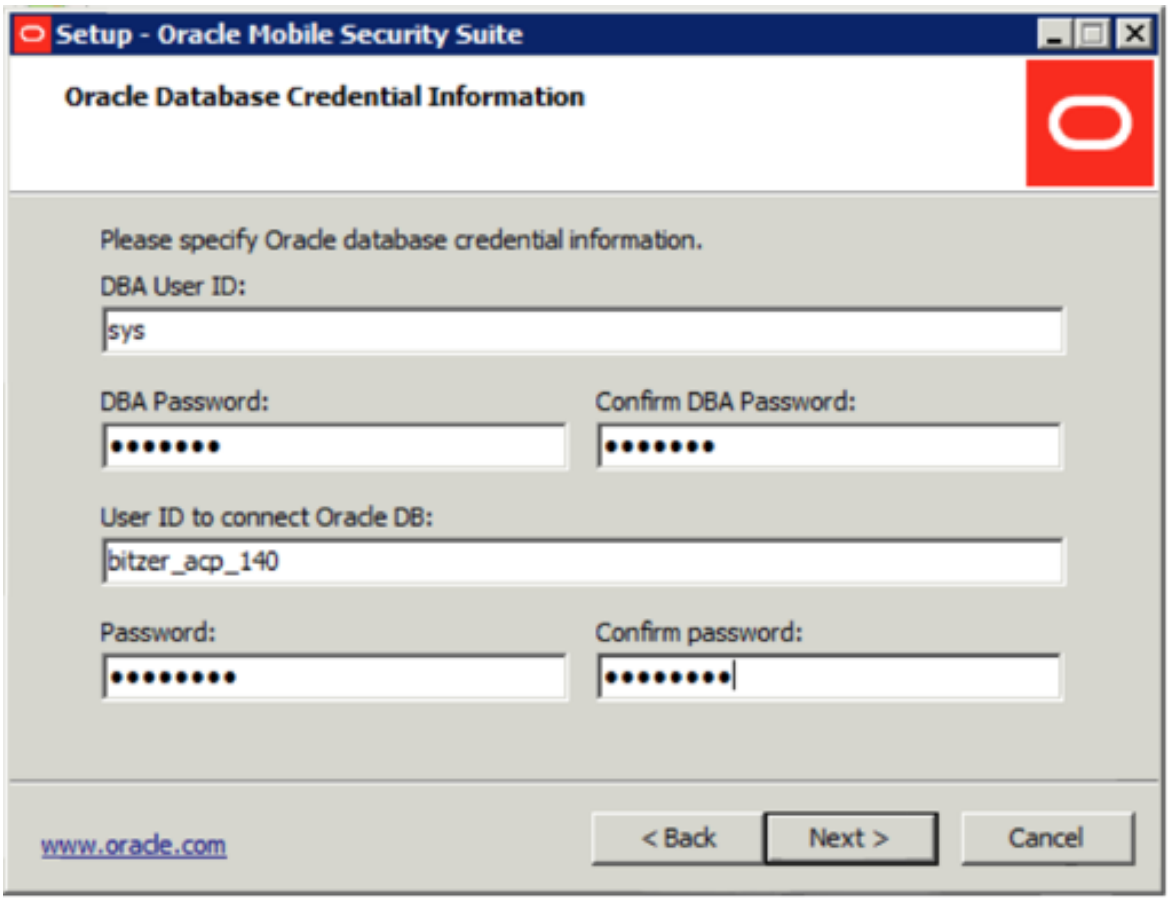


Click **Next**.

4.12 Oracle Database Credential Information Screen

This screen appears if the Mobile Security Administrative Console component was selected with the Oracle Database.

The DBA credentials are never stored on the file system and are only used to run database scripts and assign ownership to the service account specified in this screen. The Mobile Security Administrative Console uses the service account credentials to connect to the Oracle Database. The DBA and service accounts must be defined prior to running the Oracle Mobile Security Suite installer.



Click Next.

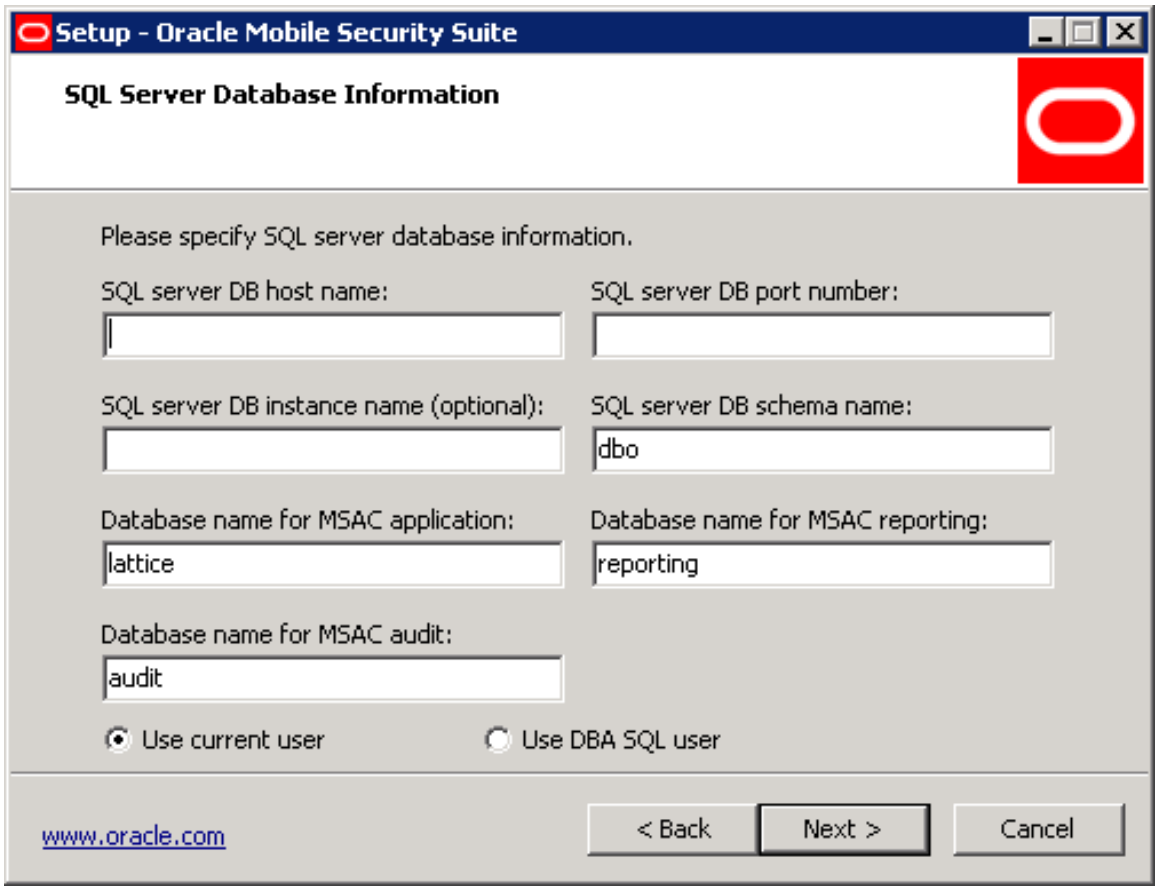
4.13 SQL Server Database Information Screen

Note: Microsoft SQL Server support has been deprecated and might not be supported in future releases. It is not recommended for new installs

If the Mobile Security Administrative Console component was selected with Microsoft SQL Server, then the following screen will be shown. Enter the **SQL Server DB host name** and **port number**. The SQL Server host can be either local or remote from the Mobile Security Administrative Console component as long as Microsoft SQL Server has been previously installed at an accessible location. However, it is best practice to have the database on a separate database server behind a firewall. The SQL Server instance will use the default instance if left blank; otherwise the specified SQL instance must exist prior to Mobile Security Administrative Console installation.

There is no need to change the database schema or database names unless there is a specific business requirement or database naming standard. If the database scripts are modified and run prior to installation, then the corresponding fields should be changed in this dialog. A dialog message will appear if the database name does match what is entered in this dialog box, or a new database is created for the first time. Choose the type of DBA credentials to be used to create the databases.

Click **Next**.



If Mobile Security Notification Server is chosen then the Database Information screen will have an additional field to specify a name for the Mobile Security Notification Server database.

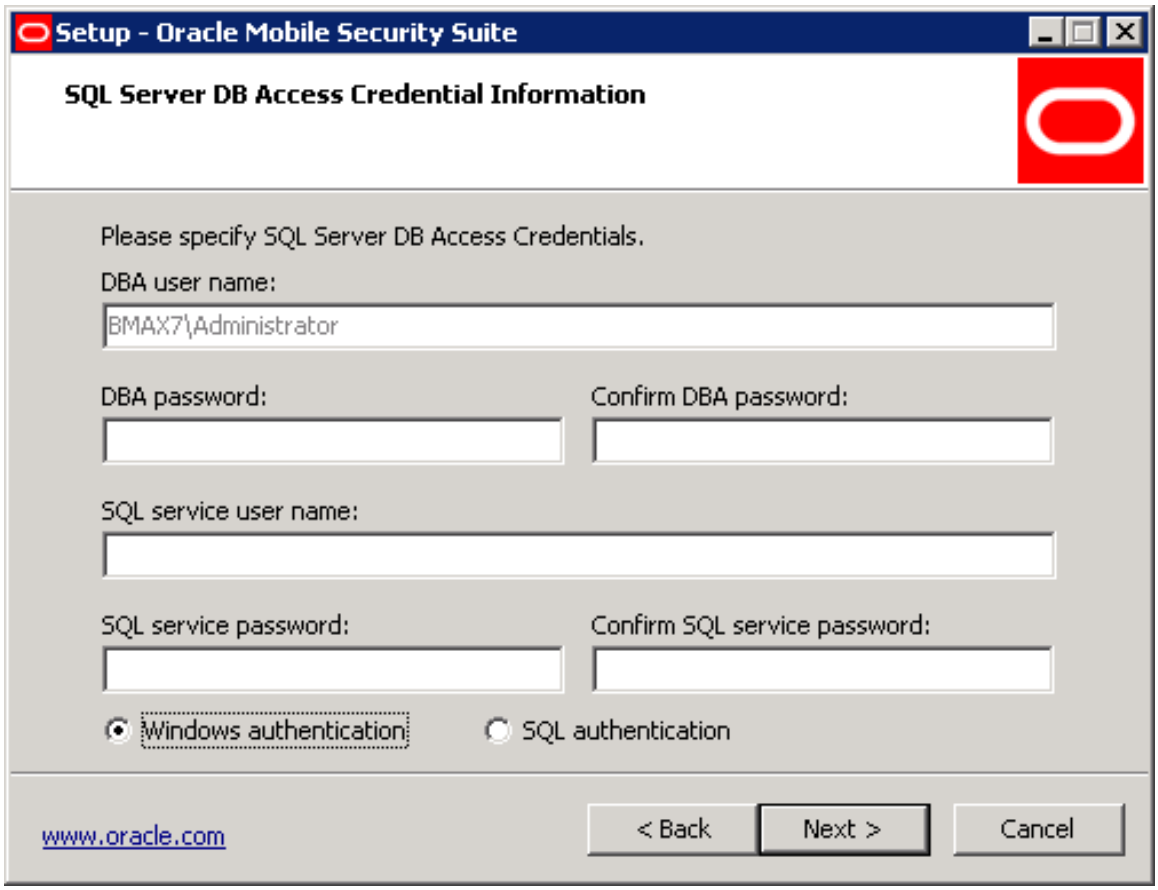
4.14 SQL Server DB Access Credential Information Screen

If the Mobile Security Administrative Console component was selected with Microsoft SQL Server, then the following screen will be shown.

In this example, on the prior screen the current user was selected for DBA credentials in order to leverage the privileges of the currently logged on Windows account. The password fields are disabled for the DBA credentials. If on the previous dialog **DBA SQL user** had been chosen then the fields would have been enabled for input of the DBA credentials. The DBA password is never stored on the file system and is only used to run database scripts and assign `dbowner` to the SQL account specified in this screen.

The SQL account can be either a Windows account or a native SQL account. The syntax used for this field is *`domain\user`* for Windows authentication, and `user` for native SQL account. This is the same behavior and syntax used in the Microsoft SQL Management Console. The installer supports a SQL account (Windows or SQL type) that is defined on the database server and not on a specific database instance. The SQL account must be defined prior to running the Oracle Mobile Security Suite installer.

Click **Next**.

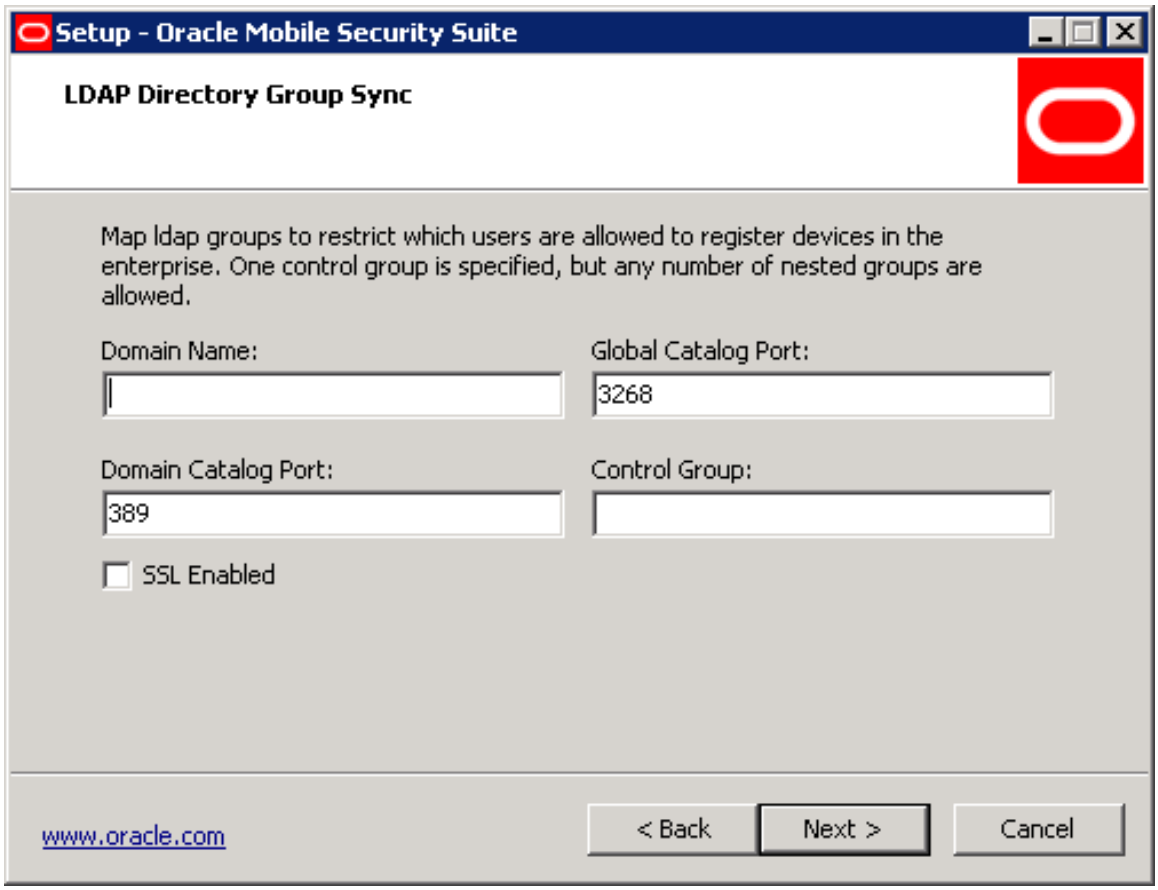


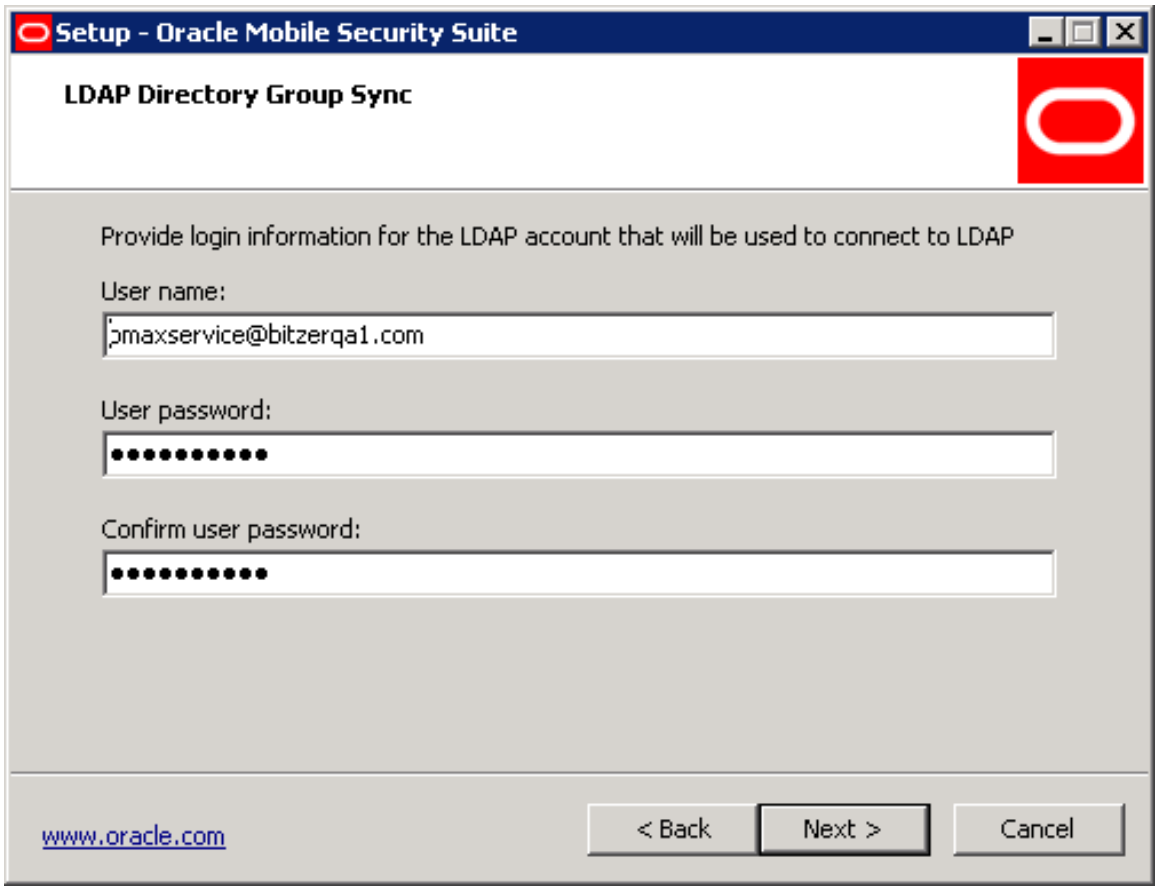
4.15 Oracle Unified Directory Group Sync Screen

The following screen appears if the Mobile Security Administrative Console component was selected with Oracle Unified Directory Sync.

Enter the host name of the LDAP server, associated port, whether SSL is enabled, and the Base DN with the LDAP directory. The LDAP control group can be any type of LDAP group (static or dynamic). Please refer to Oracle Unified Directory documentation for more information. The control group can contain users or groups, and static groups can contain nested groups. As long as a user's group membership resolves with at least one group underneath the control group, they will be allowed to register their device with the Mobile Security Access Server solution.

This option requires an LDAP account with read access for Oracle Unified Directory users and groups. The account password is encrypted on the file system.


Setup - Oracle Mobile Security Suite
LDAP Directory Group Sync
Map ldap groups to restrict which users are allowed to register devices in the enterprise. One control group is specified, but any number of nested groups are allowed.
Domain Name:
Global Catalog Port:
3268
Domain Catalog Port:
389
Control Group:
SSL Enabled
www.oracle.com
< Back
Next >
Cancel



Click **Next**.

4.16 Active Directory Group Sync Screen

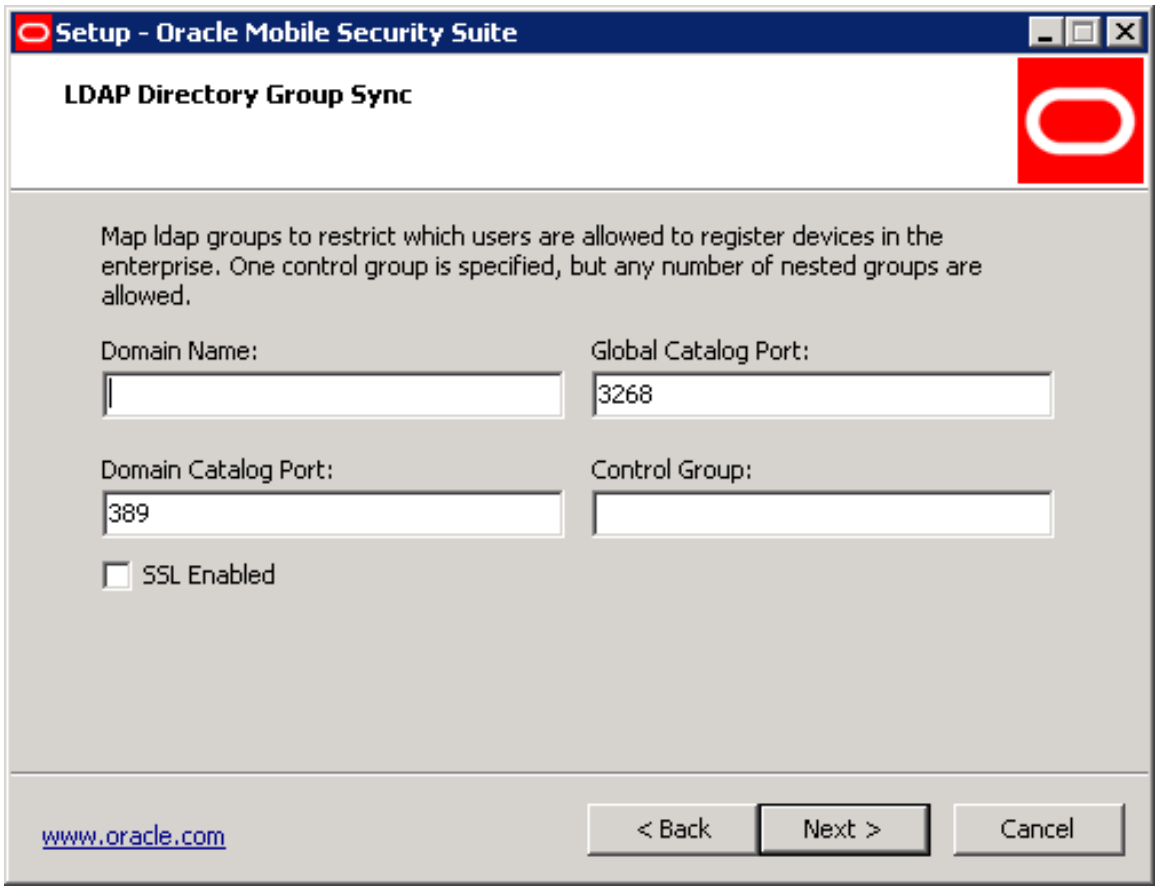
If the Mobile Security Administrative Console component was selected with Active Directory Sync, the following screen will be shown.

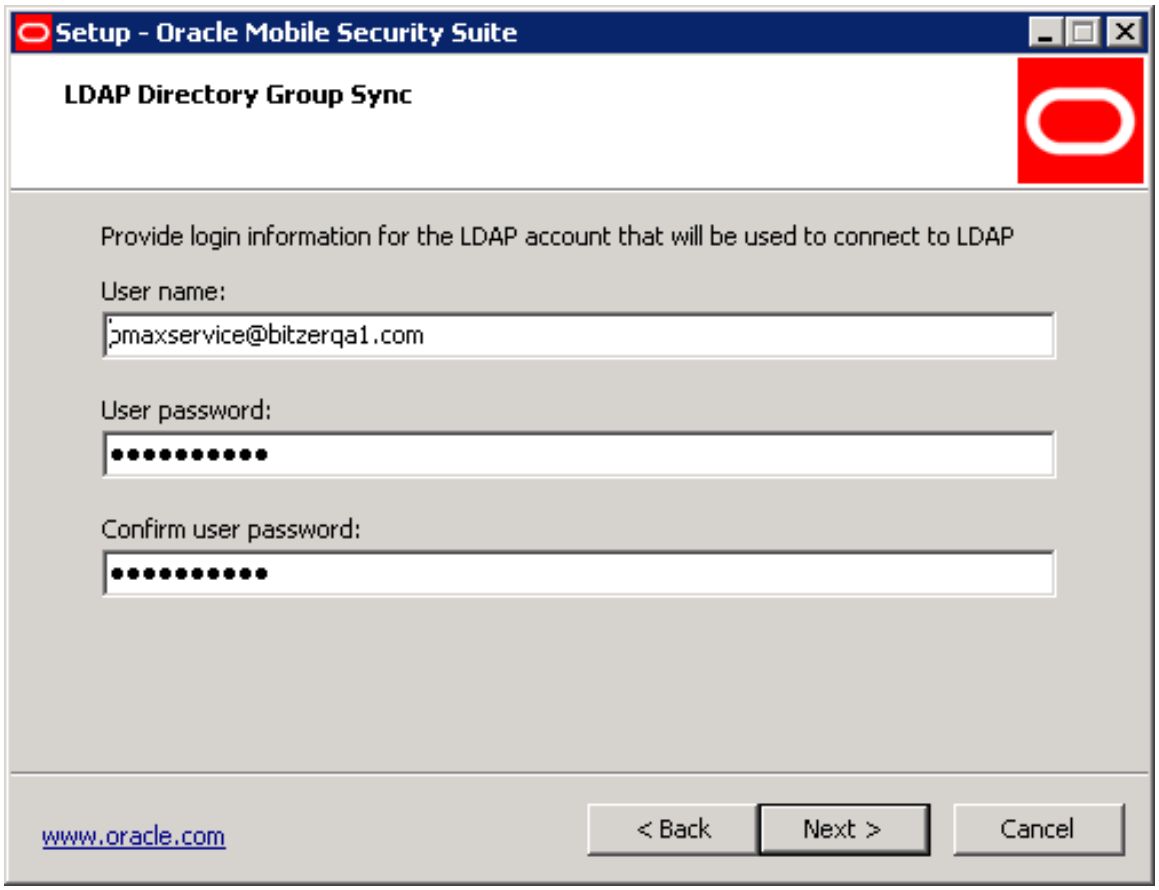
This option will automatically be selected when Mobile Security Administrative Console is installed on IIS or when User Certificate Provisioning is chosen.

Enter the domain where the control group is located. The AD control group can be any type of Windows group (Global, Local, or Universal). Please refer to Microsoft documentation on Windows groups for more information. The control group can contain users or groups, and groups can be nested. As long as a user's group membership resolves with at least one group underneath the control group, they will be allowed to register their device with the Mobile Security Access Server solution.

This option requires Windows credentials for an account with read access for Active Directory groups. Either service account User Principal Name (UPN) or the fully qualified DN (FQDN) of the user account is required. The user password is encrypted on the file system if this option is chosen.

Click **Next**.


Setup - Oracle Mobile Security Suite
LDAP Directory Group Sync
Map ldap groups to restrict which users are allowed to register devices in the enterprise. One control group is specified, but any number of nested groups are allowed.
Domain Name:
Global Catalog Port:
3268
Domain Catalog Port:
389
Control Group:
SSL Enabled
www.oracle.com
< Back
Next >
Cancel

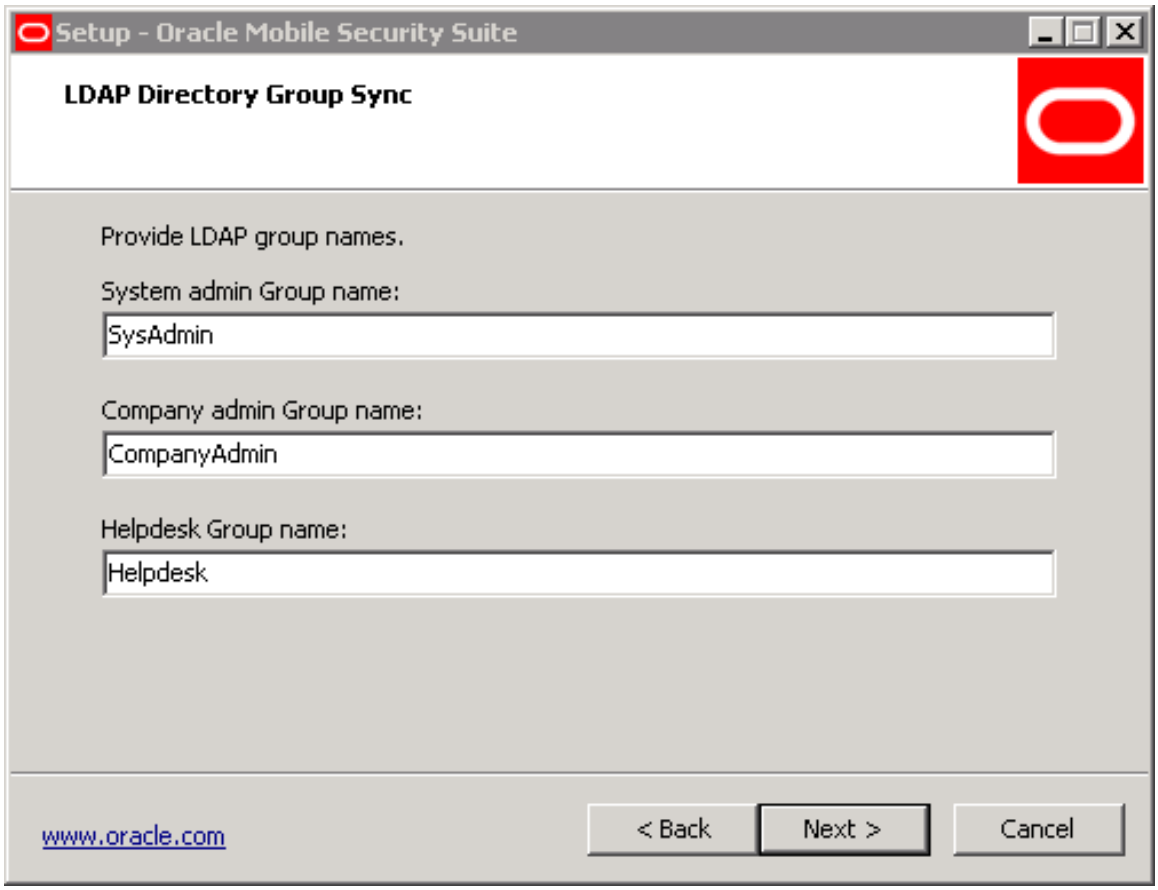


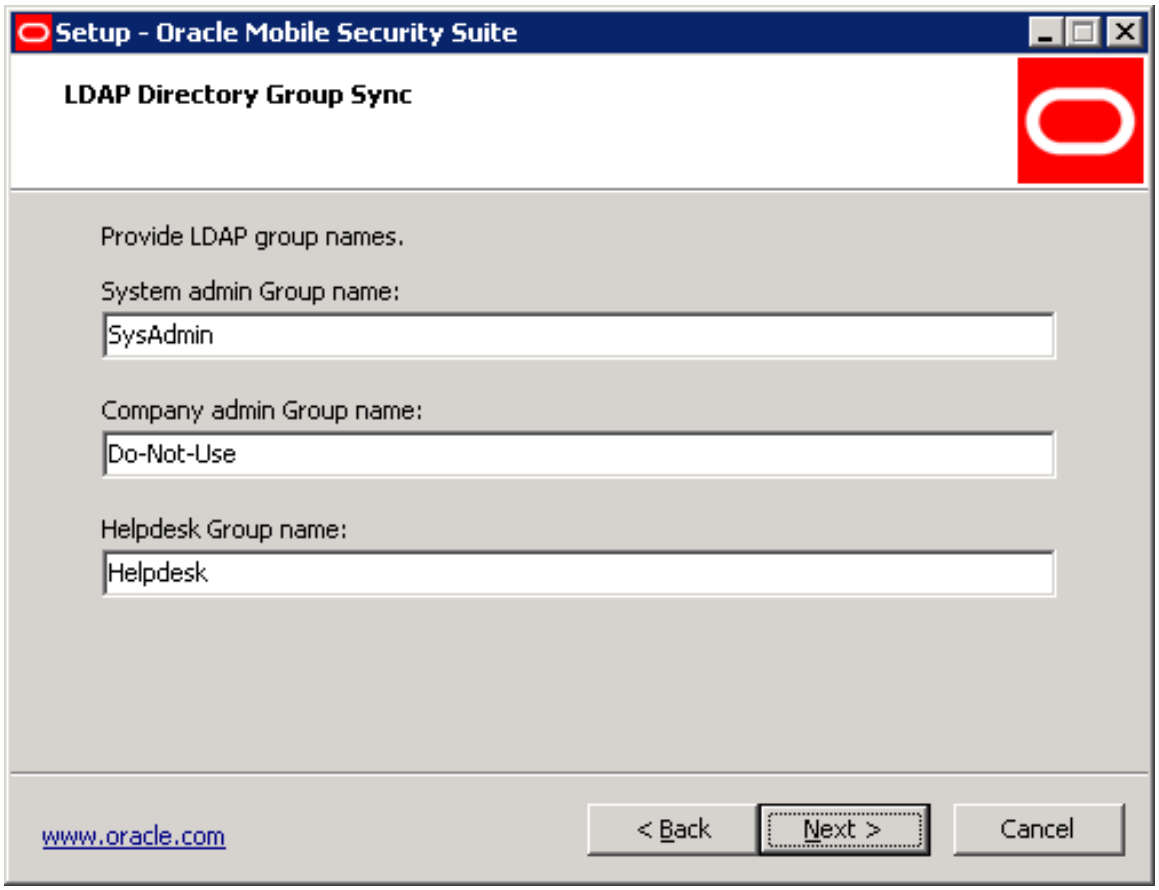
4.17 Active Directory Group Information Screen

If the Mobile Security Administrative Console component was selected and the LDAP Sync option was chosen then the following screen will be shown.

Enter the LDAP group name that you wish to associate with the system administrator, company administrator, and help-desk roles within Mobile Security Administrative Console. If you wish to use only two roles, enter a group that does not exist, for example `Do-Not-Use` as shown in the second screen.

Click **Next**.

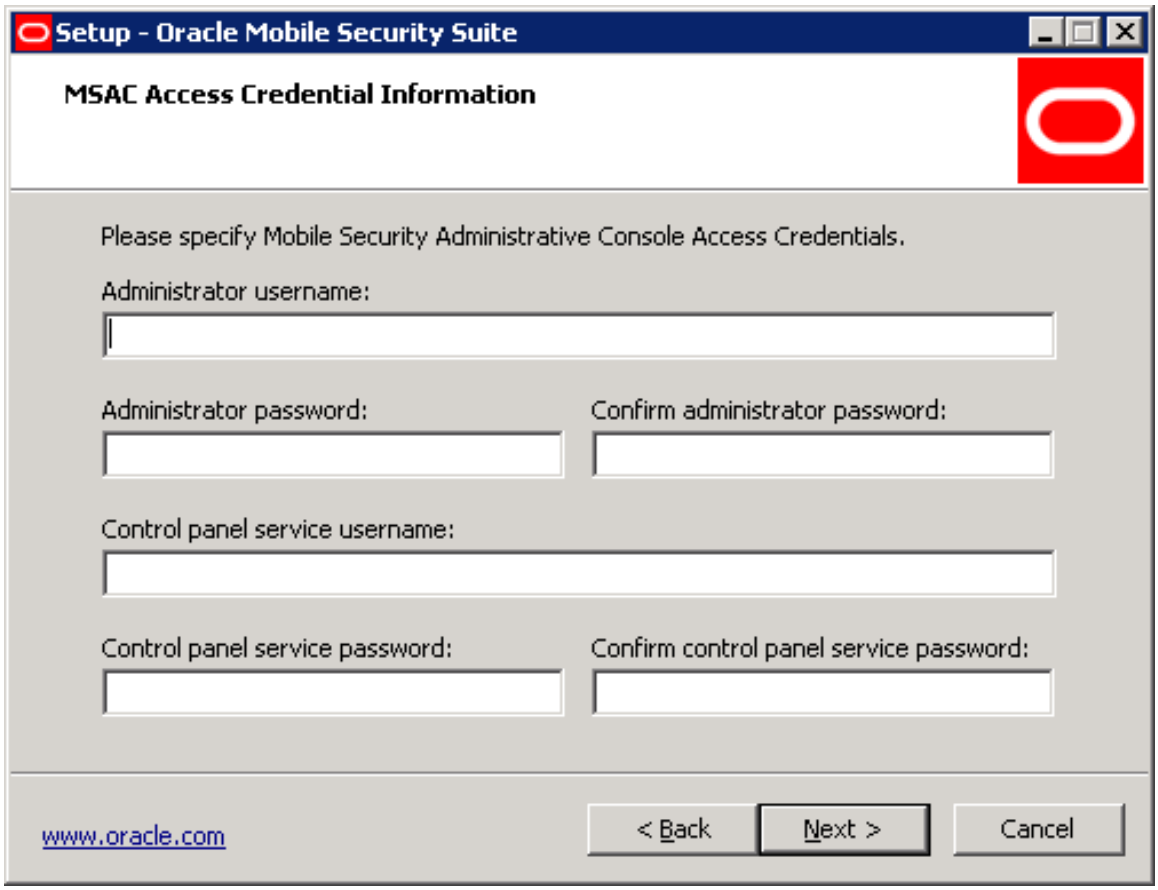

Setup - Oracle Mobile Security Suite
LDAP Directory Group Sync
Provide LDAP group names.
System admin Group name:
SysAdmin
Company admin Group name:
CompanyAdmin
Helpdesk Group name:
Helpdesk
www.oracle.com
< Back
Next >
Cancel



4.18 Administrative Console Access Credential Information Screen

Enter the desired credential information for the initial administrator user that will manage Mobile Security Administrative Console. Also enter the credentials that the Mobile Security Access Server will use to access the Administrative Console Service.

Click **Next**.



4.19 Select Certificate Screen

There are three options for providing certificates to the Mobile Security Access Server installer:

- Create separate files with the server certificate, the server private key, and the CA certificate chain for the client certificates. All three should be in PEM format.
- Use one file that contains both the server certificate and the server private key in PKCS12 format and another can contain the CA certificate chain for the client certificates in PEM format.
- Use the Windows certificate store which is part of the Windows operating system using the Cryptographic Application Programming Interface (CAPI). The certificate should already be installed prior to the installation. In addition, the CA certificate chain for the client certificates in PEM format is required.
- Generate a self-signed certificate for the Mobile Security Access Server. If using a self-signed certificate it must be explicitly trusted on the mobile device after it is generated in order for the Mobile Security Container to trust the Mobile Security Access Server.

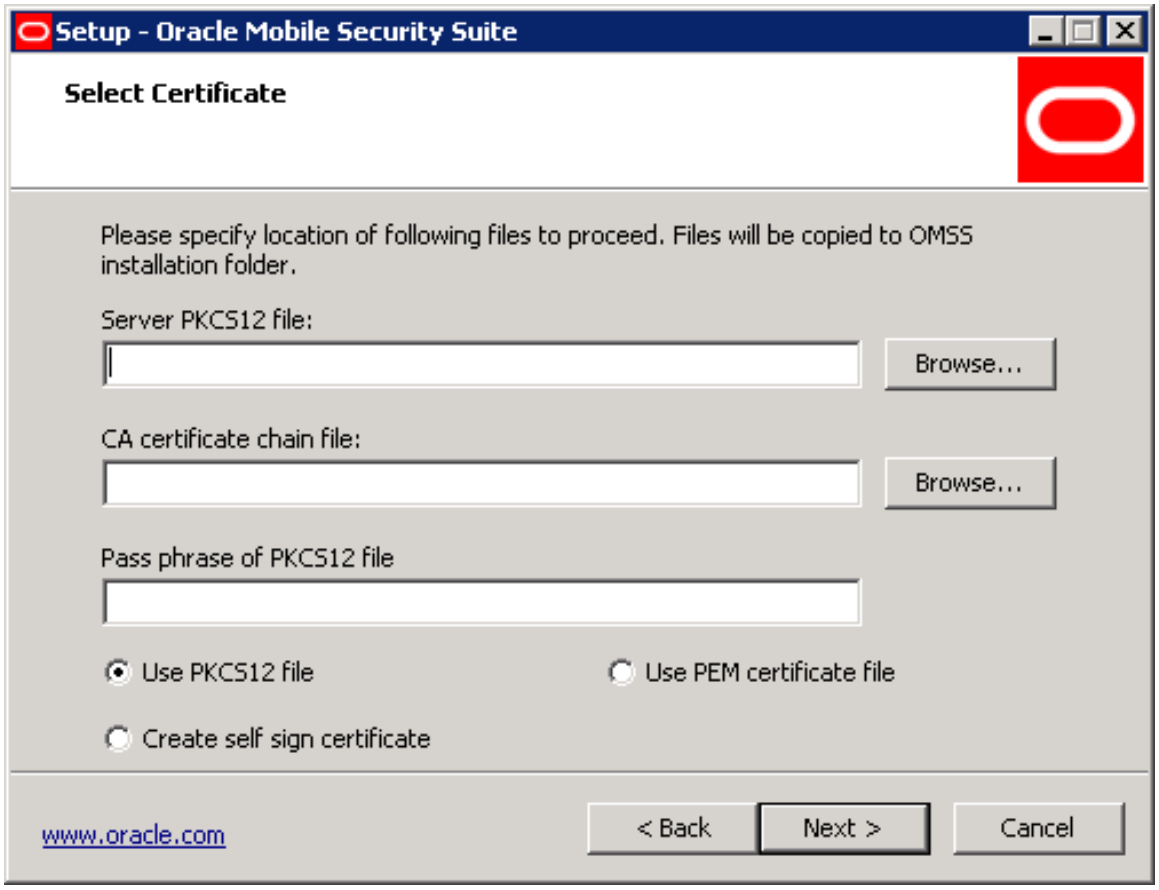
The CA certificate chain file should contain the full chain for all certificate authorities that the Mobile Security Access Server needs to trust. This should include:

- The CA certificate chain for the Active Directory domain controllers.
- The CA certificate chain for the user certificate if using PKINIT.
- The CA certificate chain for the Mobile Security Access Server certificate itself.

4.20 Select PKCS12 File Screen

Select a server PKCS12 file ending with `.pfx` or `.p12` and provide the pass phrase that was used to export the certificates/keys. Select the file in PEM format that contains the CA certificate chain for the client certificates.

Click **Next**.

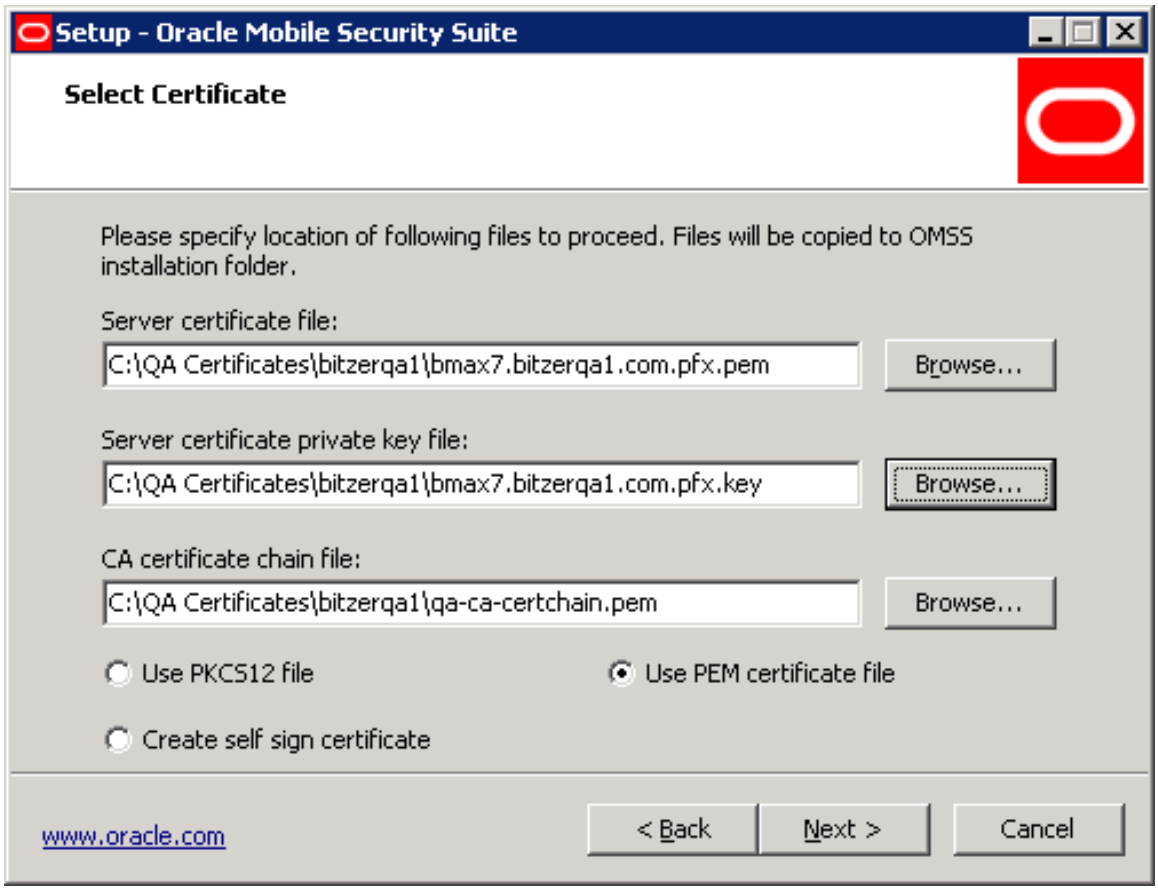


4.21 Select PEM Certificate Screen

Select the files for the server certificate, server private key, and CA certificate chain for the client certificates by clicking **Browse** next to the text field.

> **Note:** This Option Is Not Available if Mobile Security Notification Server is selected.

Click **Next**.



4.22 Select Windows Certificate Store Screen

Enter the common name (subject name) of the server certificate, and then the CA certificate chain for the client certificates by clicking on the Browse button. Choose either service account or Local System account from the **Select account type** list. The account must have rights to access the certificate in the corresponding Microsoft cryptographic store and use the private key.

It is recommended to use a service account. The advantages of using a service account personal store over the Local System account store are:

- Only the service account has access to the private key.
- Accessing the private key in the Local System store requires local administrator privileges.

Refer to Section A.10, "Configuring Certificates for Service Accounts" for more information.

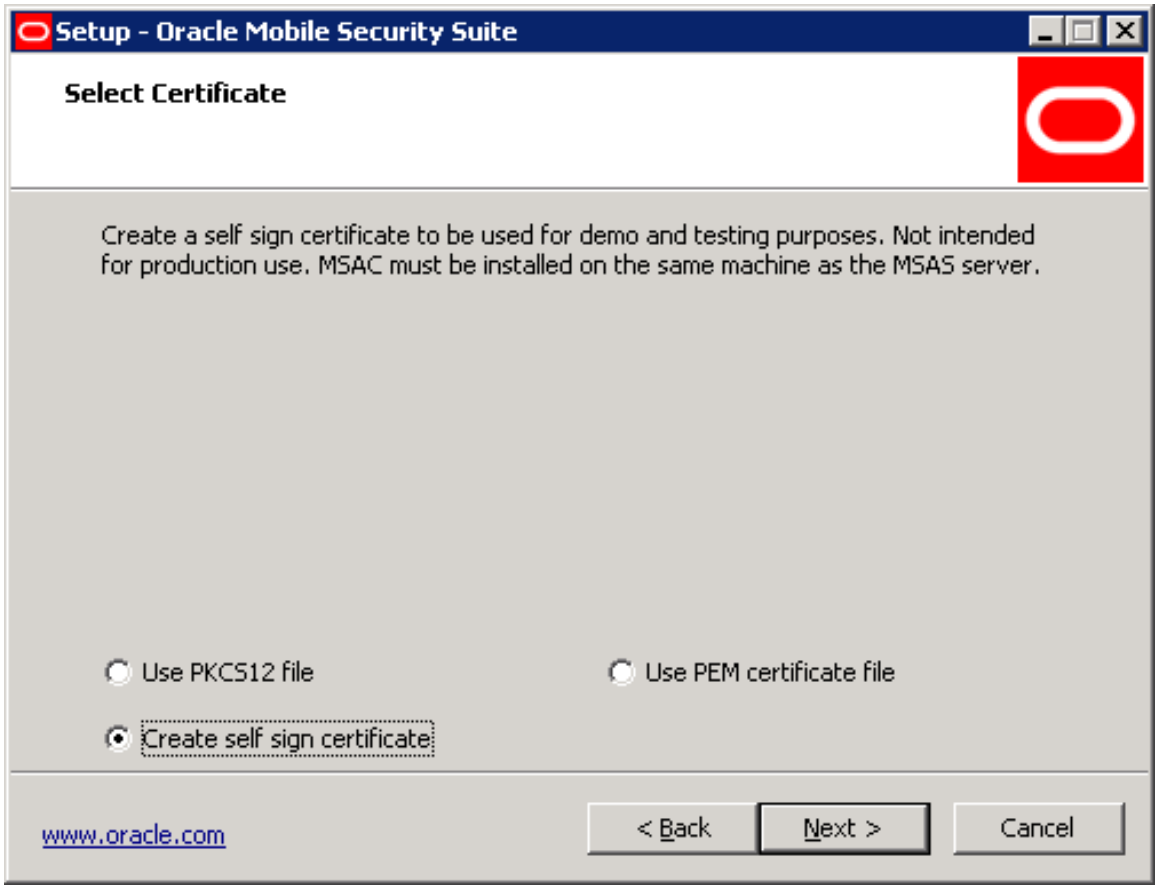
Note: This Option Is Not Available if Mobile Security Notification Server is selected.

Click **Next**.

4.23 Select Self Sign Certificate Screen

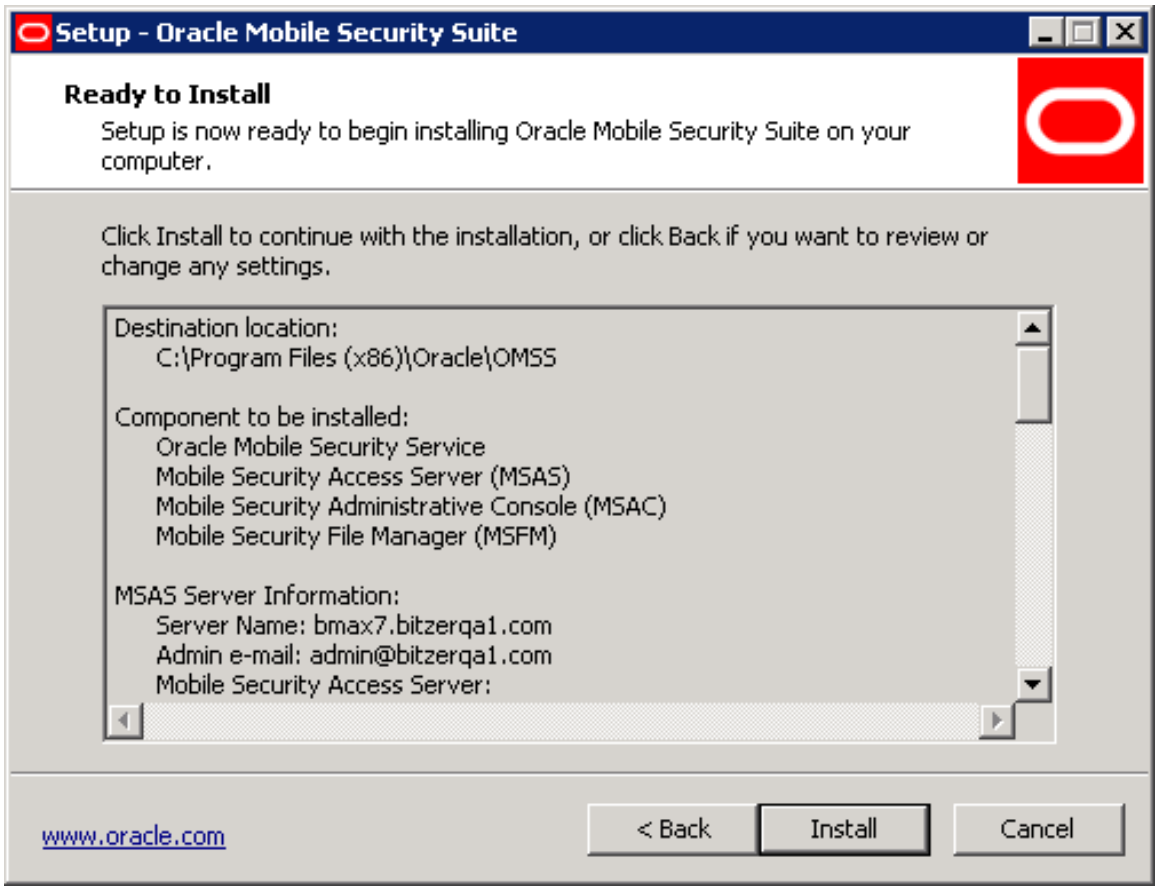
When Oracle Access Manager or KINIT is the primary authentication method, it is possible to use a self-signed certificate. This should be used only for proof of concepts and in labs, not in production. This certificate will need to be installed on the device to trust the Mobile Security Access Server.

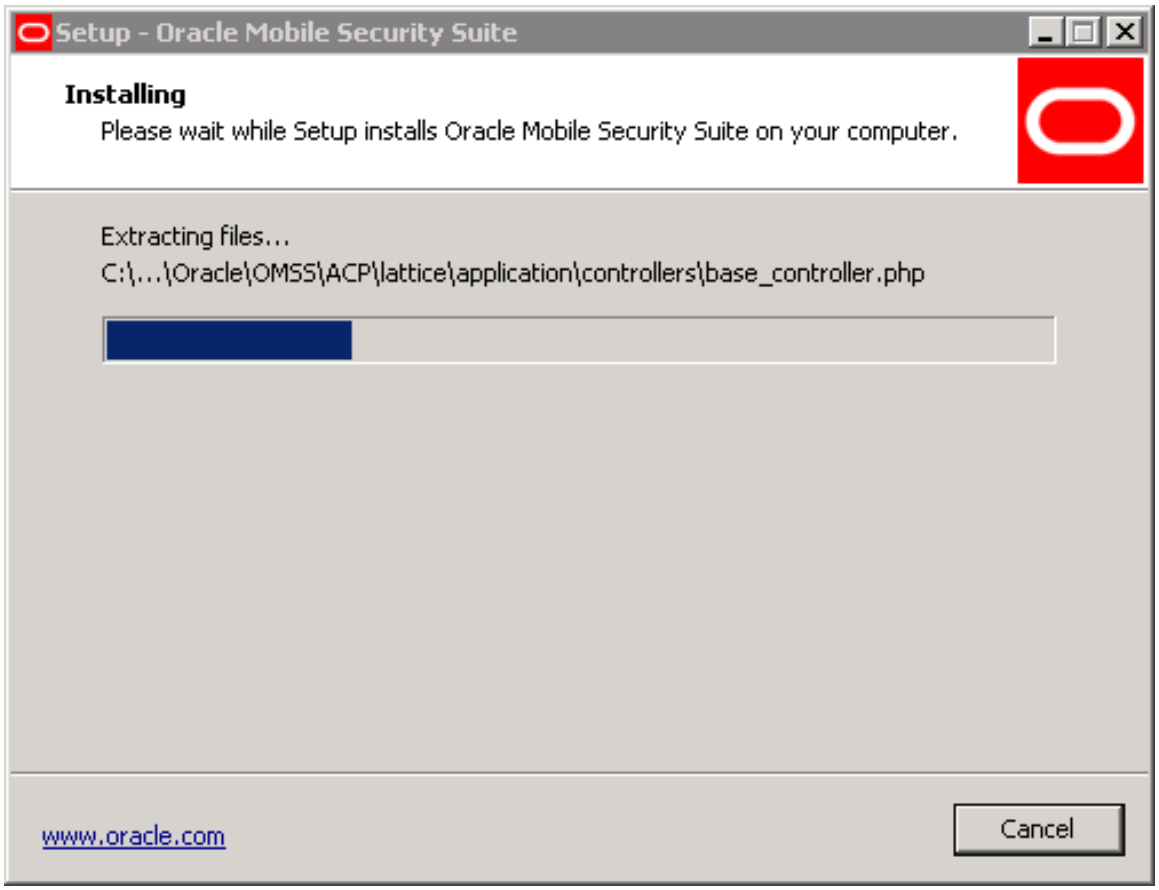
Click **Next**.



4.24 Ready to Install Screen

This screen summarizes all of the information provided so far. Review the information and select **Back** to make any changes. If everything is correct, click **Install** to perform the installation.


Setup - Oracle Mobile Security Suite
Ready to Install
Setup is now ready to begin installing Oracle Mobile Security Suite on your computer.
Click Install to continue with the installation, or click Back if you want to review or change any settings.
Destination location:
C:\Program Files (x86)\Oracle\OMSS
Component to be installed:
Oracle Mobile Security Service
Mobile Security Access Server (MSAS)
Mobile Security Administrative Console (MSAC)
Mobile Security File Manager (MSFM)
MSAS Server Information:
Server Name: bmax7.bitzerqa1.com
Admin e-mail: admin@bitzerqa1.com
Mobile Security Access Server:
www.oracle.com
< Back
Install
Cancel



4.25 Finished Screen

Click **Finish** to complete the installation. If the you select **Yes, restart the computer now**, the machine will restart. If you select **No, I will restart the computer later**, the installation ends.

5

Installing Oracle Mobile Security Suite on Linux

This chapter describes how to install Oracle Mobile Security Suite on Oracle Linux 6.

The Oracle Mobile Security Suite is delivered as a set of RPM packages, one for each of the individual server components:

You can install these RPM packages on the same or different systems, as noted in Section 2.3.2, "Mobile Security Access Server Requirements." When you install multiple server components on the same system, you must install them in the following order:

1. Mobile Security Administrative Console: `msac-3.0-0.el6.x86_64.rpm`
2. Mobile Security Notification Server: `msns-3.0-0.el6.x86_64.rpm`
3. Mobile Security File Manager: `msfm-3.0-0.el6.x86_64.rpm`
4. Mobile Security Access Server: `msas-3.0-0.el6.x86_64.rpm`

The installation processes for all server components require a PKCS#12 file containing the SSL server certificate and key, as well as the corresponding server certification CA trust chain file. Both of those files must be available on the system before installation.

All of the server components use a configuration variables file, `vars.conf`, as input to the configuration process. These files use the = character as a delimiter between a key on the left and the replacement value on the right. It is important to only modify the values to the right of the = character.

This chapter contains the following sections:

5.1 Installing Mobile Security Administrative Console

Follow these steps to install and configure the Mobile Security Administrative Console on Linux:

1. Use the following command to install the Mobile Security Administrative Console RPM:

   ```
   sudo rpm -ivh msac-3.0-0.el6.x86_64.rpm
   ```

   The Mobile Security Administrative Console RPM has several dependencies. A number of these are included with the Mobile Security Administrative Console RPM in a dependency zip package. There is a `dependency-install.sh` script in the zip package that can be run to install the included dependencies, or the dependencies can be installed individually using the commands in the scripts as a reference. Other dependencies are normally available on Oracle Linux 6 systems. You must install any that are not present. The install command fails with an error message if any dependencies are not present.

   The Mobile Security Administrative Console is installed under: `/opt/oracle/omss/msac/`

2. Edit the configuration variables file, which is installed by the Mobile Security Administrative Console RPM at: `/opt/oracle/omss/msac/templates/vars.conf`

   Edit this file to include all information necessary for configuration of the Mobile Security Administrative Console. Modify only the values to the right of the `=` character.

   The Mobile Security Administrative Console on Oracle Linux supports either a remote Oracle Database or a locally installed MySQL database. It does not support Microsoft SQL Server.

   If you are configuring the Mobile Security Administrative Console with an Oracle Database, then you must have previously created the table space and temporary table space, indicated in the respective configuration variables, in the database. The table space and temporary table space names must not be the same.

   The configuration variables that you must set for the Mobile Security Administrative Console are as follows:

   - `server_name`: The public host name of the Mobile Security Administrative Console. The server name must match the certificate subject name or subject alternative name present in the Mobile Security Administrative Console certificate.
   - `server_admin_email`: The email address of the server administrator.
   - `http_port`: The HTTP port exposed by the Mobile Security Administrative Console. By default this is 80.
   - `server_ssl_port`: The HTTPS port exposed by the Mobile Security Administrative Console. By default this is 443.
   - `db_name`: The name of the database configured with the Mobile Security Administrative Console. This should be `mysql` for the MySQL database and `oracle` for the Oracle Database. By default this is `mysql`.
   - `company_name`: The name of the company that you want displayed in the Mobile Security Administrative Console.
   - `master_server`: Indicate `yes` if this instance of the Mobile Security Administrative Console will be configured as the master server, or else `no`. The default value is `yes`.
   - `db_created`: Indicate `yes` if the database schema is already created, or else `no`. The default value is `no`. It must be `no` if the Mobile Security Administrative

Console is configured with the MySQL database. If `yes` is indicated, then none of the following table space variables should be set.

- `db_host_name`: The primary database server's host name. Leave it empty if configuring the Mobile Security Administrative Console with the MySQL database.
- `db_port`: The primary database server's port. Leave it empty if configuring the Mobile Security Administrative Console with the MySQL database.
- `sec_db_host_name`: The secondary database server's host name. Leave it empty if configuring the Mobile Security Administrative Console with the MySQL database.
- `sec_db_port`: The secondary database server's port. Leave it empty if configuring the Mobile Security Administrative Console with the MySQL database.
- `odb_service_name`: The Oracle Database service name. Leave it empty if configuring the Mobile Security Administrative Console with the MySQL database.
- `dba_user_name`: The DBA user name to use when creating and populating the database schema. Leave it empty if configuring the Mobile Security Administrative Console with the MySQL database.
- `dba_pwd`: The DBA user's password. Leave it empty if configuring the Mobile Security Administrative Console with the MySQL database.
- `acp_app_db_name`: The Mobile Security Administrative Console application schema name. The default value is `lattice`. It must be `lattice` if configuring the Mobile Security Administrative Console with the MySQL database.
- `acp_rep_db_name`: The Mobile Security Administrative Console reporting schema name. The default value is `reporting`. It must be `reporting` if configuring the Mobile Security Administrative Console with the MySQL database.
- `acp_audit_db_name`: The Mobile Security Administrative Console audit schema name. The default value is `audit`. It must be `audit` if configuring the Mobile Security Administrative Console with the MySQL database and it must NOT be `audit` if configuring with the Oracle Database.
- `db_service_uid`: The DB service UID used to access the Oracle Database by the Mobile Security Administrative Console. Leave it empty if configuring the Mobile Security Administrative Console with the MySQL database.
- `db_service_pwd`: The DB service password used to access the Oracle Database by the Mobile Security Administrative Console. Leave it empty if configuring the Mobile Security Administrative Console with the MySQL database.
- `odb_lat_tspace_name`: The table space name to create the application schema in the Oracle Database. Leave it empty if configuring the Mobile Security Administrative Console with the MySQL database.
- `odb_lat_tetspace_name`: The temporary table space name to create the application schema in the Oracle Database. Leave it empty if configuring the Mobile Security Administrative Console with the MySQL database.
- `odb_rep_tspace_name`: The table space name to create the reporting schema in the Oracle Database. Leave it empty if configuring the Mobile Security Administrative Console with the MySQL database.

- odb_rep_tetspace_name: The temporary table space name to create the reporting schema in Oracle Database. Leave it empty if configuring the Mobile Security Administrative Console with the MySQL database.
- odb_aud_tspace_name: The table space name to create the audit schema in the Oracle Database. Leave it empty if configuring the Mobile Security Administrative Console with the MySQL database.
- odb_aud_tetspace_name: The temporary table space name to create the audit schema in the Oracle Database. Leave it empty if configuring the Mobile Security Administrative Console with the MySQL database.
- odb_aapu_tspace_name: The table space name to create the application user schema in the Oracle Database. Leave it empty if configuring the Mobile Security Administrative Console with the MySQL database.
- odb_appu_tetspace_name: The temporary table space name to create the application user schema in the Oracle Database. Leave it empty if configuring the Mobile Security Administrative Console with the MySQL database.
- integrate_msns: Indicate yes if the Mobile Security Administrative Console will be integrated with the Mobile Security Notification Server, or else no. The default value is yes.
- ad_enabled: Indicate yes if the Mobile Security Administrative Console will be configured with an LDAP server for user and group management, or else no. The default value is yes.
- ldap_type: Indicate AD if the Mobile Security Administrative Console will be integrated with Microsoft Active Directory, or OUD if the Mobile Security Administrative Console will be integrated with Oracle Unified Directory. The default value is AD.
- acp_auth_email: The administrator user name to be configured for use with the Mobile Security Administrative Console.
- acp_auth_passwd: The administrator password to be configured for use with the Mobile Security Administrative Console.
- ecp_auth_email: The username to be configured for use with the Mobile Security Administrative Console control panel service.
- ecp_auth_passwd: The password to be configured for use with the Mobile Security Administrative Console control panel service.
- httpd_user_name: The user with which the server will answer requests.
- httpd_group_name: The group under which the server will answer requests.
- server_cert_p12_file_path: The location of the PKCS#12 file containing the SSL server certificate and key. The corresponding PKCS#12 password will be prompted when the configuration script is run.
- server_cert_ca_chain_file_path: The location of the server certification CA trust chain file (in PEM format).

3. After the configuration variables file has been edited with appropriate information, run the configuration script, as follows, to configure the Mobile Security Administrative Console:

```
sudo /opt/oracle/omss/msac/templates/configure.sh
```

When you run the script, you are prompted twice for the password of the PKCS#12 file containing the SSL server certificate and key. If the configuration

script runs without error, then the Mobile Security Administrative Console is configured with the values from the configuration variables file.

Note: The configuration script also locks down the permissions on the directories and files under `/opt/oracle/omss/msac/` to the user and group specified in the configuration variables file.

Refer to Section 5.5 for instructions on how to run the Mobile Security Administrative Console.

If the Mobile Security Administrative Console has been integrated with the Mobile Security Notification Server or an LDAP server, then you must update the configuration information for the system in the Mobile Security Administrative Console. Update this system configuration information as follows:

a. Login to the Mobile Security Administrative Console.

b. Go to the **Settings** tab.

c. Go to **LDAP Settings**, update the configuration information, and click **Save**.

If you have an Oracle Unified Directory installation with users under multiple domain entries (base DNs), you must specify all of the corresponding domain entries, separated by semicolons, in the base DN setting.

d. Go to **Notification Settings**, update the configuration information, and click **Save**.

5.2 Installing Mobile Security Notification Server

Follow these steps to install and configure the Mobile Security Notification Server on Linux:

1. Run the following command to install the Mobile Security Notification Server RPM:

```
sudo rpm -ivh msns-3.0-0.el6.x86_64.rpm
```

The Mobile Security Notification Server RPM has several dependencies. A number of these are included with the Mobile Security Notification Server RPM in a dependency zip package. There is a `dependency-install.sh` script in the zip package that can be run to install the included dependencies, or the dependencies can be installed individually using the commands in the script as a reference. Other dependencies are normally available on Oracle Linux 6 systems. You must install any that are not present. The install command fails with an error message if any dependencies are not present.

The Mobile Security Notification Server is installed under: `/opt/oracle/omss/msns/`

2. Edit the configuration variables file, which is installed by the Mobile Security Notification Server RPM at: `/opt/oracle/omss/msns/templates/vars.conf`

You must include all information necessary for configuration of the Mobile Security Notification Server. The configuration variables file contains two sections, and you must only edit the first section. Modifying any information in the second section will likely result in a misconfiguration. Modify only the values to the right of the = character.

You must set the following configuration variables:

- server_name: The public host name of the Mobile Security File Manager. The server name must match the certificate subject name or subject alternative name present in the Mobile Security File Manager certificate.
- http_port: The HTTP port exposed by the Mobile Security Administrative Console. By default this is 8080.
- server_ssl_port: The HTTPS port exposed by the Mobile Security Administrative Console. By default this is 8443.
- server_cert_p12_file_path: The location of the PKCS#12 file containing the SSL server certificate and key. The corresponding PKCS#12 password will be prompted when the configuration script is run.
- server_cert_ca_chain_file_path: The location of the server certification CA trust chain file, in PEM format.
- db_name: The name of the database configured with the Mobile Security Notification Server. This should be mysql for the MySQL database and oracle for the Oracle Database. By default this is mysql.
- db_created: Indicate yes if the database schema is already created, or else no. The default value is no. It must be no if you are configuring the Mobile Security Notification Server with the MySQL database. If yes is indicated, then none of the following table space variables should be set.
- db_host_name: The primary database server's host name. Leave it empty if configuring the Mobile Security Notification Server with the MySQL database.
- db_port: The primary database server's port. Leave it empty if configuring the Mobile Security Notification Server with the MySQL database.
- sec_db_host_name: The secondary database server's host name. Leave it empty if configuring the Mobile Security Notification Server with the MySQL database.
- sec_db_port: The secondary database server's port. Leave it empty if configuring the Mobile Security Notification Server with the MySQL database.
- odb_service_name: The Oracle Database service name. Leave it empty if configuring the Mobile Security Notification Server with the MySQL database.
- dba_user_name: The DBA user name to use when creating and populating the database schema. Leave it empty if configuring the Mobile Security Notification Server with the MySQL database.
- dba_pwd: The DBA user's password. Leave it empty if configuring the Mobile Security Notification Server with the MySQL database.
- msns_db_name: The Mobile Security Notification Server application schema name. The default value is bns. It must be bns if configuring the Mobile Security Notification Server with the MySQL database.
- odb_msns_tspace_name: The table space name to create the application schema in the Oracle Database. Leave it empty if configuring the Mobile Security Notification Server with the MySQL database.
- odb_msns_tetspace_name: The temporary table space name to create for the application schema in the Oracle Database. Leave it empty if configuring the Mobile Security Notification Server with the MySQL database.
- db_service_pwd: The Database service password used to access the Oracle Database by the Mobile Security Notification Server. Leave it empty if configuring the Mobile Security Notification Server with the MySQL database.

- msns_service_uname: The Mobile Security Notification Server service user name.
- msns_service_pwd: The Mobile Security Notification Server service password.

3. After you have edited the configuration variables file with complete information, run the following command to configure the Mobile Security Notification Server:

```
sudo /opt/oracle/omss/msns/templates/configure.sh
```

When you run the script, you are prompted twice for the password of the PKCS#12 file containing the SSL server certificate and key. If the configuration script runs without error, then the Mobile Security Notification Server is configured with the values from the configuration variables file.

Note: The configuration script also locks down the permissions on the directories and files under /opt/oracle/omss/msns/ to the user and group specified in the configuration variables file.

Refer to Section 5.6 for instructions on how to run the Mobile Security Notification Server.

5.3 Installing Mobile Security File Manager

Follow these steps to install and configure the Mobile Security File Manager on Linux:

1. Run the following command to install the Mobile Security File Manager RPM:

```
sudo rpm -ivh msfm-3.0-0.el6.x86_64.rpm
```

The Mobile Security File Manager RPM has several dependencies. A number of these are included with the Mobile Security File Manager RPM in a dependency zip package. There is a dependency-install.sh script in the zip package that can be run to install the included dependencies, or the dependencies can be installed individually using the commands in the script as a reference. Other dependencies are normally available on Oracle Linux 6 systems. You must install any that are not present. The install command fails with an error message if any dependencies are not present.

The Mobile Security File Manager is installed under: /opt/oracle/omss/msfm/

2. Edit the configuration variables file, which is installed by the Mobile Security File Manager RPM at: /opt/oracle/omss/msfm/templates/vars.conf

You must include all information necessary for configuration of the Mobile Security File Manager. The configuration variables file contains two sections, and you must only edit the first section. Modifying any information in the second section will likely result in a misconfiguration. Modify only the values to the right of the = character.

You must set the following configuration variables:

- server_name: The public host name of the Mobile Security File Manager. The server name must match the certificate subject name or subject alternative name present in the Mobile Security File Manager certificate.
- http_port: The HTTP port exposed by the Mobile Security Administrative Console. By default this is 8080.

- server_ssl_port: The HTTPS port exposed by the Mobile Security Administrative Console. By default this is 8443.
- `server_cert_p12_file_path`: The location of the PKCS#12 file containing the SSL server certificate and key. The corresponding PKCS#12 password will be prompted when the configuration script is run.
- `server_cert_ca_chain_file_path`: The location of the server certification CA trust chain file (in PEM format).

3. After you have edited the configuration variables file with appropriate information, run following command:

   ```
   sudo /opt/oracle/omss/msfm/templates/configure.sh
   ```

   When you run the script, you are prompted twice for the password of the PKCS#12 file containing the SSL server certificate and key. If the configuration script runs without error, then the Mobile Security File Manager is configured with the values from the configuration variables file.

   Note: The configuration script also locks down the permissions on the directories and files under `/opt/oracle/omss/msfm/` to the user and group specified in the configuration variables file.

Refer to Section 5.6 for instructions on how to run the Mobile Security File Manager.

5.4 Installing Mobile Security Access Server

Install and configure the Mobile Security Access Server on Linux as follows:

1. Install the Mobile Security Access Server RPM, using the following command:

   ```
   sudo rpm -ivh msas-3.0-0.el6.x86_64.rpm
   ```

   The Mobile Security Access Server RPM has several dependencies. A number of these are included with the Mobile Security Access Server RPM in a dependency zip package. There is a `dependency-install.sh` script in the zip package that can be run to install the included dependencies, or the dependencies can be installed individually using the commands in the script as a reference. Other dependencies are normally available on Oracle Linux 6 systems. You must install any that are not present. The install command fails with an error message if any dependencies are not present.

   The Mobile Security Access Server is installed under: `/opt/oracle/omss/msas/`

2. Edit the configuration variables file, which is installed by the Mobile Security Access Server RPM at `/opt/oracle/omss/msas/templates/vars.conf`.

   You must include all information necessary for configuration of the Mobile Security Access Server. The configuration variables file contains two sections, and you should edit only the first section. Modifying any information in the second section will likely result in a misconfiguration. Modify only the values to the right of the = character.

   You must set the following configuration variables for the Mobile Security Access Server:

   - `HTTPD_USER`: The server answers requests as this user.
   - `HTTPD_GROUP`: The server answers requests as a member of this group.

- PROXY_PORT: The HTTP port exposed by the Mobile Security Access Server for standard proxy requests. By default, this is 80.
- AUTH_PORT: The HTTPS port exposed by the Mobile Security Access Server for authentication and AppTunnel requests. By default, this is 443.
- BMAX_SERVER_NAME: The public host name of the Mobile Security Access Server. The server name must match the certificate subject name or subject alternative name present in the Mobile Security Access Server certificate. The server name need not be the host name of the Mobile Security Access Server, but it must be resolvable in DNS by the mobile clients.
- SERVER_P12_FILE: The location of the PKCS#12 file containing the SSL server certificate and key. When the configuration script is run, it prompts for the corresponding PKCS#12 password.
- SERVER_CERTCHAIN_FILE: The location of the server certification CA trust chain file, in PEM format.
- LOCAL_ACP: Indicates whether the Mobile Security Administrative Console is deployed on the same system as the Mobile Security Access Server. If they are deployed separately, then this value should be no. If they are deployed together then this value should be yes.
- ECP_SERVICE_URL: The Mobile Security Administrative Console control panel service URL, which must include including scheme (http), port, and path, for example: https://msac.example.com:443/ecp/ecpservice
- ECP_SERVICE_UID: The username that was previously configured for the Mobile Security Administrative Console control panel service.
- ECP_SERVICE_PWD: The password that was previously configured for the Mobile Security Administrative Console control panel service.
- ENABLE_OAM: Indicates whether OAM authentication should be enabled, either yes or no. If this value is yes then all of the following OAM configuration variables must be set.
- OAM_SERVER_URL: The Oracle Access Manager Server URL including scheme (http or https) and port, for example: http://oam.example.com:1234 Required for Oracle Access Manager authentication.
- OAM_SERVICE_END_POINT: The Oracle Access Manager OAuth service end point. But default this is oauthservice. Required for Oracle Access Manager authentication.
- OAM_CLIENT_UID: The username that was previously configured for the Mobile Security Access Server when it was registered as an OAuth Confidential Client with the Oracle Access Manager OAuth Service. Required for Oracle Access Manager authentication.
- OAM_CLIENT_PWD: The password/secret that was previously configured for the Mobile Security Access Server when it was registered as an OAuth Confidential Client with the Oracle Access Manager OAuth Service. Required for Oracle Access Manager authentication.
- KRB_DOMAIN_NAME_UPPER: The primary Active Directory domain (Kerberos realm) for user authentication, in uppercase, for example: EXAMPLE.COM. Required for KINIT and PKINIT authentication. Additional domains/realms can be added to the krb5.conf file after this initial configuration.
- KRB_DOMAIN_NAME: The primary Active Directory domain (Kerberos realm) for user authentication, in lowercase, for example: example.com. Required for

KINIT and PKINIT authentication. Additional domains/realms can be added to the `krb5.conf` file after this initial configuration.

- `RADIUS_SERVER_INFO`: The RADIUS server, port, and shared secret in the following format:*`radiusserver`*`:`*`port`*`:`*`sharedsecret`*. Required for RADIUS OTP authentication. Additional RADIUS servers can be added to the radius.conf file after this initial configuration.
- `BMAX_RADIUS_ENABLED`: Indicates whether RADIUS authentication should be enabled, either `yes` or `no`. If this value is `yes` then all of the following RADIUS configuration variables need to be set.
- `BMAX_RADIUS_DOMAIN_NAME`: The domain name to append to user names if the RADIUS server is configured to accept a domain name other than the UPN. By default, this is empty.

3. After you have edited the configuration variables file, use the following command to configure the Mobile Security Access Server:

```
sudo /opt/oracle/omss/msas/templates/configure.sh
```

You are prompted twice for the password of the PKCS#12 file containing the SSL server certificate and key when the configuration script is run. If the configuration script displays does not display any errors during execution then the Mobile Security Access Server is configured with the values from the configuration variables file.

Note: The configuration script also locks down the permissions on the directories and files under `/opt/oracle/omss/msas/` to the user and group specified in the configuration variables file.

Refer to Section 5.5 for instructions on how to run the Mobile Security Access Server.

5.5 Running the Mobile Security Administrative Console and Access Server

The Mobile Security Administrative Console and Access Server can be started and stopped using standard Apache `httpd` commands.

Note: The Mobile Security Administrative Console and Mobile Security Access Server run within Apache `httpd` on Oracle Linux. You must use Apache's worker MPM binary, located at: `/usr/sbin/httpd.worker`

After the Mobile Security Access Server has been installed and configured, you start and stop it by using the following commands:

```
sudo /usr/sbin/httpd.worker -f /opt/oracle/omss/msas/conf/httpd.conf -k start

sudo /usr/sbin/httpd.worker -f /opt/oracle/omss/msas/conf/httpd.conf -k stop
```

Use the same commands if the Mobile Security Administrative Console and Access Server have been installed together on the same system.

If the Mobile Security Administrative Console has been installed and configured on a system without the Access Server, you start and stop it by using the following commands:

```
sudo /usr/sbin/httpd.worker -f /opt/oracle/omss/msac/conf/httpd.conf -k start

sudo /usr/sbin/httpd.worker -f /opt/oracle/omss/msac/conf/httpd.conf -k stop
```

> **Note:** Even though `sudo` is used to launch the services, they run as the `HTTPD_USER` you specified in the configuration variables file during configuration.

You can configure `cron` jobs to automatically start the Mobile Security Administrative Console and Access Server on system reboot.

5.6 Running the Mobile Security Notification Server and File Manager

Use the `omss` command to start and stop the Mobile Security Notification Server and File Manager.

> **Note:** The Mobile Security Notification Server and File Manager run within Tomcat on Oracle Linux.

After you have configured the Mobile Security Notification Server and File Manager, run the following commands to start and stop them.

```
sudo /sbin/service omss start
sudo /sbin/service omss stop
```

> **Note:** Even though sudo is used to launch the services, they run under the tomcat user account by default. You can customize this using the standard Tomcat configuration.

You can configure `cron` jobs to automatically start the Mobile Security Notification Server and File Manager on system reboot.

A

Advanced Configuration Options

This appendix describes advanced configuration options for Oracle Mobile Security Suite.

The Mobile Security Access Server supports a number of advanced configuration options that can be modified after installation. Although these options are described below, it is strongly recommended that customers engage Oracle professional services to set up these advanced configurations.

The instructions in this chapter 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.

This appendix contains the following sections:

A.1 Oracle Access Manager Configuration

In order for the Mobile Security Access Server to authenticate users against Oracle Access Manager and retrieve Oracle Access Manager and OAuth tokens for integrated single sign on, the Mobile Security Access Server must be registered as an OAuth Confidential Client with the Oracle Access Manager OAuth Service. This registration can be performed using the following steps:

1. Log in to the Oracle Access Manager Console, for example: `http://oamhost.example.com:7001/oamconsole`.
2. Select **Launch Pad -> Mobile and Social -> OAuth Service**.

3. Open **Default Domain** from the list of OAuth Identity Domains.
4. Select **OAuth Client -> OAuth Web Clients**.
5. Create a new OAuth client profile for the Mobile Security Access Server, for example:
   - **Name**: `Mobile Security Access Server`
   - **Client ID**: `8ec37bb7afa84d9eade6253a57d22f99` (this can be any value you choose)
   - **Client Secret**: `2Ni4yUJnFdFgLzdpuxMM` (this can be any value you choose)
6. Under Privileges, select **Allow access to all scopes**.
7. Under **Privileges-> Grant Types**, select all grant types.
8. Click **Create**.

During installation of the Mobile Security Access Server, you are prompted to enter the Client UID and Client Password. These must be the same values you just configured as the **Client ID** and **Client Secret**.

A.2 Oracle Unified Directory Configuration

To get optimal performance for LDAP sync with Oracle Unified Directory, it is recommended that all the entries and groups be in the OUD database cache and all the groups be in the OUD entry cache.

As a reference, for a deployment with 100k users (of size 1-4KB per entry) containing approximately 5k moderately large static groups, a reasonable value is to reserve 6GB for the OUD heap size.

The steps for configuring the desired heap size are different for OpenJDK than for Oracle Java Hotspog. Follow the approrpriate steps to configure the desired heap size.

OpenJDK

1. Edit *OUD_INSTANCE*`/OUD/config/java.properties` and set the following:

   ```
   start-ds.java-args=-Xmn1g -Xms6g -Xmx6g -d64 -server
   ```

2. Launch: *OUD_INSTANCE*`/OUD/bin/dsjavaproperties`
3. Restart the OUD instance:

   OUD_INSTANCE`/OUD/bin/stop-ds;` *OUD_INSTANCE*`/OUD/bin/start-ds`

Oracle Java HotSpot

- Set up the 6GB OUD heap size at instance creation using: *MIDDLEWARE_HOME*`/Oracle_OUD1/oud-setup` (both graphical user interface and command-line interface)
- If the instance has already been created and you must reconfigure it, you can use: *OUD_INSTANCE*`/OUD/bin/dstune` and set a 6GB heap size for the OUD instance.

In addition, it is recommended that you enable the entry cache to store the static groups and increase its capacity from 20 to 30 percent, as follows:

```
dsconfig set-entry-cache-prop \
          --cache-name Group\ Cache \
          --set enabled:true \
```

```
--set max-memory-percent:30 \
--hostname localhost \
--port 4444 \
--trustAll \
--bindDN cn=directory\ manager \
--bindPasswordFile <pwdFile> \
--no-prompt
```

For more details about tuning Oracle Unified Directory, see "Tuning Performance" in *Oracle Fusion Middleware Administrator's Guide for Oracle Unified Directory*.

A.3 Additional Active Directory Domains

To add additional Active Directory forests and domains, edit the Kerberos configuration file found at *installation_directory*/gateway/conf/krb5.conf. The following syntax is required. When opening the file, you will notice that the default domain was populated by the installer. Only domains for additional forests or domains that do not have transitive trust need to be added for application servers that will be accessed by Mobile Security Access Server and mobile devices.

```
[domain_realm]
 .<domain_name> = <KRB_REALM_NAME>
```

For example:

```
[domain_realm]
 .bitzermobile.dev = BITZERMOBILE.DEV
 .bitzermobile.prod = BITZERMOBILE.PROD
```

A.4 Pointing to Specific Domain Controllers

By default, after installation Mobile Security Access Server is configured to find the domain controllers for a specific domain by doing a DNS looking. The entries for each domain in the *installation_directory*/gateway/conf/krb5.conf file will look something like the following:

```
BITZERMOBILE.DEV = {
  kdc = bitzermobile.dev
  default_domain = bitzermobile.dev
}
```

It is possible to configure Mobile Security Access Server to point to specific domain controllers for a given domain, for example:

```
BITZERMOBILE.DEV = {
  kdc = dc1.bitzermobile.dev
  kdc = dc2.bitzermobile.dev
  random_fallback = true
  default_domain = bitzermobile.dev
}
```

There should be a separate kdc line for each domain controller. By default when there are multiple domain controllers configured Mobile Security Access Server will try each of them in order. It is possible to configure Mobile Security Access Server to try the individual domain controllers in random order by adding the statement random_ fallback = true to the realm configuration. For example:

```
BITZERMOBILE.DEV = {
```

```
  kdc = dc1.bitzermobile.dev
  kdc = dc2.bitzermobile.dev
  random_fallback = true
  default_domain = bitzermobile.dev
}
```

A.5 Environments with Alternate UPN Suffixes

An alternate UPN suffix occurs when the domain in the UPN after the @ symbol is different than the Windows domain where the user resides, or any other Windows domain that can refer authentication requests to the user's domain.

For environments using accounts with alternate UPN suffixes and Windows password (KINIT) it is necessary to configure Mobile Security Access Server to perform Kerberos authentication using what are known as Enterprise Accounts. To turn on support for alternate UPN suffixes, edit the Kerberos configuration file found at *installation-directory*`/gateway/conf/krb5.conf`. Add the following configuration line after the existing lines in the `libdefaults` section:

```
[libdefaults]
   enterprise = true
```

When using this flag it is important to set the `default_realm` parameter in the `libdefaults` section to point to the root domain that is below all sub-domains that contain users that need to authenticate.

A.6 Configuring Mobile Security Access Server Load Balancing

This section contains the following topics:

- Section A.6.1, "Mobile Security Access Server Load Balancing Support"
- Section A.6.2, "Configuring Active-Active Load Balancing"
- Section A.6.3, "Load Balancing Configuration Requirements"
- Section A.6.4, "Known Issue with Older F5 BIG-IP Firmware"

A.6.1 Mobile Security Access Server Load Balancing Support

The Mobile Security Access Server server supports load balancing across a cluster of multiple Mobile Security Access Servers. This clustering functionality allows multiple Mobile Security Access Servers to share authentication state such that any Mobile Security Access Server is able to verify a secure token generated by another Mobile Security Access Server (at the conclusion of the Kerberos authentication process).

A.6.2 Configuring Active-Active Load Balancing

Follow these steps to configure active-active load balancing:

1. For multiple Mobile Security Access Servers to serve the same authenticated requests they must share the same secure token PKI certificate. By default during installation the secure token PKI certificate is set to be the same as the SSL certificate. However, it is possible to configure each Mobile Security Access Server to use a different PKI certificate for the secure token function from that used for SSL. The secure token PKI certificate should have key usage enabled for both signature and encryption, but does not have any specific requirements of subject

alternative names, etc. For multiple Mobile Security Access Servers to share the same secure token PKI certificate two options are possible:

- Option 1: Provision a separate PKI certificate specifically for use as the shared secure token PKI certificate.
- Option 2: Use the existing SSL certificate from one of the Mobile Security Access Servers in the cluster as the shared secure token PKI certificate.

2. Ensure that all Mobile Security Access Servers in the cluster are able to communicate to each other at their IP addresses over SSL (port 443 by default).
3. If using PEM files, copy the certificate and key files of the chosen shared secure token PKI certificate to the `\BMAX\gateway\conf\ssl\` directory of all Mobile Security Access Servers in the cluster. If using CAPI, import the chosen shared secure token PKI certificate into the appropriate Microsoft cryptographic store of all Mobile Security Access Servers in the cluster.
4. Edit the Mobile Security Access Server `httpd.conf` file on all Mobile Security Access Servers in the cluster to update the `AuthBMAXSSLCertificateKeyFile` configuration directive to point to the key file or CAPI cryptographic store of the chosen secure token PKI certificate.
5. Restart the Mobile Security Access Server on all Mobile Security Access Servers in the cluster.

A.6.3 Load Balancing Configuration Requirements

The following requirements apply:

- Load balancing across multiple Mobile Security Access Servers requires that source or SSL session stickiness be configured on the load balancer such that all client requests during the authentication process hit the same Mobile Security Access Server instance. Following the authentication process, subsequent requests can hit any Mobile Security Access Server instance.
- The load balancer must pass through SSL connections such that the Mobile Security Access Servers terminate the SSL communication.
- All load balancing algorithms (round-robin, least busy, etc.) are supported.

A.6.4 Known Issue with Older F5 BIG-IP Firmware

There is a known issue with older F5 BIG-IP firmware that did not support newer cryptographic algorithms such as AES, resulting in SSL negotiation failures. This issue will only occur if the F5 is terminating SSL communication on behalf of a back-end HTTPS web site, and is independent of any load balancing or clustering configuration. If this issue is experienced, it is recommended to upgrade the F5 BIG-IP to the latest firmware with support for new cryptographic algorithms. A short-term workaround is to disable newer cryptographic algorithms in Mobile Security Access Server by updating the Mobile Security Access Server `httpd.conf` file with the configuration line `SSLProxyCipherSuite RC4:3DES:DES`.

A.7 Installing Mobile Security Access Server Behind a Reverse Proxy

The Mobile Security Access Server can be deployed behind a reverse proxy. In this deployment configuration, the reverse proxy terminates the original SSL connections coming from the client devices, and initiates new SSL connections to the Mobile Security Access Server.

When deployed in this manner the Mobile Security Access Server must be installed with a host name and certificate that matches the public host name that resolves to the reverse proxy.

For KINIT authentication there is no special configuration required on the Mobile Security Access Server itself. For PKINIT authentication the httpd.conf file must be edited to make client-SSL enforcement by Mobile Security Access Server optional. In the httpd.conf file, change the configuration directive `SSLVerifyClient required` to `SSLVerifyClient optional`, save the file, and restart the Mobile Security Windows service.

This section contains the following topics:

- Section A.7.1, "Example Apache httpd Reverse Proxy Configuration for KINIT"
- Section A.7.2, "Example Apache httpd Reverse Proxy Configuration for PKINIT"

A.7.1 Example Apache httpd Reverse Proxy Configuration for KINIT

```
<VirtualHost *:80>

   ProxyPreserveHost on
   ProxyPass / http://bmax.domain.com:80/

</VirtualHost>

<VirtualHost *:443>

   SSLEngine On
   SSLVerifyDepth 10
   SSLOptions +StrictRequire

   SSLCertificateFile "conf/ssl/bmax.cer"
   SSLCertificateKeyFile "conf/ssl/bmax.key"
   SSLCACertificateFile "conf/ssl/bmax-cachain.pem"

   SSLProxyEngine On
   SSLProxyVerify none
   SSLProxyCheckPeerCN off
   SSLProxyCheckPeerExpire off

   ProxyPreserveHost off
   ProxyPass / https://bmax.domain.com:443/

</VirtualHost>
```

A.7.2 Example Apache httpd Reverse Proxy Configuration for PKINIT

Since PKINIT authentication behind a reverse proxy involves moving client-SSL enforcement from the Mobile Security Access Server to the reverse proxy, it is necessary for the reverse proxy to additionally pass some custom headers to the Mobile Security Access Server providing it with information on the successful client-SSL authentication. The following is an example of an Apache `httpd` reverse proxy configuration:

```
<VirtualHost *:80>

   ProxyPreserveHost off
   ProxyPass / http://bmax.domain.com:80/

</VirtualHost>
```

```
<VirtualHost *:443>

   SSLEngine On
   SSLVerifyDepth 10
   SSLOptions +StrictRequire

   SSLCertificateFile "conf/ssl/bmax.cer"
   SSLCertificateKeyFile "conf/ssl/bmax.key"
   SSLCACertificateFile "conf/ssl/bmax-cachain.pem"

  SSLProxyEngine On
   SSLProxyVerify none
   SSLProxyCheckPeerCN off
   SSLProxyCheckPeerExpire off

   <Location /AUTHN_BMAX_PKINIT_HEIMDAL>
      SSLVerifyClient require
  RequestHeader set X-SSL-CLIENT-CERT "%{SSL_CLIENT_CERT}s"
  RequestHeader set X-SSL-CLIENT-M-SERIAL "%{SSL_CLIENT_M_SERIAL}s"
  RequestHeader set X-SSL-CLIENT-I-DN "%{SSL_CLIENT_I_DN}s"
   </Location>

   ProxyPreserveHost off
   ProxyPass / https://bmax.domain.com:443/

</VirtualHost>
```

A.8 Certificate Revocation List and Online Certificate Status Protocol

Mobile Security Access Server Certificate Revocation List (CRL) checking and Online Certificate Status Protocol (OCSP) for verifying client certificates on devices when connecting to the Mobile Security Access Server. The configuration options for this support are in the `httpd.conf` file and are:

- `SSLCARevocationFile`
- `SSLCARevocationCheck`
- `SSLOCSPDefaultResponder`
- `SSLOCSPEnable`
- `SSLOCSPOverrideResponder`
- `SSLOCSPResponderTimeout`
- `SSLOCSPResponseMaxAge`
- `SSLOCSPResponseTimeSkew`

For more information, see `http://httpd.apache.org`.

This section contains the following topics:

A.8.1 Configuration

The following settings are required for both CRL and OSCP certificate verification. These settings are configured against the primary proxy authentication section; the default is port 443.

```
SSLCARevocationFile conf/ssl/PEM-ALL.crl
```

This file should contain CRLs for all the CAs in the Mobile Security Access Server certificate chain. The certificate file is in PEM format, and the PEM files for each CA should simply be concatenated together. Also specify the type of CRL check (either leaf or chain):

```
SSLCARevocationCheck leaf
```

For OCSP support, only the following options are required:

```
SSLOCSPEnable on
SSLOCSPDefaultResponder http://ocspresp.domain.name/ocsp
```

If the certificate was issued with the OCSP extension, the address of the default responder will be included in the certificate. Typically, CA certificates are issued prior to the OCSP server's configuration, so they may not include the OCSP extension. This is why the Default Responder is required. Otherwise, any certificates that don't have the OCSP extension will be rejected, including CAs in the chain.

A.8.2 CRL Tips for the Microsoft CA

When using a Microsoft CA, the CRL files can be found in:

```
C:\Windows\System32\certsrv\CertEnroll
```

Note that these are CER files and that they must be converted to PEM for the Mobile Security Access Server to parse them. The `openssl` tool can be used to accomplish this:

```
# openssl crl -inform DER -outform PEM -in DEV-CA1.crl -out PEM-DEV-CA1.crl
# openssl crl -inform DER -outform PEM -in DEV-CA2.crl -out PEM-DEV-CA2.crl
# cat PEM-DEV-CA1.crl PEM-DEV-CA2.crl  > PEM_ALL.crl
```

All the CRLs for the entire CA chain must be present in the file. When revoking certificates using the Microsoft CA manager, be sure to publish the new CRL; otherwise, you will have to wait until the next publishing cycle. Right click on **Revoked Certificates -> All Tasks -> Publish**.

A.8.3 OCSP Tips for the Microsoft CA

The process for setting up a Windows OCSP responder is documented in the *Online Responder Installation, Configuration, and Troubleshooting Guide* on `http://technet.microsoft.com`.

You must have Windows 2008 Enterprise or Data Center edition. In addition, be sure to enable the NONCE extension for each responder configuration. The easiest way to test the OCSP responder is to use the Microsoft `certutil` utility. For example:

```
certutil -url DEV-CA2.cer
```

A.9 Administrative Console Installation on Internet Information Services

The Mobile Security Administrative Console can be installed using Internet Information Services as a web server, and can then use Active Directory groups to

leverage existing domain accounts for authentication and authorization to the Mobile Security Administrative Console console using Windows SSO. The following procedure is used to configure Internet Information Services after running the Mobile Security Access Server installation program.

This section contains the following topics:

A.9.1 Requirements

- Windows 2008 R2
- Internet Information Services 7.5 and above
- Latest service pack and security updates
- 4 GB memory
- 2.2 GHZ processor
- 30GB hard drive

A.9.2 Summary

1. Add the `webserver` role using Windows server manager with the following features:
   - Application Development
     - CGI
   - Security
     - Basic Authentication
     - Windows Authentication
   - Management Tools
     - IIS Management Scripts and Tools
     - IIS 6 Metabase Compatibility
     - IIS 6 WMI Compatibility
     - IIS 6 Scripting Tools
2. Run Mobile Security Access Server and Administrative Console installation Program.
3. Configure port 443 and Install the web server certificate at the IIS web site level.
4. Application virual directory test will fail unless Basic Settings are set to the app pool id.

A.10 Configuring Certificates for Service Accounts

This section describes how to install a certificate into the Windows certificate store (CAPI) for a particular Windows service account.

The service account must be defined in Active Directory or as a local account on the Mobile Security Access Server, as follows:

1. Open command line

2. Execute `runas` command to open a new command line window under the service account: `runas /env /user:`*`yourserviceaccount`*`@ct.com` *`cmd`*
3. Open Microsoft Management Console `mmc`.
4. Choose `Certificate snapin` and choose `MY certificate store`.
5. Import certificate or request a certificate from the store depending on your process.