Oracle Fusion Middleware

Release Notes for Oracle Mobile Security Suite

Release 3.0.1

E52134-02

March 2014

This document describes known issues for this release of Oracle Mobile Security Suite.

Oracle Fusion Middleware Release Notes for Oracle Mobile Security Suite, Release 3.0.1

E52134-02

Primary Author: Ellen Desmond

Contributing Author:

Contributors: John Boyer, Andy Smith

Contents

6 Mobile Security Container for iOS

7 Mobile Security Container for Android

8 Mobile Security App Containerization Tool for iOS

9 Mobile Security App Containerization Tool for Android

10 Secure Mobile Mail Manager for iOS

11 Secure Mobile Mail Manager for Android

Preface

Oracle Mobile Security Suite enhances employee productivity by allowing secure access to corporate applications and data from mobile devices while preserving rich user experience. Its Mobile Security Container creates the enterprise workspace on any mobile device - corporate owned or personal, and for all mobile platforms. Employees get seamless access to intranet, corporate data and applications with enterprise-grade security and deep integration with Windows Authentication for true Single Sign-On.

Audience

This document is intended for system administrators who are deploying and managing Oracle Mobile Security Suite components.

Documentation Accessibility

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

Access to Oracle Support

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

Related Documents

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

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

Conventions

The following text conventions are used in this document:

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

1 Introduction

This chapter introduces Release Notes for Oracle Mobile Security Suite, Release 3.0.1

It includes the following topics:

- Section 1.1, "Latest Release Information"
- Section 1.2, "Purpose of this Document"

1.1 Latest Release Information

This document is accurate at the time of publication. Oracle will update the release notes periodically after the software release. You can access the latest information and additions to these release notes on the Oracle Technology Network at:

http://www.oracle.com/technetwork/indexes/documentation/index.html

1.2 Purpose of this Document

This document contains the release information for Release Notes for Oracle Mobile Security Suite Release 3.0.1. Oracle recommends you review its contents before installing or working with the product.

2

Oracle Mobile Security Access Server

This chapter describes the release notes for Oracle Mobile Security Access Server.

It contains the following sections.

2.1 New Features

The following new features are included in the 3.0.0 release.

- Oracle rebranding.
- Integration with Oracle Access Manager (OAM) for username/password authentication.
- Retrieval of OAM and OAuth 2.0 tokens for single sign-on to back end resources protected with either or those token types, including:
  - OAM WebGate protected resources
  - Oracle Web Services Manager (OWSM) protected resources
  - Oracle API Gateway (OAG) protected resources
- Various security improvements, including integrating security patches for all underlying open source components.
- Support for passing GSSAPI Kerberos flags from Mobile Security Access Server configuration files.
- Merging of cookies set during multi-pass NTLM SSO negotiation exchanges.
- Support for PIN management features through Radius protocol.
- Failover across multiple Radius servers.

The following new features are included in the 3.0.1 release.

- Support for Oracle Linux 6 Update 1 and higher

2.2 System Requirements

The following system requirements are required for this release of the Mobile Security Access Server:

- Windows 2008 SP2 or Oracle Linux 6 Update 1+
- Latest service pack and security updates
- 4 GB memory
- 2.2 Gz processor
- 30GB hard drive

2.3 Compatibility

This release is compatible with the following Oracle Mobile Security Suite components.

- Mobile Security Administrative Console v3.0.x
- Mobile File Manager Server v3.0.x
- Mobile Security Notification Server v3.0.x
- Mobile Security Container v2.4.x, v2.5.x, v3.0.x
  - for iOS
  - for Android
- Mobile Security App Containerization Tool v2.5.x, v3.0.x
  - for iOS
  - for Android

2.4 Bug Fixes

The following bug fixes are included in the 3.0.0 release.

- Escape embedded commas in LDAP DNs during certificate provisioning and lifecycle operations.

2.5 Known Limitations

The following limitations are known in this release.

- For user authentication with Kerberos PKINIT (X509 certificates), Mobile Security Access Server requires that the RSA with SHA-512 algorithm be allowed for domain authentication. This is enabled by default in standard domain configurations.
- For user authentication with Kerberos username and password, Mobile Security Access Server requires that the RC4-HMAC algorithm be allowed for domain authentication. This is enabled by default in standard domain configurations.
- 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.

3 Mobile Security Administrative Console

This chapter describes the release notes for the Oracle Mobile Security Administrative Console.

It contains the following sections.

- Section 3.1, "New Features"
- Section 3.2, "System Requirements"
- Section 3.3, "Compatibility"
- Section 3.4, "Bug Fixes"
- Section 3.5, "Known Limitations"

3.1 New Features

The following new features are included in the 3.0.0 release.

- Oracle rebranding.
- Integration with Oracle Unified Directory as the authoritative repository for user and group information
- Integration with Oracle Database for data storage.
- Removal for license keys.
- Support for LDAP bind for administrative user authentication to the Administrative Console UI.
- LDAP-synchronization performance and scalability improvements, verified up to 100k users and 5k groups.
- Containerized app automatic update enhancements.
- Ability to generate time-limited passcodes (TLPs) to provision a new Container without sending an email.
- Support for LDAPS.
- Improved handling of transient LDAP connection failures.
- New policy for disabling custom redirects out of the workspace.
- Display OS version compatibility for containerized apps.
- Ability to change company logo during upgrade.
- Upgrade alerts for containerized apps.
- Enable "install on homepage" feature for containerized apps.

The following new features are included in the 3.0.1 release.

- Support for Oracle Linux 6 Update 1 and higher

3.2 System Requirements

The following system requirements are required for this release of the Mobile Security Administrative Console:

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

3.3 Compatibility

This release is compatible with the following Mobile Security Suite components.

- Mobile Security Access Server v2.5.x, v3.0.x
- Mobile Security File Manager v2.5.x, v3.0.x
- Mobile Security Notification Server v2.5.x, v3.0.x
- Mobile Security Container v2.4.x, v2.5.x, v3.0.x
  - for iOS
  - for Android
- Mobile Security App Containerization Tool v2.5.x, v3.0.x
  - for iOS
  - for Android

Upgrade is supported from Mobile Security Administrative Console v2.5.x.

3.4 Bug Fixes

The following bug fixes are included in the 3.0.0 release

- Resolved vApps deleted from the catalog remain on the workspace homepage.
- Resolved scheduled tasks not being created for some complex passwords used with service accounts.
- Resolved detailed error messages being returned for some invalid inputs in web service calls.
- Resolved some policy violation events not displaying in the container audit log.
- Resolved wrong policy being applied to containers associated with deleted users.

3.5 Known Limitations

The following limitations are known in the 3.0.0 release:

- Long invite template subject will affect email format

- Mouse over line charts with IE10 shows wrong data point
- If a container is locked due to a policy violation before a successful registration then it will remain the locked state after registration and need to be manually unlocked.
- After an authentication session timeout in the Admin Console UI the user is not automatically redirected back to the login screen.
- There is no validation of APNS certificates when they are uploaded.
- Containerized apps are not wiped or locked when they are deleted from the catalog.
- Only a single Active Directory forest is supported for LDAP sync.
- Nested groups underneath Oracle Unified Directory dynamic groups are not supported.

4

Mobile Security Notification Server

This chapter describes the release notes for Mobile Security Notification Server.

It contains the following sections.

- Section 4.1, "New Features"
- Section 4.2, "System Requirements"
- Section 4.3, "Compatibility"
- Section 4.4, "Bug Fixes"
- Section 4.5, "Known Limitations"

4.1 New Features

The following new features are included in the 3.0.0 release.

- Integration with Oracle Database for data storage.
- Encryption for all passwords stored in the database.
- Push notifications for Oracle Secure Mail Manager.

The following new features are included in the 3.0.1 release.

- Support for Oracle Linux 6 Update 1 and higher

4.2 System Requirements

The following minimum system requirements are required for this release of the Mobile Security Notification Server:

- Windows 2008 R2 or Oracle Linux 6 Update 1+
- Latest service pack and security updates
- 4 GB memory
- 2.2 GHz processor
- 30GB hard drive
- Supports Exchange 2007 and 2010

4.3 Compatibility

This release is compatible with the following Oracle Mobile Security Suite components.

- Mobile Security Administrative Console v3.0.x
- Mobile File Manager Server v2.5.x, v3.0.x
- Mobile Security Access Server v2.5.x, v3.0.x
- Mobile Security Container v2.4.x, v2.5.x, v3.0.x
  - for iOS
  - for Android
- Mobile Security App Containerization Tool v2.5.x, v3.0.x
  - for iOS
  - for Android
- Upgrade supported from Mobile Security Notification Server v2.5.x.

4.4 Bug Fixes

No bug fixes are included in the 3.0.0 and 3.0.1 releases.

4.5 Known Limitations

The following limitations are included in the 3.0.0 release.

- Push notifications may still be delivered after an app is deleted if device deregistration does not occur.

5 Mobile Security File Manager Server

This chapter describes the release notes for Mobile Security File Manager Server.

It contains the following sections.

- Section 5.1, "New Features"
- Section 5.2, "System Requirements"
- Section 5.3, "Compatibility"
- Section 5.4, "Bug Fixes"
- Section 5.5, "Known Limitations"

5.1 New Features

The following new features are included in the 3.0.0 release.

- Verified compatibility with Storage Made Easy WebDav Android app.

The following new features are included in the 3.0.1 release.

- Support for Oracle Linux 6 Update 1 and higher.

5.2 System Requirements

The following minimum system requirements are required for this release of the Mobile Security File Manager:

- Windows 2008 R2 or Oracle Linux 6 Update 1+
- Latest service pack and security updates
- 4 GB memory
- 2.2 GHz processor
- 30GB hard drive
- CIFS/SMB enabled file shares

5.3 Compatibility

This release is compatible with the following Oracle Mobile Security Suite components.

- Mobile Security Administrative Console v3.0.x
- Mobile File Access Server v2.5.x, v3.0.x

- Mobile Security Notification Server v3.0.x
- Mobile Security Container v2.4.x, v2.5.x, v3.0.x
  - for iOS
  - for Android
- Mobile Security App Containerization Tool v2.5.x, v3.0.x
  - for iOS
  - for Android

Upgrade is supported from Mobile Security File Manager v2.5.x.

5.4 Bug Fixes

No bug fixes are included in the 3.0.0 and 3.0.1 releases.

5.5 Known Limitations

The following limitations are included in the 3.0.0 release.

- Access to Kerberos or NTLM protected file shares is only available when using Active Directory authentication.

6 Mobile Security Container for iOS

This chapter describes the release notes for the Mobile Security Container for iOS.

It contains the following sections.

- Section 6.1, "New Features"
- Section 6.2, "System Requirements"
- Section 6.3, "Compatibility"
- Section 6.4, "Bug Fixes"
- Section 6.5, "Known Limitations"

6.1 New Features

The following new features are included in the 3.0.0 release.

- Oracle rebranding.
- Containerized app automatic update enhancements.
- Verified compatibility with Oracle iOS apps.
- Multi-tab browsing enhancements.
- Hide secure browser settings for auth-only policy.
- New policy for disabling custom redirects out of the workspace.
- Additional options for white-labeled version of the app.
- Upgrade alerts for containerized apps.
- Enable "install on homepage" feature for containerized apps.

6.2 System Requirements

The following system requirements are required for this release.

The minimum requirements for installing the Mobile Security App Containerization Tool for iOS are as follows:

- OSX 6.x and 7.x
- Xcode 5 on OSX v10.7 Lion or v10.8 Mountain Lion, to rebuild the app and sign it with an enterprise certificate

6.3 Compatibility

This release is compatible with the following Oracle Mobile Security Suite components.

- Mobile Security Administrative Console v3.0.x
- Mobile Security Access Server v3.0.x
- Mobile File Manager Server v3.0.x
- Mobile Security Notification Server v3.0.x
- Mobile Security App Containerization Tool for iOS v2.5.x, v3.0.x

Upgrade is supported from Mobile Security Container for iOS v2.4.x, v2.5.x.

6.4 Bug Fixes

The following bug fixes are included in the 3.0.0 release.

- Various memory leak fixes
- Resolved inconsistent crashes handling large file sizes in file manager.
- Resolved copying image URLs in secure browser.
- Resolved multiple audit events being sent on lock.
- Resolved various image download problems.
- Resolved file manager displaying root folder instead of custom user folder.
- Resolved opening Safari bookmarks launching multiple tabs in secure browsers.
- Resolved ability to automatically launch a URL saved in the clipboard in the when existing tabs open in secure browser.

6.5 Known Limitations

The following limitations are known in the 3.0.0 release:

- The integrated document editor present in previous versions of the Mobile Security Container for iOS has been removed.
- v2.5.x containerized apps will be blocked from communicating to a v3.0.x container if the new "redirects to container allowed" policy is set to "no"; the workaround is to either set this policy to "yes" or to upgrade to v3.0.0 containerized apps.
- Uploading files from secure browser to website not supported.
- Videos continue playing in the background after the secure browser is exited while the container app is still running.
- Playing videos multiple times in file manager may not work; the workaround is to exit and reenter the current folder before playing the video again.
- Some lock alert messages may display and disappear quickly, as user is logged out.
- File manager displays the error message `resource does not exist` when attempting to manually add a shared folder that was previously added.
- Renaming a file with a period in file manager will prompt to change the extension of the file.

- Browsing through folders in file manager too quickly will result in intermittent crashes.
- When using the Secure Mail Manager with Oracle Access Manager authentication, the user will need to enter their username and password when Exchange ActiveSync is not an OAM-protected resource.

7 Mobile Security Container for Android

This chapter describes the release notes for the Mobile Security Container for Android.

It contains the following sections.:

7.1 New Features

The following new features are included in the 3.0.0 release.

- Oracle rebranding.
- Containerized app automatic update enhancements.
- Verified compatibility with Oracle Android apps.
- Verified compatibility with Storage Made Easy WebDav Android app.
- Secure sharing of encrypted files between apps
- Secure clipboard copy/paste between apps.
- Android 4.4 (KitKat) support.
- New policy for disabling custom redirects out of the workspace.
- Ability to create white-labeled version of the app.
- Download progress display for container upgrades and containerized apps.
- Ability to switch between mobile view and desktop view in the secure browser.
- Upgrade alerts for containerized apps.
- Enable "install on homepage" feature for containerized apps.
- Consolidation of multiple app log files into a single file.
- Ability to automatically launch a URL saved in the clipboard in the secure browser.

7.2 System Requirements

The following system requirements are required for this release of the Mobile Security Container for Android:

- Android 4.x
- JDK 1.6 or higher, OSX v10.7 Lion or v10.8 Mountain Lion, for Mobile Security App Containerization Tool to customize the app and sign it with an enterprise certificate

7.3 Compatibility

This release is compatible with the following Oracle Mobile Security Suite components.

- Mobile Security Administrative Console v3.0.x
- Mobile Security Access Server v3.0.x
- Mobile File Manager Server v3.0.x
- Mobile Security Notification Server v3.0.x

Upgrade is supported.

7.4 Bug Fixes

The following bug fixes are included in the 3.0.0 release.

- General app stability improvements.
- Improved handling of low device memory situations.
- Improved session expiry handling.
- Resolved issue with file downloaded using secure browser not appearing the download list

7.5 Known Limitations

The following limitations are included in the 3.0.0 release.

- The integrated document viewer and editor present in previous versions of the Mobile Security Container for Android has been removed.
- Uploading files from secure browser to website not supported.
- Send logs only works for Gmail app, native Android app has bug that drops attachment.
- If the container is removed and reinstalled then the containerized apps will have to be removed and reinstalled again as well.
- Videos continue playing in the background after the secure browser is exited while the container app is still running.
- There may be a slight delay before the login screen is displayed when devices are low on memory.
- Opening a URL in the secure browser from the clipboard will cause previously opened tabs to be closed.

8 Mobile Security App Containerization Tool for iOS

This chapter describes the release notes for the Mobile Security App Containerization Tool for iOS.

It contains the following sections.

- Section 8.1, "New Features"
- Section 8.2, "System Requirements"
- Section 8.3, "Compatibility"
- Section 8.4, "Bug Fixes"
- Section 8.5, "Known Limitations"

8.1 New Features

The following new features are included in

- Oracle rebranding.
- Verified compatibility with Oracle iOS apps.
- App startup performance enhancements.
- Support for apps that do their own internal swizzling.
- Secure storage stability enhancements.
- Error checking on app signing cert.
- New policy for disabling custom redirects out of the workspace.
- Compatibility with Apple Media Player.
- Compatibility with QLPreview.
- Compatibility with HTTP Basic authentication.
- Secure user preferences.
- Workspace-level idle timeout

8.2 System Requirements

The following system requirements are required for this release of the Mobile Security App Containerization Tool for iOS:

- OSX 6.x and 7.x (for the containerized apps)

- Xcode 5 on OSX v10.7 Lion or v10.8 Mountain Lion

8.3 Compatibility

This release is compatible with the following Oracle Mobile Security Suite components.

- iOS Mobile Security Container v3.0.x
- Mobile Security Access Server v3.0.x
- Mobile File Manager Server v3.0.x
- Mobile Security Notification Server v3.0.x
- Mobile Security Containerization for iOS v3.0.x

Upgrade is supported from Mobile Security App Containerization Tool for iOS 2.5.x.

8.4 Bug Fixes

The following improvements and bug fixes are included in the 3.0.0 release.

- Various cookie-handling fixes.
- Resolved disabling location services in policy still prompts the user for location services.
- Resolved incorrect removal of existing custom URL schemes

8.5 Known Limitations

The following limitations are known in the 3.0.0 release

- Secure networking for apps directly using socket-level communication is not supported. This includes apps built with Oracle Mobile Application Framework (formerly ADF Mobile).
- Encryption of data stored in statically-linked SQLite databases is not supported

9

Mobile Security App Containerization Tool for Android

This chapter describes the release notes for the Mobile Security App Containerization Tool for Android.

It contains the following sections.

- Section 9.1, "New Features"
- Section 9.2, "System Requirements"
- Section 9.3, "Compatibility"
- Section 9.4, "Bug Fixes"
- Section 9.5, "Known Limitations"

9.1 New Features

The following new features are included in the 3.0.0 release.

- Secure networking, secure storage, and data leakage prevention controls, and policy controls for Android apps.
- Verified compatibility with Oracle Android apps.
- Verified compatibility with Storage Made Easy WebDav Android app.
- Secure sharing of encrypted files between apps.
- Secure clipboard copy/paste between apps.
- Workspace-level authentication policies, including idle timeout.

9.2 System Requirements

The following system requirements are required for this release of the Mobile Security App Containerization Tool for Android:

- Android 4.x
- JDK 1.6 or higher, OSX v10.7 Lion or v10.8 Mountain Lion, for Mobile Security App Containerization Tool to customize and sign with an enterprise certificate.

9.3 Compatibility

This release is compatible with the following Oracle Mobile Security Suite components.

- Mobile Security Administrative Console v3.0.x
- Mobile Security Access Server v3.0.x
- Mobile File Manager Server v3.0.x
- Mobile Security Notification Server v3.0.x
- Mobile Security Containerization for Android v3.0.x

Upgrade is not supported.

9.4 Bug Fixes

As this is the first release of the Mobile Security App Containerization Tool for Android there are no bug fixes included.

9.5 Known Limitations

The following limitations are included in the 3.0.0 release.

- Secure networking for apps directly using socket-level communication is not supported. This includes apps built with Oracle's Mobile Application Framework (formerly ADF Mobile).
- NDK-level function calls made directly from apps are not intercepted and secured.

10

Secure Mobile Mail Manager for iOS

This chapter describes the release notes for the Oracle Mobile Security Mail Manager for iOS.

It contains the following sections.

10.1 New Features

The following new features are included in the 3.3.5 release.

- Oracle rebranding.
- Pre-containerized version with App Containerization Tool v2.5.5 and v3.0.0.

10.2 System Requirements

The following system requirements are required for this release of the Mobile Security Container for iOS:

- iOS 6.x and 7.x.
- Xcode 5 on OSX v10.7 Lion or v10.8 Mountain Lion, to sign the app with an enterprise certificate.

10.3 Compatibility

This release is compatible with the following OMSS components.

> **Note:** Use the version pre-containerized with Oracle App Containerization Tool v2.5.5 for v2.5.x environments. Use the version pre-containerized with Oracle App Containerization Tool v3.0.0 for v3.0.x environments.

- Mobile Security Administrative Console v3.0.x.
- Mobile Security Access Server v3.0.x.

- Mobile File Manager Server v3.0.x.
- Mobile Security Notification Server v3.0.x.
- Mobile Security Container for iOS v3.0.x.

Upgrade is supported from Mobile Security Mail Manager for iOS v3.2.x and 3.3.x.

10.4 Bug Fixes

The following bug fixes are included in the 3.3.5 release.

- Resolved issue with mixing content of S/MIME messages when created from client.

10.5 Known Limitations

The following limitations are included in the 3.3.5 release.

- Out of Office setting with Exchange 2007 not supported by ActiveSync.
- Calendar create weekly recurring event and invite attendees from an iPad with Exchange 2007 shows up on next day in attendee's Calendar.
- Calendar delete single occurrence button in response to canceled meeting not working.
- Cancelled event email in Inbox prevents response to other invites. Workaround is to re-start TD app.
- On iPhone3GS auto-configuration may crash first time. Launch again and you can recover.
- Not able to access UI to format compose email body on iPhone.
- Open in TD from other apps is not working if TD is closed.
- Messages with attachments cannot be sent encrypted. The attachments will be lost. They must be downloaded and re-attached.

11

Secure Mobile Mail Manager for Android

This chapter describes the release notes for the Oracle Mobile Security Mail Manager for Android.

It contains the following sections.

- Section 11.1, "New Features"
- Section 11.2, "System Requirements"
- Section 11.3, "Compatibility"
- Section 11.4, "Bug Fixes"
- Section 11.5, "Known Limitations"

11.1 New Features

The following new features are included in the 3.3.5 release.

- Support for Android 4.4.

11.2 System Requirements

The following system requirements are required for this release of the Mobile Security Container for Android:

- Android 4.x.
- OSX v10.7 Lion or v10.8 Mountain Lion, to use Mobile Security App Containerization Tool sign with an enterprise certificate.

11.3 Compatibility

This release is compatible with the following OMSS components.

- Mobile Security Administrative Console v3.0.x.
- Mobile Security Access Server v3.0.x.
- Mobile File Manager Server v3.0.x.
- Mobile Security Notification Server v3.0.x.
- Mobile Security Container for Android v3.0.x.

Upgrade is not supported.

11.4 Bug Fixes

The following bug fixes are included in the 3.3.5 release.

- UI enhancements.
- S/MIME improvements.
- Improved syncing with Lotus servers.
- Improved performance for initial sync.

11.5 Known Limitations

The following limitations are included in the 3.3.5 release.

- To view attachments, you must open them in a separate document viewer. The integrated document viewer and editor present in previous versions of the Mobile Security Container for Android has been removed.
- When using the Secure Mail Manager with Oracle Access Manager authentication, the user must enter their username and password when Exchange ActiveSync is not an OAM-protected resource.
- If TD app is removed and re-installed, Container app must be force stopped and restarted
- After unlock, multiple logins are prompted.
- Audio and video attachments can not be played in Container.
- If Container is removed and re-installed then TD app will have to be removed and re-installed also.
- If TD app is removed and re-installed, Container app must be force stop and restart.
- Click on address does not re-direct to maps.