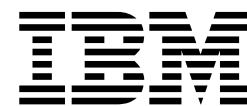


Installation Guide

Version 2 Release 4



Installation Guide

Version 2 Release 4

Note

Before using this information and the product it supports, read the information in "Notices" on page 113.

This edition applies to version 2, release 4, modification level 0 of IBM MobileFirst Protect (program number 5725-R11) and to all subsequent releases and modifications until otherwise indicated in new editions.

© **Copyright IBM Corporation 2014, 2016.**

US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Contents

Chapter 1. Overview and Supported

Devices 1

Supported Devices and Infrastructure	1
Device Management	1
Platform-Based Management	1

Chapter 2. Deployment Architecture. . . 3

Chapter 3. Support Services 7

Chapter 4. Hardware Requirements 9

VMware and Oracle Servers	9
IBM MobileFirst Protect Cloud Extender	9
Mobile Enterprise Gateway	10
Load Balancer	10

Chapter 5. Software Requirements 11

Software Licenses and Downloads	11
Certificate Requirements	12

Chapter 6. Network Requirements 15

Firewall and Proxy Settings	16
Pre-deployment Checklist.	18

Chapter 7. Part 1: Installing the Database. 21

Chapter 8. Part 2: Deploying the IBM MobileFirst Protect On-Premise Virtual Appliance 27

Chapter 9. Part 3: Configuring the IBM MobileFirst Protect On-Premise Servers 35

Chapter 10. Part 4: Customizing the Service Features 43

Customizing Your Portal	45
Connecting to Mail Service	45
Configuring SMTP (outgoing mail) Settings	45
Configuring Mail Sender Address and Display Name	46
Setting the System Alerts Email Recipient	47
Configuring File and Mobile App Storage	47
Connecting to Third-Party Applications and Services 48	
Adding an APNS Proxy Server	
Client-Authentication Certificate	48
Add an Apple MDM Profile Signing Certificate	50
Add the Microsoft Bing Maps Feature	51
Enable Android Notifications	51
Enter SMS Gateway Account Details	52
Enter Network Time Protocol (NTP) Server Details	54

Integrate with an Application Reputation Engine	55
Integrating with Android for Work	56
Setting up SNMP Monitoring	56
Setting up System Monitoring	58
Monitoring Applications Using SNMP	58
Checking Server Connectivity	59

Chapter 11. Part 5: Configuring the Instance 61

Chapter 12. Part 6: Checking Live Connectivity 63

Chapter 13. Part 7: Creating an Organization Account 65

Chapter 14. Continuing Maintenance 67

Using the Administration Console for Maintenance	67
Reconfiguring the Instance	68
Replacing Certificates	69
Backing Up and Restoring Your Service and Data	69
Learn About Data Retention	72
About Application Log Retention	73
About Database Table Retention	73
Managing Resource Allocation	74
Manage Files and Downloads	75
Downloading IBM MobileFirst Protect On-Premise Optional Installers	77
Downloading Additional IBM MobileFirst Protect On-Premise Management Tools	77
Managing Passwords	77
Applying Patches	80
Applying patches smaller than 500MB	81
Applying patches over 500MB	81

Chapter 15. Troubleshooting Problems 83

Audit Configuration Changes	83
View Application Status	84
Troubleshoot in Basic Mode	85
Download Certificates	87
Download Configuration Summary File for Support	88
Troubleshoot in Advanced Mode	89
Create a Support Code	91

Chapter 16. The Next Step	93
Chapter 17. Appendix A: VM Internal Hostnames and IP Requirements	95
Chapter 18. Appendix B: Sample DNS Entries.	97
Chapter 19. Appendix C: VM Shell Commands	99
Chapter 20. Appendix D: SSL Certificate Password Removal	105
Chapter 21. Appendix E: High Availability Environment	107
High Availability / Reverse Proxy Requirements	107

High Availability Architecture	107
Deploy the vApp in a VMware Cluster.	108
Configure Network File System (NFS) Service	110
Chapter 22. Appendix F: System Monitoring Alerts	111
Notices	113
Trademarks	115
Terms and conditions for product documentation	115

Chapter 1. Overview and Supported Devices

The IBM MobileFirst™ Protect On-Premise product deployment consists of:

- Verifying hardware, software, certificate, and network requirements.
- Installing or configuring the Oracle Database.
- Deploying the IBM MobileFirst Protect On-Premise Virtual Appliance.
- Configuring the IBM MobileFirst Protect On-Premise Servers.
- Customizing the Service Features.
- Configuring the Instance.
- Checking Live Connectivity.
- Creating an Organizational Account.
- Installing the IBM MobileFirst Protect Cloud Extender® (optional; not covered in this guide)

Supported Devices and Infrastructure

IBM MobileFirst Protect On-Premise supports most mobile devices and infrastructures.

Devices can be managed by an agent installed on the device or through platform-specific management tools, such as BlackBerry Enterprise Server, Exchange Server, and so on.

Device Management

Devices can be managed by agents installed directly on the device or through OEM APIs.

The following OS versions support agent based and OEM API management:

- iOS 5.x, 6.x, 7.x, 8.x, 9.x
- Android 2.2+ for IBM MobileFirst Protect On-Premise MDM
- Android 4.0+ for IBM MobileFirst Protect On-Premise Secure Productivity Suite (SPS)
- Windows Phone 8.0, 8.1, 10

Platform-Based Management

Devices can be managed through platform management tools using the IBM MobileFirst Protect Cloud Extender. For more information, see the IBM MobileFirst Protect Cloud Extender Installation Guide.

The IBM MobileFirst Protect Cloud Extender can be integrated with the following platforms:

- Microsoft Exchange Server 2007, 2010, 2013
- Microsoft Office 365
- BlackBerry Enterprise Server 5.0
- IBM Lotus Domino 8.5.2+

- IBM Notes Traveler 8.5.2+

Chapter 2. Deployment Architecture

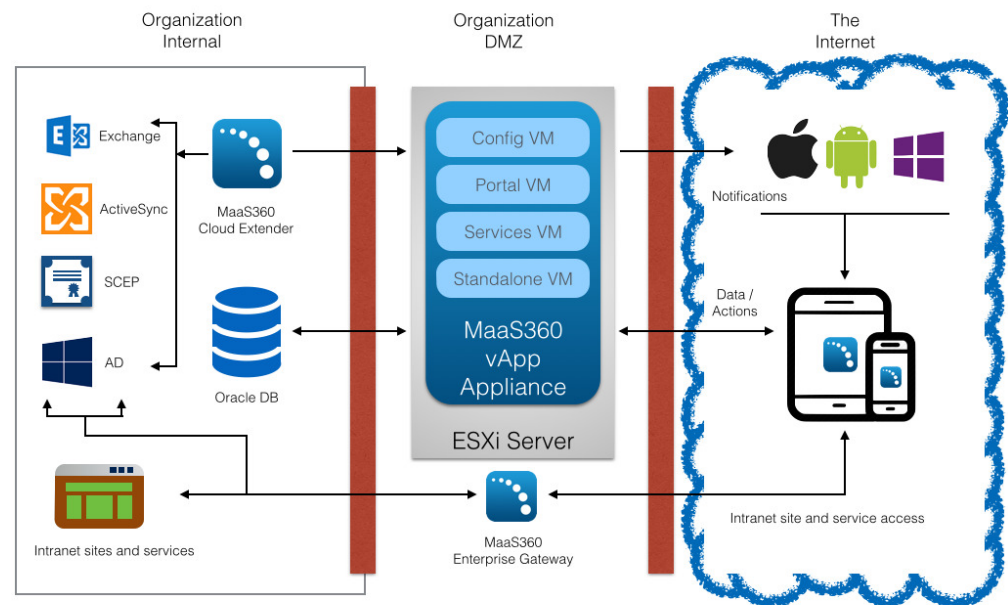
IBM MobileFirst Protect On-Premise is deployed as a set of virtual machines within a Virtual Appliance format (vApp) on the VMware ESXi Servers. The virtual machines interact with various other services hosted in the network to deliver additional features and management tools.

The virtual appliance can be deployed in the DMZ or inside the internal network (as shown below) by configuring a reverse proxy or load balancer in the DMZ to interact with the virtual appliance.

The virtual appliance must be able to communicate with the mobile devices as well as services on the internal network.

The following diagram outlines the interaction between the components:

Basic Deployment Architecture



Virtual Machines

The IBM MobileFirst Protect On-Premise vApp includes seven virtual machines (VMs). Internal hostnames for the VMs can be found in Chapter 17, "Appendix A: VM Internal Hostnames and IP Requirements," on page 95.

Configuration VM

This virtual machine is used for deployment and administration of IBM MobileFirst Protect On-Premise. It also hosts the IBM MobileFirst Protect

On-Premise Administration Console, a web-based utility for configuring and deploying IBM MobileFirst Protect On-Premise. This is referred to as the *Configuration VM* in this document. There is one Configuration VM.

Portal VM

This includes the IBM MobileFirst Protect On-Premise Portal—a console that allows administrators to manage end users' devices; End User Portal—an application to allow end users to manage their own devices; Device Enrollment—a workflow allowing end users to enroll new devices. This is referred to as the *Portal VM* in the documentation. There are two Portal VMs.

Standalone Batch Jobs VM

This virtual machine runs the different scheduled batch jobs for IBM MobileFirst Protect On-Premise. This is referred to as the *Standalone VM* in the documentation. There are two Standalone Batch Jobs VMs.

Services and CDN (Content Delivery Network) VM

This virtual machine acts as a gateway for all end user device communications and API calls. It also hosts the content repository for distributing applications and documents to different end user devices. There are two Services and CDN VMs.

When any document or application is uploaded through the IBM MobileFirst Protect On-Premise Portal, the content gets uploaded onto the content repository. Devices are notified to pull the content from a specified services tier. This VM is referred to as the Services VM.

Databases

IBM MobileFirst Protect On-Premise creates four databases on your Oracle database server.

VPN2

This is the real-time transactional database that hosts device data and data for most portal workflows.

AGILINK

This database is the primary point of entry for new account information.

EDW

This is a vast data warehouse for supporting reports. Data from the VPN2 database is periodically loaded into the EDW.

P03

This database is used for log processing.

IBM MobileFirst Protect Cloud Extender

The IBM MobileFirst Protect Cloud Extender connects IBM MobileFirst Protect On-Premise to various enterprise systems such as:

- Active Directory servers
- SCEP servers
- BES servers
- Exchange ActiveSync
- and Lotus Traveler.

It is a Windows application that is installed on a separate Windows Server or Windows Virtual Server. This application must be downloaded and installed after the IBM MobileFirst Protect On-Premise virtual appliance deployment is complete.

IBM MobileFirst Protect Mobile Enterprise Gateway

The IBM MobileFirst Protect Mobile Enterprise Gateway is an optional component that allows organizations to provide secure access to behind-the-firewall resources such as SharePoint, Windows File Share content, and Intranet sites on Mobile devices without a VPN connection. It has to be installed on a separate Windows Server or Windows Virtual Server within the DMZ.

Chapter 3. Support Services

Other network services support the functions of IBM MobileFirst Protect On-Premise. They aren't provided by the vApp Appliance but need to be running to get full use from all of its features.

SMTP Service

An SMTP email server is required to send email to administrators and users.

Ensure that the SMTP email server is within your firewall and that the port selected during installation is open. The default port is typically port 25.

Network File System (NFS) Service

An NFS server can be used for Content Data Network (CDN) storage. This is a mandatory requirement for native high availability deployment. See Appendix E to set up NFS for high availability deployment.

Reverse Proxy Service

IBM MobileFirst Protect On-Premise has to be integrated with an external reverse proxy server for reverse proxy deployment mode.

For more details, see Appendix E .

Chapter 4. Hardware Requirements

A number of hardware components are required based on your anticipated device enrollment and deployment architecture.

The primary hardware components are a VMware ESXi Server where a vApp is deployed, and an Oracle Database Server.

VMware and Oracle Servers

There are recommended specifications for a non-native high availability deployment, based on the number of managed devices.

Important: For high availability deployment the specifications mentioned below have to be doubled.

The following table describes the recommended specifications.

Table 1. Recommended Specifications

Managed Devices	Oracle Database Server Storage in GB	Oracle Database Server Memory in GB	Oracle Database Server CPU Cores	ESXi Server Storage in GB	ESXi Server Memory in GB	CPU Cores
2000	150	8	1	400	44	8
5000	150	8	2	400	44	8
10000	200	16	4	400	44	8
25000	200	24	4	400	48	8
50000	350	48	8	500	56	10
100000	500	96	8	700	64	12
200000	700	144	10	1000	80	16
400000	1000	256	12	1500	112	16
500000	1000	304	12	1500	128	20

Note: The storage space that is specified for the database server is required for IBM MobileFirst Protect On-Premise data and memory only. Extra storage and memory must be available for the OS, Oracle, and to backup data.

IBM MobileFirst Protect Cloud Extender

The IBM MobileFirst Protect Cloud Extender is an optional component in your deployment architecture.

Cloud Extender requirements vary based on the size of your deployment. The minimum specifications for the Cloud Extender are:

- Physical or virtual machine
- Windows Server 2008, 2008 R2, 2012, or 2012 RC2
- Pentium III, 500 MHz

- 1 GB RAM
- 2 GB Storage

For more information about the IBM MobileFirst Protect Cloud Extender, see the IBM MobileFirst Protect Cloud Extender Installation Guide.

Mobile Enterprise Gateway

The IBM MobileFirst Protect Mobile Enterprise Gateway is an optional component in your deployment architecture. You deploy it when you want to give devices web access to your intranet sites.

Mobile Enterprise Gateway requirements vary based on the size of your deployment. The minimum specifications for the Mobile Enterprise Gateway are:

- Physical or virtual machine
- Windows Server 2008, 2008 R2, 2012, or 2012 RC2
- Dual core CPU
- 4 GB RAM
- 2 GB Storage

For more information about the IBM MobileFirst Protect Mobile Enterprise Gateway, see the IBM MobileFirst Protect Mobile Enterprise Gateway 2.0 Quick Start Guide.

Load Balancer

This is mandatory for native high availability deployment.

IBM MobileFirst Protect On-Premise supports integration with either hardware or software load balancers for native high availability deployment.

Chapter 5. Software Requirements

IBM MobileFirst Protect On-Premise requires a series of software components including software licenses, certificates, and network settings. You should obtain or configure these elements before installation.

Software Licenses and Downloads

The following software licenses and components are required for installation.

Database

Oracle Standard Edition Two, or Oracle Enterprise edition 12.1.0.2 (64 bit).

An Oracle supported OS for the database server (see Oracle Support Statement).

Oracle Database Configuration Assistant (DBCA).

Virtual Machine

VMware software for your ESXi Server:

ESXi 5.x, 6.x

vCenter Server 5.x, 6.x

vSphere Client 5.x, 6.x

Distributed Resource Scheduler (DRS)

VMware vSphere Client to connect to your ESXi deployment from a Windows computer.

Administration

Remote Connection Tools to connect to hosts and the Oracle database.

Chrome, Firefox, or Internet Explorer Browser version 11 or later.

IBM MobileFirst Protect On-Premise services and features

IBM MobileFirst Protect On-Premise Virtual Application package (.ova).

IBM MobileFirst Protect On-Premise Database Artifact package for Oracle 12.1.0.2

Android device management (optional)

Google Cloud Messaging (GCM) API key

Android for Work account with an Enterprise Service Account (ESA) certificate.

iOS device management (optional)

Apple ID for your organization.

Apple Device Enrollment Program (DEP) account.

Third party service integration (optional)

Microsoft Bing Maps key for device tracking.

SMS Gateway account from Tropo, Clickatell, or other providers (supported through SMPP 3.4 protocol).

Veracode account for Application Reputation ratings.

Certificate Requirements

Several certificates are required for secure communication between infrastructure components.

To ensure a quick installation process, you are recommended to acquire these certificates before beginning installation.

Table 2. Certificates

Certificate	Description
Symantec Windows Phone Code Signing Certificate	To enroll Windows Phone 8+ devices, the MaaS360® for Windows Phone agent must be signed by your Windows Phone Code Signing certificate. For more information, see the IBM MobileFirst Protect On-Premise Configuration Guide. This certificate is required to manage Windows Phone devices only.
Apple Push Notification Service (APNS)	To manage iOS devices that have the App Store agents, you need a Client Authentication Certificate from IBM Support. For more information about configuring APNS, see “Connecting to Third-Party Applications and Services” on page 48.

Table 2. Certificates (continued)

Certificate	Description
SSL Certificates	<p>One or more SSL certificates, signed by a trusted certificate authority (CA), are required for IBM MobileFirst Protect On-Premise DNS URLs.</p> <p>If you are using an external load balancer or reverse proxy then ensure you use only trusted SSL certificates for them.</p> <p>SSL certificate private keys are normally protected by a password.</p> <p>This password must be removed from the private key. For more information, see Chapter 20, "Appendix D: SSL Certificate Password Removal," on page 105.</p> <p>SSL certificate should have wildcard domain URL or an exact DNS URL per SSL certificate. Using multiple Subject Alternative Names in one SSL certificate or EV certs is not supported.</p> <p>Note: You can also use self-signed certificates or SSL certificates issued by an internal CA. For more information, see IBM MobileFirst Protect On-Premise Configuration Guide.</p>

Make the key size 2048 bit or more for the SSL certificate.

Chapter 6. Network Requirements

Check your network configuration before beginning the installation to make sure that the following requirements are met:

Table 3. Network Requirements

Item	Description
Internal IP Addresses (7)	<p>The IBM MobileFirst Protect On-Premise vApp requires seven internal IP addresses from the same subnet for the virtual machines.</p> <p>It also requires IP addresses for the DNS servers, subnet mask and default gateway.</p> <p>For more information, see Chapter 17, "Appendix A: VM Internal Hostnames and IP Requirements," on page 95.</p>
External IP Addresses (1-4)	<p>One external IP address and up to four external IP addresses at the external load balancer for native high availability deployment.</p> <p>One external IP address and up to two external IP addresses at the external reverse proxy for reverse proxy deployment.</p> <p>For non-native high availability deployment, a set of two external IP addresses for the Portal VM and the Services VMs. One external IP can be used for the Portal, End User Portal and Enrollment DNS. The Services DNS requires a dedicated external IP.</p>

Table 3. Network Requirements (continued)

Item	Description
DNS Entries	<p>Make the following DNS entries for virtual hosts and map them to the IP addresses reserved for respective URLs:</p> <p>Device Services</p> <p>End User Portal</p> <p>Enrollments</p> <p>Admin Portal</p> <p>Gateway Service—required if you use IBM MobileFirst Protect Mobile Enterprise Gateway</p> <p>Administration Console—you can configure a FQDN for IBM MobileFirst Protect On-Premise Administration Console on internal DNS server to avoid accessing the console via IP address.</p> <p>It is recommended that the DNS entries be in the same domain.</p> <p>This allows a single wildcard SSL cert to be used. For example DNS entries, see Chapter 18, “Appendix B: Sample DNS Entries,” on page 97.</p> <p>Based on native high availability, reverse proxy or non-native high availability deployment, the DNS entries should be made suitably.</p> <p>Note: Ensure the External URLs are accessible from IBM MobileFirst Protect On-Premise virtual appliance.</p>
Network Ports and Firewall	<p>Make sure all network ports are configured on your external and internal firewall. For more information, see “Firewall and Proxy Settings” on page 18.</p> <p>Content filter firewall rules for media content must be enabled for accessing the Apple VPP URL at https://vpp.itunes.apple.com/WebObjects/MZFinance.woa/wa/VPPServiceConfigSrv.</p> <p>Note: The firewall must not be configured with a timeout, especially for idle database connections.</p>

Firewall and Proxy Settings

Firewall Port Settings

Some ports must be opened on your firewalls to allow IBM MobileFirst Protect On-Premise to communicate with necessary resources.

From	To	Port (TCP)	Description
IBM MobileFirst Protect On-Premise virtual appliance	Oracle DB	1521 (or as configured)	Device, account, and reporting storage
IBM MobileFirst Protect On-Premise virtual appliance	DNS	53, 123	Name resolution
IBM MobileFirst Protect On-Premise virtual appliance	SMTP	25	Outgoing mail notifications
IBM MobileFirst Protect On-Premise virtual appliance	http://www.apple.com/DTDs/PropertyList-1.0.dtd	80	Mobile Enterprise Gateway uses the DTD to parse persona policy XML
IBM MobileFirst Protect On-Premise virtual appliance	MaaS360 APNS Proxy (apns.maas360.com)	2195	iOS device notifications proxy for Apple App Store MaaS360 apps
IBM MobileFirst Protect On-Premise virtual appliance	Apple Notification Service (at various IPs in the 17.0.0.0/8 range)	2195, 2196	iOS device notifications (for all other iOS apps)
IBM MobileFirst Protect On-Premise virtual appliance	Google Cloud Message Server	5228, 5229, 5230	Android device notifications
IBM MobileFirst Protect On-Premise virtual appliance	Microsoft Notification Server	80, 443	Windows Phone device notifications
IBM MobileFirst Protect On-Premise virtual appliance	Apple App store	443	App store interactions
IBM MobileFirst Protect On-Premise virtual appliance	Google Play Store	443	App store interactions
IBM MobileFirst Protect On-Premise virtual appliance	Windows App Store	443	App store interactions
IBM MobileFirst Protect On-Premise virtual appliance	SMS Gateway	2775 (or as configured)	Custom SMS Gateway interactions
IBM MobileFirst Protect On-Premise virtual appliance	NFS Server	2049 (or as configured)	NFS server interactions
IBM MobileFirst Protect On-Premise virtual appliance	NTP Server	UDP 123 (or as configured)	NTP server time synchronization
SNMP Clients	IBM MobileFirst Protect On-Premise virtual appliance	161	SNMP client interaction with the virtual appliance
Cloud Extender	IBM MobileFirst Protect On-Premise virtual appliance	443	Push account and management data to IBM MaS360 vApp

From	To	Port (TCP)	Description
Cloud Extender	Internal services	varies	Query internal services for directory and account data
Mobile Enterprise Gateway	Internal services	varies	Pass device traffic to internal network
Mobile Enterprise Gateway	Devices	443	Pass internal service traffic to devices
Devices	Mobile Enterprise Gateway	443	Send device traffic to internal network
Devices	IBM MobileFirst Protect On-Premise virtual appliance	443	Report device data to vAppliance
Administrator console	IBM MobileFirst Protect On-Premise virtual appliance	8443	Control the vAppliance

Forward Proxy Whitelist

In your forward proxy, create a whitelist for the traffic from the IBM MobileFirst Protect VMs to the following URLs:

Company	Push Notification	App Stores
IBM MobileFirst Protect On-Premise iOS APNS Forward Proxy	https://apns.maas360.com:2195	
Apple	https://gateway.push.apple.com:2195	https://itunes.apple.com/search
Google	https://android.googleapis.com/gcm/send	https://play.google.com/store
Microsoft	http://*.notify.live.net/ and http://*.notify.windows.com/	https://www.windowsphone.com and https://www.microsoft.com

Important: You have to whitelist the above URLs in the forward proxy server for proper functioning of IBM MobileFirst Protect.

Pre-deployment Checklist

Use the following list of steps and finish all of the tasks before you start the installation of IBM MobileFirst Protect On-Premise.

Task	Status
Database server is set up and root access credentials to database server are available.	
Database server time zone is set to GMT.	
No idle timeout exists between IBM MobileFirst Protect On-Premise VMs and the database server listener port.	

Task	Status
Database is running in archive mode for the RMAN backup.	
VMware server is set up with the ESXi vCenter Server and it is accessible from the vSphere client.	
Remote connectivity tools for the VMware host and database server are available.	
DNS entries for URLs are created. These include Services, End User Portal, Enrollment URL, Portal URL, Gateway URL, and Database virtual machine hosts.	
Network ports on the external firewall are configured and opened, as per the list in the Firewall Ports section. Proxy whitelists are configured for device access, as well.	
<p>SSL Certificates for Services, End User Portal, Portal, and Enrollment URLs are available.</p> <p>An iOS signing certificate must also be available if you are using reverse proxy with http deployment.</p>	
Password from SSL Certificate private keys is removed.	
SMTP Server is set up and the hostname and port details are available.	
NFS Server is set up and it is accessible from the Services and Standalone VMs.	
Started the process of obtaining required certificates.	
IBM MobileFirst Protect On-Premise Virtual appliance package (.OVA), and the Database Artifact package for Oracle is downloaded from PPA.	
Optional: Symantec Windows Phone Code Signing Certificate is procured. It is required if you want to manage Windows Phone devices.	

Chapter 7. Part 1: Installing the Database

The first component of your IBM MobileFirst Protect On-Premise deployment that must be installed is your database infrastructure.

Step 1: Preparing the database server

Before proceeding, configure an Oracle Database Server running version 12.1.0.2 and prepare it to create new databases.

Procedure

1. Download the database artifacts file from IBM Passport Advantage.
The database artifacts are Oracle database templates, created using Oracle's Database Configuration Assistance (DBCA). DBCA is required to import the templates and create new databases on your server.

Note: The database artifact includes installation scripts for Linux and AIX platforms only. If you intend to use any other platform, review the scripts and rewrite them for the platform you have chosen.
2. Set the database server time to GMT.
3. Set no idle time out configuration on the firewall between the IBM MobileFirst Protect On-Premise VMs and the database server.
4. Number of database connections from the IBM MobileFirst Protect On-Premise VMs to the database server should be unbounded.
5. Continue to deploy the database template.

Database Default Parameters

The database templates have default values associated with them.

Some of the database template default values can be overridden to suit your deployment, if necessary. Others must not be overridden.

Any parameters that are not listed below are set at Oracle default values. These values can be changed at your discretion.

The following database parameters **must not** be overridden:

SID

Character Set

Database Name

The following database parameters can be overridden, if necessary:

Archive log mode - Enable this parameter to allow database backup.

Storage Type

Storage Location

Data Directory

Faster Recovery Area (FRA) size and directory - If you choose to override the FRA size, ensure that the value is greater than the default.

Sys and System User passwords

PGA size

SGA size components:

Shared pool

Buffer cache

Java™ pool

Large pool

If you choose to override any of these memory parameters, ensure that the value is greater than the default:

Number of processes - If you choose to override this parameter, ensure the value is greater than the default.

Connection mode - **Dedicated** mode is recommended for best performance.

Note: Enable Archive Log Mode for all four databases so that you can use RMAN.

Step 2: Deploying the Database Template

With an Oracle environment set up, the IBM MobileFirst Protect On-Premise database template must be deployed to create four databases.

About this task

To deploy the IBM MobileFirst Protect On-Premise database artifacts, perform the following steps:

Procedure

1. As the root user, check and update the following Oracle parameters at the OS level so they are at least at the values below:

Table 4. Oracle parameters

Parameter	Value
Maximum Open File Descriptors for user	Minimum: 65536
Maximum Processes Available for user	Minimum: 65536
Maximum Total Shared Memory (SHMMAX)	Minimum: 6442450944
Shared Memory Pages (SHMALL)	Minimum: 2097152

Database system parameters, like PGA and SGA, in the database templates have been tuned for 5000 devices by default.

To use your own device number, multiply the base SGA and PGA configuration by the factor of the increase in the physical database memory.

Refer to VMware and Oracle Servers section for physical database memory value based on number of devices.

Base PGA and SGA values (in MB) set in the templates are as follows:

Table 5. PGA and SGA values

Database	pga_aggregate_target	sga_target / sga_max_size
AGLINK	100 M	1229 M
EDW	400 M	1229 M
P03	100 M	1229 M
VPN2	800 M	4000 M

Note: Perform the following steps as the system user that manages the Oracle database (typically the Oracle user).

2. Copy the IBM MobileFirst Protect On-Premise Database Artifact package file that was obtained from Passport Advantage to the database server and extract the file.
3. Copy the following database template files from *base folder/12.1.0.2/* to the *assistants/dbca/templates* directory under *ORACLE_HOME*:
 - agilink_clone.ctl
 - agilink_clone.dbc
 - agilink_clone.dfb
 - edw_clone.ctl
 - edw_clone.dbc
 - edw_clone.dfb
 - p03_clone.ctl
 - p03_clone.dbc
 - p03_clone.dfb
 - vpn2_clone.ctl
 - vpn2_clone.dbc
 - vpn2_clone.dfb
4. Using DBCA, import the following templates. You can override the default values in the templates according to your environment in accordance with the rules described in “Database Default Parameters” on page 21.
 - agilink_clone
 - edw_clone
 - p03_clone
 - vpn2_clone
5. Edit the *db_update.ini* file in the extracted folder, and update the following parameters to values that fit the availability in your environment. Do not change the values of any other parameters.
 - ORACLE_HOME
 - ORACLE_VAL_VERSION=12.1.0.2
 - DB_DOMAIN
 - APP_PASS – Change this only if you intend to change the default password for all DB users to a password of your choice.

- DB_SYSTEM_PASS – Should be configured with **SYS** user password. SYS user password should be configured to be the same across VPN2, AGILINK, P03 and EDW databases.
6. If the database management user is not the oracle user, you must edit the `update_m360_databases.sh` file in the extracted folder. Replace all references to `zoracle` to `zzdatabase_management_user`.
 7. If Oracle RAC is used, modify the file `update_m360_databases.sh`:
 - a. Update the following lines:


```
export ORACLE_SID=$AGILINK_SID: replace $AGILINK_SID with the correct Agilink
database SID for the Oracle RAC node.
export ORACLE_SID=$VPN2_SID: replace $VPN2_SID with the correct VPN2 database SID for
the Oracle RAC node.
export ORACLE_SID=$EDW_SID: replace $EDW_SID with the correct EDW database SID for
the Oracle RAC node.
export ORACLE_SID=$P03_SID: replace $P03_SID with the correct P03 database SID for
the Oracle RAC node.
```
 - b. Modify the following line to include a storage clause as required by your environment. The following line occurs four times in `update_m360_databases.sh`; update each occurrence:

Example command:

```
alter tablespace TEMP add datafile 'storage_location\Temp02.dbf' size 100M
autoextend on maxsize 4000M;
```
 8. Create or edit `network/admin/tnsnames.ora` under `ORACLE_HOME`, and add or edit the following TNS names. Replace the bracketed values in each line with the correct values.


```
agilink=(DESCRIPTION=(ADDRESS_LIST=(ADDRESS=(HOST=ip_address_or_hostname)(PORT=listener_port)(PROTOCOL=TCP))(ADDRESS=(HOST=ip_address_or_hostname)(PORT=listener_port)(PROTOCOL=TCP)))(CONNECT_DATA=(SID=agilink_sid)(SERVER=DEDICATED)))
vpn2=(DESCRIPTION=(ADDRESS_LIST=(ADDRESS=(HOST=ip_address_or_hostname)(PORT=listener_port)(PROTOCOL=TCP))(ADDRESS=(HOST=ip_address_or_hostname)(PORT=listener_port)(PROTOCOL=TCP)))(CONNECT_DATA=(SID=vpn2_sid)(SERVER=DEDICATED)))
p03=(DESCRIPTION=(ADDRESS_LIST=(ADDRESS=(HOST=ip_address_or_hostname)(PORT=listener_port)(PROTOCOL=TCP))(ADDRESS=(HOST=ip_address_or_hostname)(PORT=listener_port)(PROTOCOL=TCP)))(CONNECT_DATA=(SID=p03_sid)(SERVER=DEDICATED)))
edw=(DESCRIPTION=(ADDRESS_LIST=(ADDRESS=(HOST=ip_address_or_hostname)(PORT=listener_port)(PROTOCOL=TCP))(ADDRESS=(HOST=ip_address_or_hostname)(PORT=listener_port)(PROTOCOL=TCP)))(CONNECT_DATA=(SID=edw_sid)(SERVER=DEDICATED)))
NODE_LISTENER=(DESCRIPTION=(ADDRESS=(HOST=ip_address_or_hostname)(PORT=listener_port)(PROTOCOL=TCP)))
REMOTE_LISTENER=(DESCRIPTION=(ADDRESS_LIST=(ADDRESS=(HOST=ip_address_or_hostname)(PORT=listener_port)(PROTOCOL=TCP))(ADDRESS=(HOST=ip_address_or_hostname)(PORT=listener_port)(PROTOCOL=TCP))))
```
 9. Create or edit `network/admin/listener.ora` under `ORACLE_HOME` and add or edit the following line:


```
LISTENER=(DESCRIPTION=(ADDRESS=(HOST=i/p address / hostname)(PORT=listener_port)(PROTOCOL=TCP)))
```
 10. Stop the Oracle database and listener if they are already running and restart the database only.
 11. Execute `update_m360_databases.sh`, to perform post installation updates to the databases. If any errors are reported, they have to be corrected before you proceed further.

12. Restart the Oracle database listener.
13. Execute `validate_database_setup.sh`, to perform a validation of the database installation and configuration.
If any errors are reported, they have to be corrected before you proceed further.

What to do next

Note: Do not proceed with the Instance Configuration through the IBM MobileFirst Protect On-Premise Administration Console unless all errors reported by the validation script have been resolved.

Chapter 8. Part 2: Deploying the IBM MobileFirst Protect On-Premise Virtual Appliance

IBM MobileFirst Protect On-Premise is deployed as a VMware Virtual Appliance, or vApp, on an ESXi server or ESXi cluster. The vApp contains several virtual machines that constitute the bulk of your IBM MobileFirst Protect On-Premise deployment.

Step 1: Creating a Resource Pool

About this task

A VMware resource pool is a pre-requisite for the successful deployment of the vApp in a VMware Cluster. You can use an existing resource pool or deploy one from the VMware vSphere client.

To deploy a resource pool, perform the following steps from the vSphere client, which must be connected to your VMware Virtual Center:

Procedure

1. Navigate to the ESXi host designated for your IBM MobileFirst Protect On-Premise vApp deployment using the VMware vSphere client.
2. Right-click and select **New Resource Pool** from the drop-down menu. The **Create Resource Pool** window opens.
3. Enter a name for the Resource Pool, and enter values appropriate for your VMware environment.

Step 2: Deploying the vApp

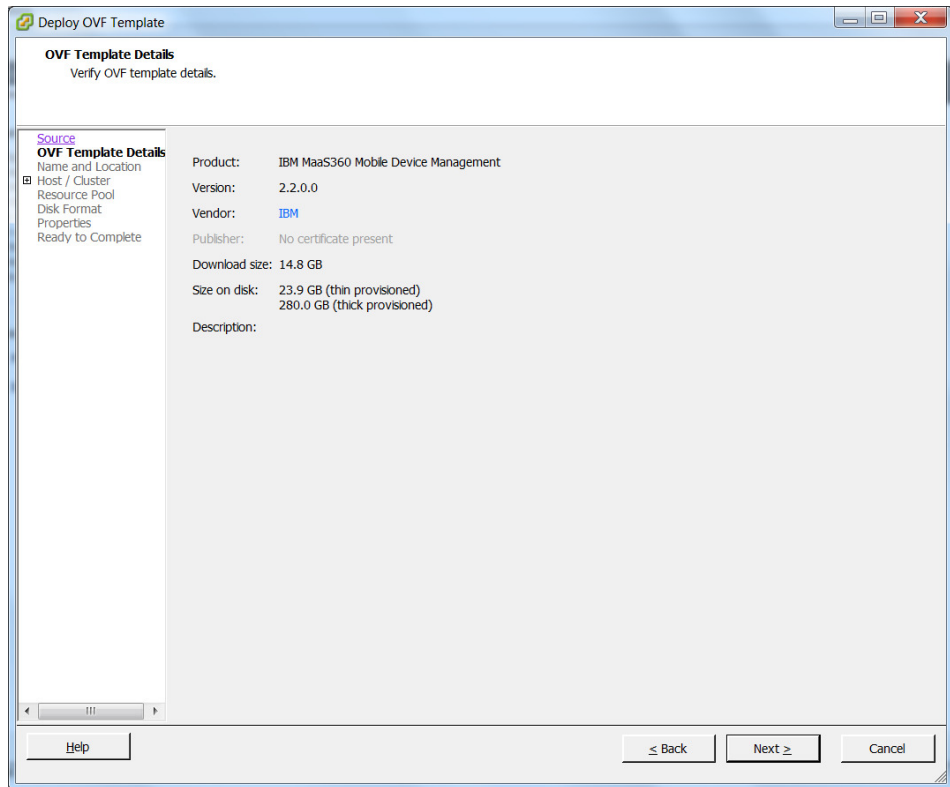
After creating a resource pool, the vApp must be imported and configured.

About this task

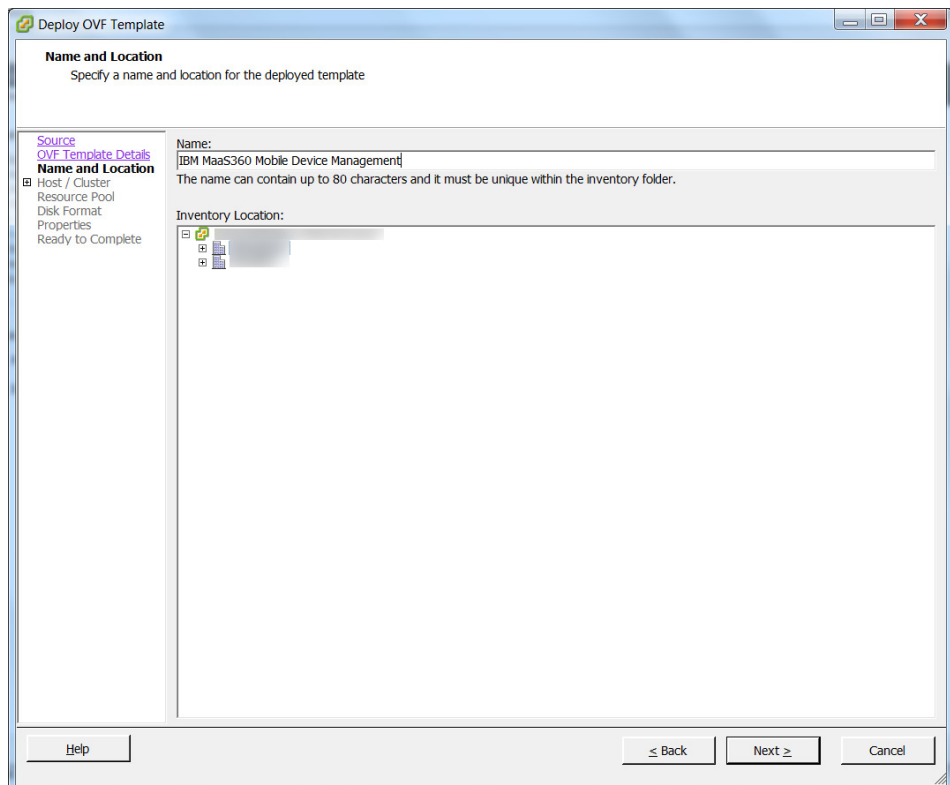
From the vSphere Client, connect to your VMware Virtual Center and perform the following steps:

Procedure

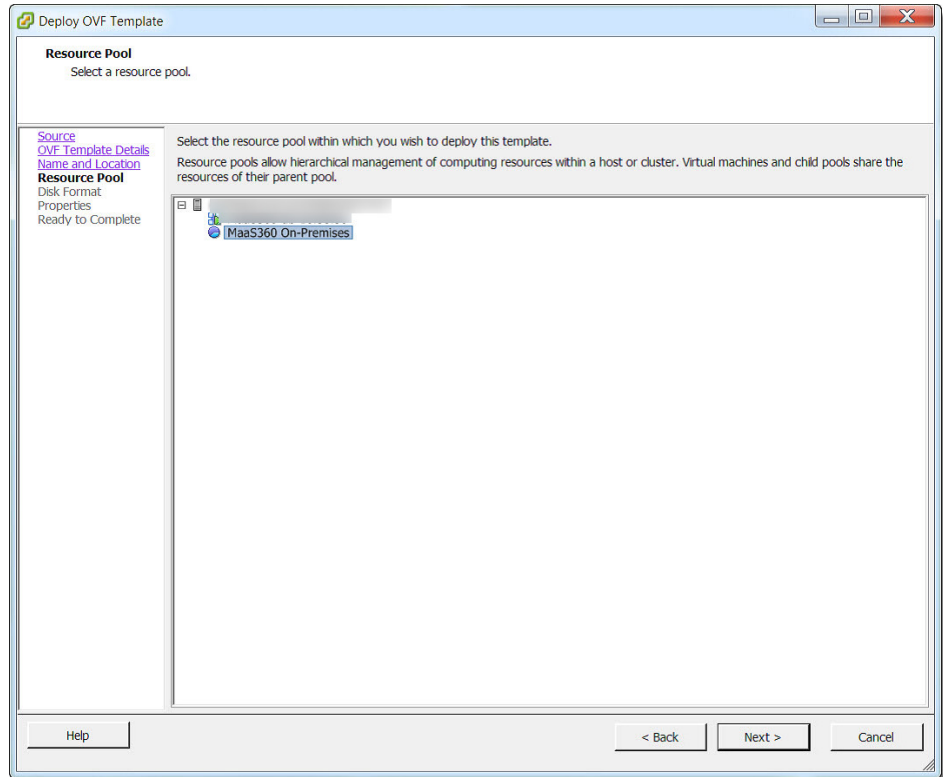
1. Select the relevant resource pool on the left navigation panel where you import the IBM MobileFirst Protect On-Premise vApp.
2. From the **File** menu, click **Deploy OVF Template**.
The **Deploy OVF Template** screen opens.
3. Click **Browse** and navigate to the location of the OVA file.
4. Select the OVA file and click **Next** to view the **OVF Template Details** window.



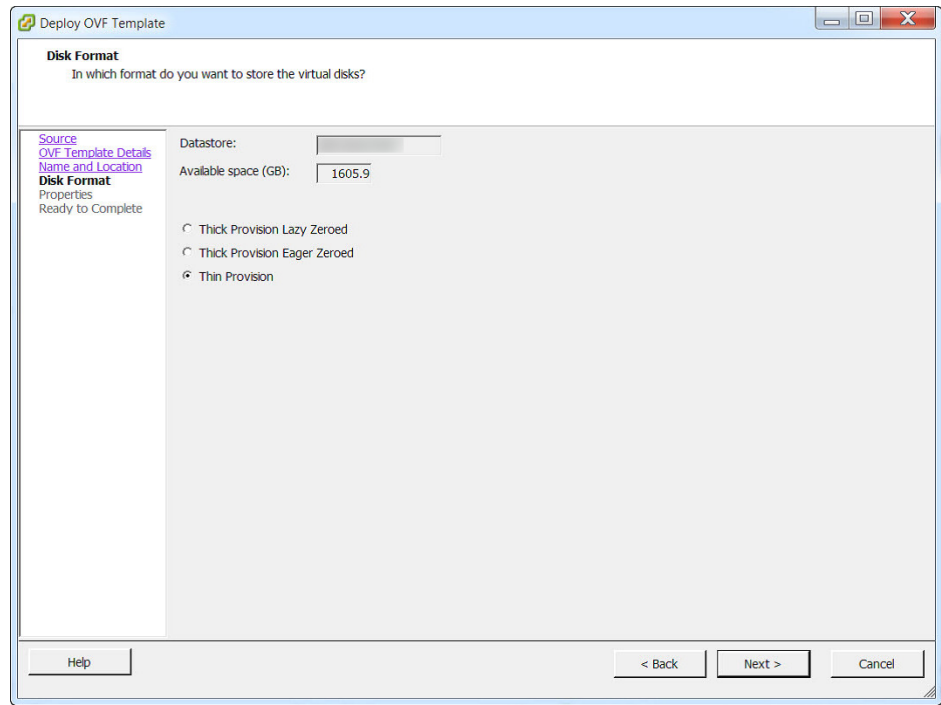
5. Click **Next** to display the **Name and Location** screen. Edit the name of the vApp, if desired.
6. Select the appropriate inventory location and click **Next**.



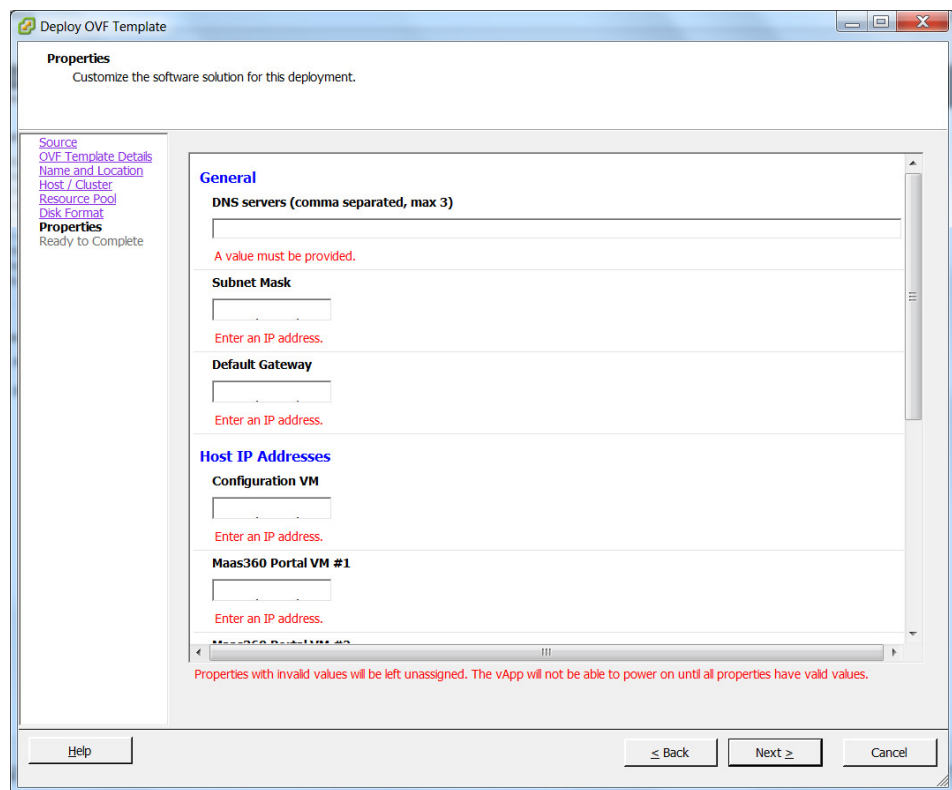
7. If you did not select the newly created resource pool when deploying the template, designate a resource pool. Click **Next** to proceed or skip this step.



8. If only one storage resource is configured, skip this step. If multiple storage resources are available, select the storage resource for hosting the virtual appliance using the **Storage** screen.
If you are configuring your deployment for High Availability, select **shared storage**.
Click **Next** to proceed.
9. Choose the provisioning type and data store details on the **Disk Format**.
For better capacity planning use **Thick Provision**.
Click **Next** to proceed.



10. On the **Properties** screen, enter the IP addresses for the DNS servers, Subnet mask, and default gateway for the network where the vApp is deployed.



11. Under the **Host IP Addresses** heading on the same screen, enter the internal IP addresses reserved for the seven virtual machines.
 - IBM MobileFirst Protect On-Premise Configuration VM
 - IBM MobileFirst Protect On-Premise Portal VM #1—node 1 of the Portal VM

- IBM MobileFirst Protect On-Premise Portal VM #2—node 2 of the Portal VM
- IBM MobileFirst Protect On-Premise Services and CDN VM #1—node 1 of the Services VM
- IBM MobileFirst Protect On-Premise Services and CDN VM #2—node 2 of the Services VM
- IBM MobileFirst Protect On-Premise Standalone Batch Jobs VM #1—node 1 of the Standalone Batch Jobs VM
- IBM MobileFirst Protect On-Premise Standalone Batch Jobs VM #2—node 2 of the Standalone Batch Jobs VM

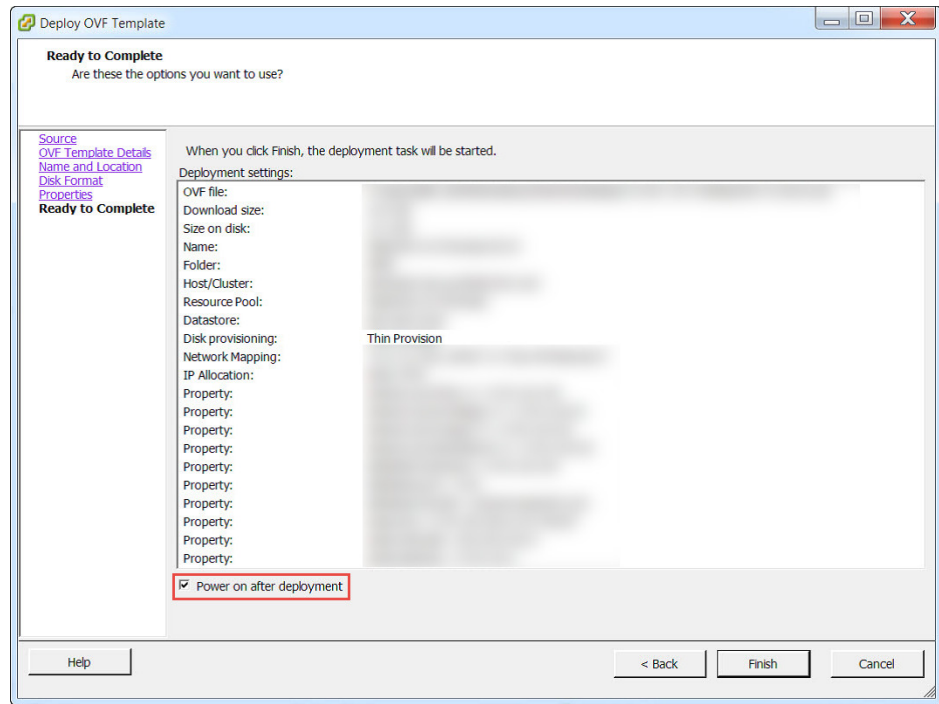
Note: All seven IP addresses must be valid to deploy the vApp in native High Availability mode

To deploy it in non-native High Availability mode, enter valid IP addresses for the following:

- IBM MobileFirst Protect On-Premise Configuration VM
- IBM MobileFirst Protect On-Premise Portal VM #1
- IBM MobileFirst Protect On-Premise Services and CDN VM #1
- IBM MobileFirst Protect On-Premise Standalone Batch Jobs VM #1

You could enter 255.255.255.255 for the IP addresses of the IBM MobileFirst Protect On-Premise Portal VM #2, IBM MobileFirst Protect On-Premise Services and CDN VM #2 and IBM MobileFirst Protect On-Premise Standalone Batch Jobs VM #2. These Node 2 VMs aren't used in non-native High Availability mode.

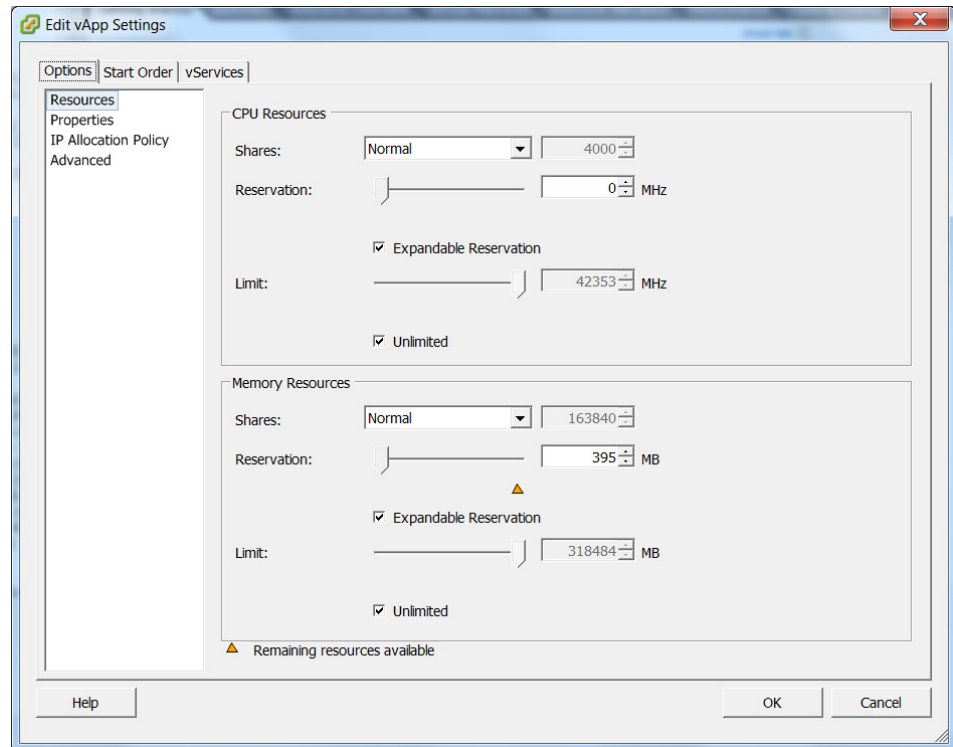
12. Click **Next** to view the **Ready to Complete** screen.
13. Confirm all of the deployment settings before the vApp import starts.
If necessary, click **Back** to return to the previous screen to change any settings.



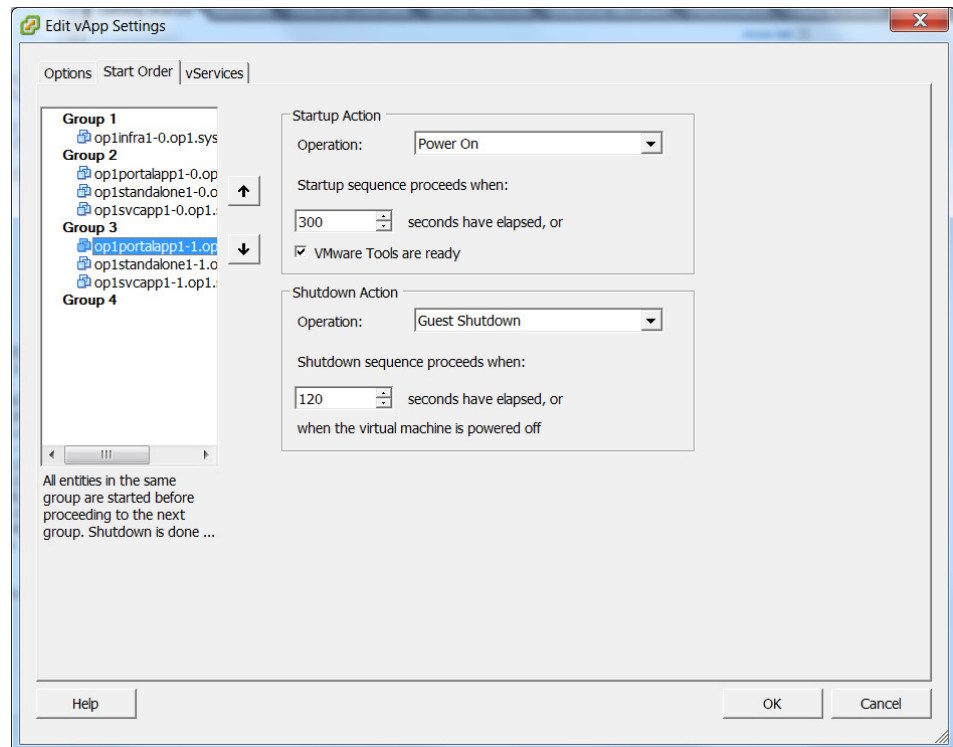
14. Select the **Power on after deployment** checkbox.

Note: If you are deploying the vApp in non-native High Availability mode, clear this checkbox instead.

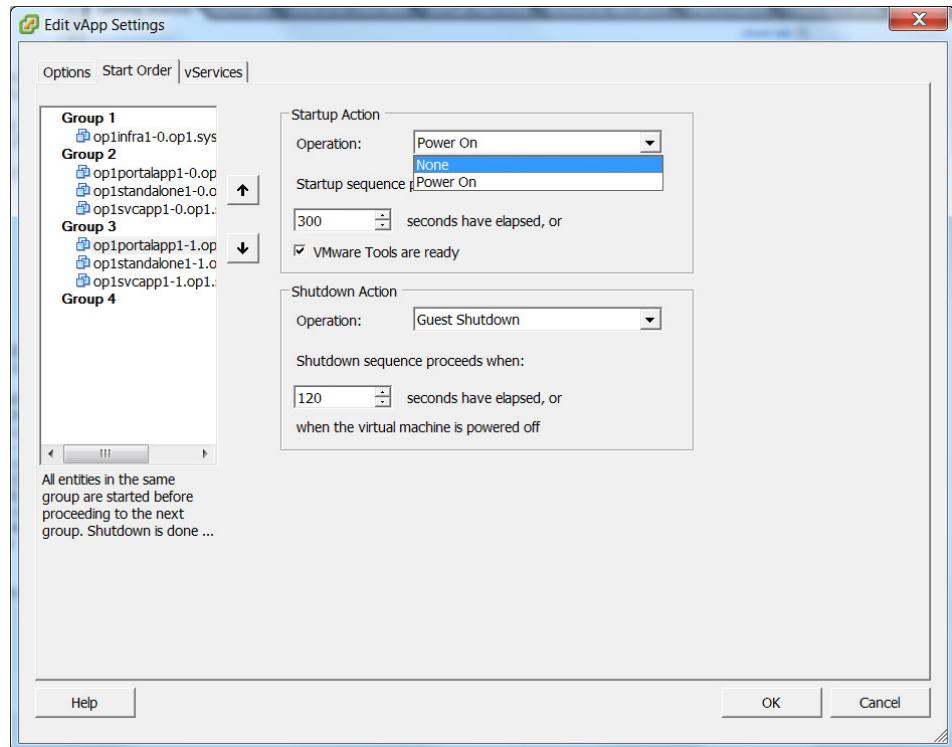
15. Click **Finish** to continue with the deployment process.
A bar shows the progress and time remaining for the process to finish.
It might take more than an hour for this process to run.
You receive a success message if the deployment has completed successfully.
16. If you have deployed the vApp in native High Availability mode, skip these Steps and proceed to Step 21.
17. Stop Power On operation for Node 2 VMs.
18. Click the deployed vApp in the vCenter and select **Edit vApp Settings**.



19. Click the **Start Order** tab and select the VMs in **Group 3**.



20. Change the **Startup Action - Operation** to *None* for each of the three VMs in **Group 3**.



21. Click **OK** to save the changes.
22. Power on the vApp, and verify that only the VMs in Group 1 and Group 2 have been powered on.

Step 3: Synchronizing Time Between Servers

Procedure

Ensure the VMware ESXi hosts and Oracle database servers synchronize time to a common NTP server.

Chapter 9. Part 3: Configuring the IBM MobileFirst Protect On-Premise Servers

After the IBM MobileFirst Protect On-Premise virtual appliance has been installed, the next step is to configure the deployment.

About this task

Configure the service using the IBM MobileFirst Protect On-Premise Administration Console through a browser.

Procedure

Before proceeding, ensure that the certificates and network requirements have been met as described in Chapter 5, “Software Requirements,” on page 11. This procedure can take approximately two hours to complete.

Step 1: Accessing the Administration Console

About this task

You can access the Administration Console with any browser (if you use Internet Explorer, use version 11 or later).

The Administration Console is hosted on the Configuration VM.

Procedure

1. Using any browser, navigate to `http://Configuration_VM_IP_Address`.
If you get a warning that the address is untrusted, you can ignore this warning.
2. Enter the default user name and password and click **Log In**.
User: *admin*
Password: *manage*
3. Accept the series of license agreements and continue.

Step 2: Choosing the Deployment Type

About this task

After accepting the license agreements, the **Deployment** screen is displayed.



Choose Deployment Architecture for MaaS360

MaaS360 On-Premises supports high availability architecture for better service uptime. It also supports reverse proxy configuration in case you don't want to expose the service to internet directly.

This virtual appliance has been shipped to you with seven virtual machines. In High Availability mode, MaaS360 will deploy all the 7 virtual machines and each of Portal, Services and Batch Apps will be deployed in a cluster of 2 virtual machines. Configuration virtual machine will still be one as its used during deployment purposes only. In case of Non-High Availability mode, only the first four virtual machines will be configured, you should shut down the other 3 VMs.

Please note that this is one time configuration and you will have to deploy the entire virtual appliance again if you want to change this configuration.

Deploy MaaS360 In High Availability	<input checked="" type="radio"/> Yes	<input type="radio"/> No
Deploy MaaS360 with Reverse Proxy	<input type="radio"/> Yes	<input checked="" type="radio"/> No
Deploy MaaS360 over HTTPS	<input checked="" type="radio"/> Yes	<input type="radio"/> No

IBM MobileFirst Protect On-Premise can be deployed in the following ways:

- *Native High Availability mode (using an external load balancer)*
You can choose to offload/terminate SSL at the load balancer or do it in IBM MobileFirst Protect On-Premise vApp.
A trusted SSL domain certificate has to be installed in the load balancer.
- *Non-native High Availability mode*
In this mode native High Availability is turned off and you should use VMware's High Availability capability in case you still need high availability.
- *Behind an external Reverse Proxy*
An external reverse proxy can shield IBM MobileFirst Protect On-Premise vApp from direct interaction with the Internet. You have to offload/terminate SSL at the reverse proxy. You can either initiate http or https communication from the reverse proxy to the IBM MobileFirst Protect On-Premise VMs.
A trusted SSL domain certificate has to be installed in the reverse proxy.

Procedure

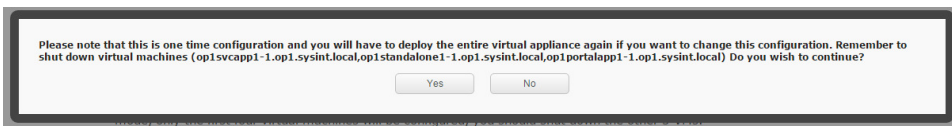
1. Choose the deployment architecture based on your requirements and configure the instance according to the instructions below.
 - **Deploy IBM MobileFirst Protect On-Premise in High Availability**
 - Yes—turn on the native High Availability
 - No (default)—turn off the native High Availability feature and deploy the vApp in non-native High Availability mode.
 - **Deploy IBM MobileFirst Protect On-Premise with a Reverse Proxy**
 - Yes—integrate the vApp with an external Reverse Proxy
 - No (default)—disable integration with an external Reverse Proxy
 - **Deploy IBM MobileFirst Protect On-Premise over HTTPS**
This is only valid if you selected Yes for integration with Reverse Proxy.
 - Yes—offload or terminate SSL at the Reverse Proxy, and then use another SSL certificate to encrypt the traffic and forward HTTPS requests to the IBM MobileFirst Protect On-Premise vApp (for enhanced security)

- No (default)— offload or terminate SSL at the Reverse Proxy and then forward HTTP requests to the IBM MobileFirst Protect On-Premise vApp

Important: The deployment settings are irreversible for the lifetime of the instance. If these deployment settings must be changed, you have to redeploy the entire instance.

If you choose the *non-native High Availability* option, you should shut down the Node 2 VMs by following instructions in “Step 2: Deploying the vApp” on page 27.

2. Click Continue.
3. Click **OK** if you are sure of the chosen deployment settings to continue. Click **Cancel** to review the deployment settings.



Step 3: Entering Database Settings

Procedure

1. Enter the following values for your database configuration:
 - **Oracle Host**
Use the hostname (recommended) or IP address of your Oracle database.
For an Oracle RAC setup, you can enter the hostnames or IP addresses of all your RAC nodes, separated by commas. IBM MobileFirst Protect On-Premise supports maximum of four RAC nodes as part of this configuration.
 - **Port**
Use the database port. The default value is 1521.
 - **DB Service Name**
Enter `standard_vpn2.DB_DOMAIN`
Enter the database domain you specified during your Oracle database installation for IBM MobileFirst Protect On-Premise. This should be same as the domain value entered for the `DB_DOMAIN` parameter in the `db_update.ini` file used during database set up.
 - **Password**
Enter the password for your database deployment. This should be same as the password value specified for the `APP_PASS` parameter in the `db_update.ini` file used during database set up.



Please provide Oracle database connection parameters. This is a mandatory step before configuring MaaS360 instance. You can provide comma separated values of multiple hosts for Oracle Host field.

Oracle Host	<input type="text"/>	DB time zone	<input type="text"/>	GMT	<input type="text"/>
Port	<input type="text" value="1521"/>	Host	IP	Database	Connectivity
DB Service Name	<input type="text" value="standard_vpn2.oprenmaas360.com"/>	op1svccapp1-1			
Oracle Config UI User	<input type="text" value="config_ui"/>	op1svccapp1-0			
Password	<input type="password"/>	op1portalapp1-0			
	<input type="button" value="Test Connection"/> <input type="button" value="Save"/>	op1infra1-0			
		op1portalapp1-1			
		op1standalone1-1			
		op1standalone1-0			

2. Verify that correct values have been entered and then click **Test Connection**.

If database is not reachable from the Configuration VM or if any of the other VMs in the vApp are unable to connect to the database, you see an error message below the text button.

- Fix all connection failures before continuing on.

The status of the database connectivity for all the VMs is displayed on the right hand side of the screen. You cannot proceed unless all tests show a green checkmark.

Example database connection failure:

Please provide Oracle database connection parameters. This is a mandatory step before configuring MaaS360 instance. You can provide comma separated values of multiple hosts for Oracle Host field.

Oracle Host:
 Port: 1521
 DB Service Name: standard_vpn2.onpremmaas360.com
 Oracle Config UI User: config_ui
 Password:

DB time zone: GMT ✓

Host	IP	Database Connectivity
op1svccpp1-0		✓
op1infra1-0		✓
op1portalapp1-0		✗
op1standalone1-0		✓

✗ Hosts "op1portalapp1-0" Failed to connect to database.

- After correcting all errors click on **Test Connection** again. Repeat this process till you see green checkmarks for all tests.

Example test success:

Please provide Oracle database connection parameters. This is a mandatory step before configuring MaaS360 instance. You can provide comma separated values of multiple hosts for Oracle Host field.

Oracle Host:
 Port: 1521
 DB Service Name: standard_vpn2.onpremmaas360.com
 Oracle Config UI User: config_ui
 Password:

DB time zone: GMT ✓

Host	IP	Database Connectivity
op1svccpp1-1		✓
op1svccpp1-0		✓
op1portalapp1-0		✓
op1infra1-0		✓
op1portalapp1-1		✓
op1standalone1-1		✓
op1standalone1-0		✓

✓ Database connectivity test is successful. Please follow the documentation for configuring MaaS360

- When all tests are successful, click **Save** to configure and start the database connections.

Note: This process may take up to 15 minutes to finish. Do not refresh the page.

Step 4: Changing the Password

About this task

The **Change Password** box appears. You are prompted to set a new password for increased security.

Change Password

Password should be 8 character long with at least one of each upper case, lower case, numeric and special character [~.,!@#,\$,%^,&.*_,-]

Enter E-mail Address

Confirm E-mail Address

Old Password

New Password

Confirm password

Procedure

1. Follow the specified guidelines.
2. Enter a valid email address.
If you forget your password, a newly generated password can be sent to that address as part of the password reset process.
3. Click **Save** to continue.

Configuring for Proxy Servers (optional)

You can configure the IBM MobileFirst Protect On-Premise virtual appliance to use a proxy server in the Forward Proxy Configuration page in IBM MobileFirst Protect On-Premise Administration Console.

About this task

Note: This feature is optional and can be skipped if you do not want to route outgoing requests through a proxy server.

Outgoing requests to the internet, from the virtual appliance, can be forwarded to your organization's proxy server.

Your organization's proxy server should be a standard HTTP proxy server deployed in the same network as the virtual appliance. HTTP and HTTPS requests originating from the virtual appliance can pass through this proxy server. Username and password based authentication require a valid user in the proxy server.

IBM MobileFirst Protect On-Premise sends outgoing requests to Apple, Google, and Microsoft servers for push notifications and also to access their corresponding mobile app stores. You need to allow for network traffic to those servers.

If you need to change these settings in the future, you can do so without having to reinstall the instance.

Procedure

1. In your forward proxy server, create a whitelist for the traffic from the IBM MobileFirst Protect On-Premise VMs to the following URLs:

Company	Push Notification	App Stores
Apple	https://gateway.push.apple.com:2195	https://itunes.apple.com/search
Google	https://android.googleapis.com/gcm/send	https://play.google.com/store
Microsoft	http://*.notify.live.net/ and http://*.notify.windows.com/	https://www.windowsphone.com and https://www.microsoft.com


Important: You have to whitelist the above URLs in the forward proxy server for proper functioning of IBM MobileFirst Protect On-Premise.

Other URLs in the proxy server, other than the ones mentioned above, could be redirect requests from the above sites. By default you should block or blacklist the other URLs in the proxy server. You should consult with IBM if there is any functionality loss due to the blacklisting of these URLs.

2. If you use Apple push notification service, add routing rules in your firewall to allow the Apple push notification requests, originating from IBM MobileFirst Protect On-Premise VMs, to Apple Servers at port 2195 to go out to the internet.

Typically the Apple push notification servers are hosted in the IP range 17.0.0.0/8. SSL communication with Apple push notification servers cannot be handled by a HTTP-based proxy server because a non-standard port (2195) is used.



3. If you configure an NTP server in the Administration Console, add routing rules in your firewall to allow NTP requests originating from IBM MobileFirst Protect On-Premise VMs to go out.
4. On initial configuration, select **Proxy Configuration** from the left settings panel,

then click the pencil icon  .



Proxy Configuration

- Solution Branding
- Mail Configuration

Forward Proxy Configuration  

Use this workflow to specify forward proxy configuration. On editing there are no forward proxies to use.

Use Proxy Yes

Server

Username maas

5. Select **Manual Proxy**. If you do not want to use a proxy server, select **Do not use proxy**.

6. Enter the proxy server settings:
 - Server: The hostname or IP address of the forward proxy server
 - Port: The listening port of the proxy server
 - Username: A valid user name, as defined in the proxy server
 - Password: The user's password

Note: If you do not enter username and password then IBM MobileFirst Protect On-Premise assumes the proxy server does not support authentication.

7. Select a URL from the pop-up menu or enter a valid whitelisted URL. Make sure the Apple, Google and Microsoft server URLs listed above have been already whitelisted in the proxy server.
8. Click **Test** to test the connection to the test URL from the virtual appliance through the proxy server.
9. If the test succeeds, click **Save** to save the entered configuration.

Important: Enabling or disabling the proxy server restarts the application modules in the IBM MobileFirst Protect On-Premise vApp. Account for downtime until all the application modules restart.

Validating Proxy Server Configuration

After instance configuration is successful, you should perform the following validation to confirm that the integration of the virtual appliance with the proxy server is successful.

About this task

Execute the below validation tests on Configuration VM [op1infra1-0/1-1] and Portal VM [op1portalapp1-0/1-1] using Secure Shell.

Note: Curl should exit with a zero status in all of the cases.

Procedure

1. Test the external URLs for access, then check the proxy logs.

```
$ curl https://itunes.apple.com/search
$ curl https://play.google.com/store >> /dev/null
$ curl http://www.windowsphone.com/en-us >> /dev/null
```

2. Test the domain URLs (Portal, Enrollment, End user portal and Services URLs) for access.

```
$ curl https://services_url/mdm-enroll/
Example : $ curl https://services.example.com/mdm-enroll/
```

```
$ curl https://portal_url/monitor-all/monitor.htm
Example : $ curl https://portal.example.com/monitor-all/monitor.htm
```

```
$ curl https://enrollment_url/dp/monitor.htm
Example : $ curl https://enrollment.example.com/dp/monitor.htm
```

```
$ curl https://end_user_portal_url
Example : $ curl https://eup.example.com
```

3. Test few internal URLs that do not resolve via proxy.

```
$ curl http://op1portalapp1-0.op1.sysint.local:8280/dp/monitor.htm > /dev/null
```

```
$ curl http://portalapp.op1.sysint.local:8280/dp/monitor.htm > /dev/null
```

```
$ curl http://scep.op1.sysint.local:9080/monitor/monitor.htm > /dev/null
```

Chapter 10. Part 4: Customizing the Service Features

About this task

Now that your servers are configured and communicating with each other, you can configure other features such as portal branding, email service integration, file storage location, and more.

You configure these features depending on your own organization's needs. For example, if you are not using SMS gateway service for your devices, you don't have to configure it.

All these customizations are done through the Administration Console.

Accessing the Administration Console

About this task

If you've just finished the IBM MobileFirst Protect On-Premise server configuration, you are already logged in through the console.

If you're returning, first connect to the Administration Console using any browser.

Note: If you are using Internet Explorer, version 11+ is required.

Procedure

1. Using any browser, navigate to `http://Configuration_VM_IP_Address`.
You might be presented with a warning that the address is untrusted, but this warning can be ignored.
2. Enter the username and new password and click **Log In**.
User: *admin*
Password: *as configured earlier*

Configuring Access URLs and Certificates

Set up your portal's URLs and certificate settings.

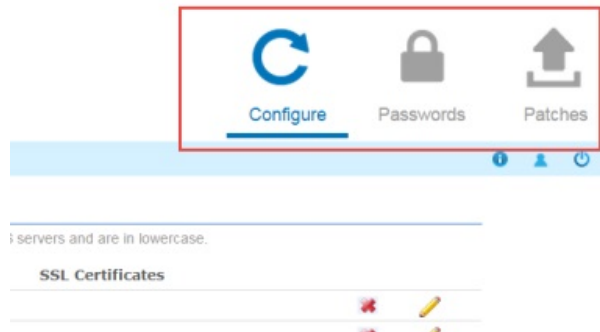
About this task


After the instance is configured the URLs cannot be changed. A fresh deployment is necessary if URLs have to be changed.

The DNS entries should follow the guidelines in Chapter 6, "Network Requirements," on page 15.

Procedure

1. Click **Configure** from the upper-right corner, then click **Solutions Branding**.



2. In the URL Branding section, click the pencil icon  to enter the DNS settings and SSL Certificates for each host.
3. Enter the External DNS host name for each component according to your high availability and reverse proxy configuration.
4. Enter the Internal DNS host name for each component.
 - Internal DNS is valid only if Reverse Proxy has been chosen for deployment. In that case, enter the DNS entries configured for internal routing.
 - Enter http URLs if http traffic is forwarded to IBM MobileFirst Protect On-Premise VMs.
 - Enter https URLs if https traffic is forwarded to IBM MobileFirst Protect On-Premise VMs.
5. Choose to upload a new SSL certificate or to use an SSL certificate that you recently uploaded during the configuration of this instance.
 - If you select **Use Previous**, the only visible field is a drop down list of existing uploaded certificates. A properly configured wildcard certificate can be used for all hosts.
 - If **New** is chosen then a completely new SSL certificate can be uploaded for the URL.

The SSL certificates should be issued from a trusted CA. You could use a wildcard certificate for all URLs or separate certificate for each URL.

For a Reverse Proxy with HTTPS deployment you can use self-signed certificates here, although it is recommended to use trusted SSL certificates. However at the Reverse Proxy you should have trusted SSL Certificates.

6. Select the SSL Sub CA Certificates file.

This is either a .crt or .pem file that contains the issuer Sub CA or a chain in which the issuer Sub CA is present.
7. Browse to the private key for the SSL Certificate for the host.

This is a .key file. The private key must not be password protected. For more information on removing the password, see Chapter 20, "Appendix D: SSL Certificate Password Removal," on page 105.
8. Repeat this process for the Portal, Enrollment, End User Portal and Device Services domains.

Use the **Use Previous** radio button to select certificates that were previously entered.
9. After entering all the information, click **Test** to ensure the settings are configured properly.

Errors are reported in red at the top of the screen while a successful test is indicated by a green checkmark. If the test is not successful, check the fields carefully and ensure they match your previous installation settings.

About Certificates


SSL certificates should be .crt or .pem files.

You can upload new/renewed certificates after the instance is configured. Make sure you upload renewed certificates and reconfigure the instance before the certificates expire.

Customizing Your Portal

You can add your own branding and logo to the IBM MobileFirst Protect On-Premise Portal.

Procedure

1. Click the pencil icon  .
2. Enter a solution name.
There is a limit of 32 characters.
3. Click Choose File to upload a logo.
The logo should be 93x43 pixels.
4. Click **Save** to close.

Connecting to Mail Service

Procedure


Use the **Mail Configuration** tab on the left side of the screen to configure your mail service settings.



Configuring SMTP (outgoing mail) Settings

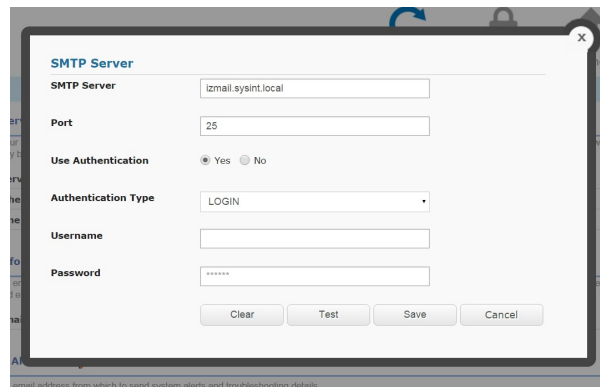
If you want the service to send email, it needs to use your organization's existing SMTP service.

Procedure

1. Click the pencil icon  to edit your SMTP server settings.

Setting	Instruction
SMTP Server	Enter the domain name of your SMTP server. For example, smtp.company.com.

Setting	Instruction
SMTP Port	Enter your SMTP server port. The default value is 25.
User Authentication	Choose Yes or No, as needed for your mail system. The default is "no."
Authentication Type (authenticated SMTP only)	Choose the authentication type enabled on your SMTP server from the pop-up list: LOGIN (default), PLAIN, DIGEST-MD5, MD5, CRAM-MD5.
Username and password (authenticated SMTP only)	This is the user mail account from which mail is sent.




2. Click **Test** to ensure that the settings are configured properly.
Errors are reported in red at the top of the screen while a successful test is indicated by a green checkmark. If the test is not successful, check the fields carefully and ensure that they match your deployment.
3. Click **Save**

Configuring Mail Sender Address and Display Name

About this task

Email messages that the service sends to administrators and end users must be from a provisioned mail user of your organization's mail system. All emails sent from the IBM MobileFirst Protect On-Premise deployment originates from this email address.

Procedure


1. Click the pencil icon  to set the email address.
This email address must be an existing mail user.
2. Set the display name.
The display name set on your SMTP server may override the value entered here.

Setting the System Alerts Email Recipient

About this task

If problems arise with the IBM MobileFirst Protect On-Premise deployment, the system sends emails to the indicated address. In addition, system level emails such as support logs are sent to this address.

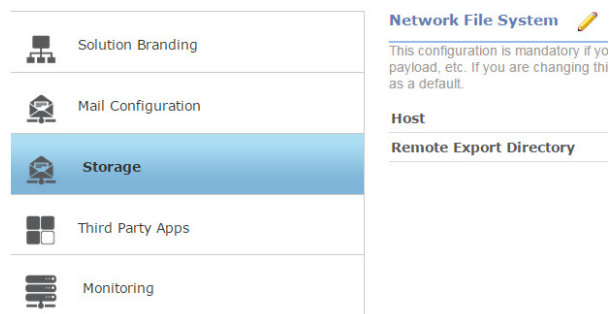
Procedure

Click the pencil icon  to set an administrator email account that receives service messages.

Configuring File and Mobile App Storage

About this task

The Storage tab allows for configuring storage in an external Network File System (NFS) server, a shared storage for CDN content including applications, documents, and IBM MobileFirst Protect On-Premise Agent Application artifacts.



External storage is mandatory for a native High Availability deployment, and optional in other deployment types.

Note: This is an irreversible configuration for the life of the instance.

Procedure

1. Make sure you have a backup and restore solution for the NFS server and files.
2. Set up the NFS server for high availability to avoid data or service loss.
3. Make sure the NFS server and the export directory is accessible from the IBM MobileFirst Protect On-Premise vApp.

If you lose accessibility, you lose the uploaded content.

4. Click the pencil icon  to edit the storage settings:

Setting	Instruction
Host	Enter the hostname or IP Address of the remote NFS server. Ensure the host is reachable from the Services and Standalone VMs of the IBM MobileFirst Protect On-Premise vApp.
Port	Enter the port number of the NFS server. The default value is 2049.
Remote Export Directory	Enter the remote directory in the NFS server that is exported as CDN storage space for IBM MobileFirst Protect On-Premise.

5. Click **Test**, and then **Save**.

Connecting to Third-Party Applications and Services

The **Third Party Apps** tab allows the configuration of several features that use third-party systems to enhance IBM MobileFirst Protect On-Premise.



Adding an APNS Proxy Server Client-Authentication Certificate

If you use the App Store IBM MobileFirst Protect agents, you must upload this certificate in IBM MobileFirst Protect On-Premise Administration Console to enable push notification to iOS devices.

About this task

You can enroll iOS devices into your IBM MobileFirst Protect On-Premise instance with the IBM MobileFirst Protect iOS agent applications available in Apple App Store.

Important: To enable this feature, you must choose this option at the time of initial instance configuration or reconfiguration through the IBM MobileFirst Protect On-Premise Administration Console. This setting is an instance level property and is applicable to all customer accounts created in the instance. You can reconfigure these settings at any time after installation.

The following agents available in iTunes App Store are compatible with IBM MobileFirst Protect On-Premise.

- MaaS360 for iOS: <https://itunes.apple.com/in/app/maas360-for-ios/id459732007?mt=8>

- Secure Browser: <https://itunes.apple.com/in/app/maas360-browser/id591773034?mt=8>
- Secure Editor: <https://itunes.apple.com/in/app/maas360-secure-editor/id834866167?mt=8>

For these App Store agent applications, the IBM MobileFirst Protect On-Premise portal routes notification messages to the apps on iOS devices through an APNS proxy server hosted in IBM cloud.

The URL for this proxy server is `apns.maas360.com`. Messages posted from the portal to the APNS proxy server are encrypted, then re-encrypted using Apple certificates and forwarded to Apple's push notification servers. The IBM MobileFirst Protect On-Premise APNS proxy server doesn't analyze the messages or keep them.

Important: You must open access to this URL in your external firewall so that IBM MobileFirst Protect On-Premise VMs can connect to it and post the notification messages.

Getting a Client Authentication Certificate

A client certificate is used to authenticate the On-Premise instance of the customer when it connects to the APNS proxy server.

About this task

IBM Support distributes a client authentication certificate unique to each customer after the customer provides some required customer details.

The certificate is valid for five years, and you need to ask for a new one from IBM Support when it expires. IBM can revoke this certificate at any time for security reasons, and issues a new replacement certificate as needed.

The certificate is p12 format. The same client certificate can be installed for multiple On-Premise instances for the same customer.

Important: This certificate is a secured and unique file, and must not be shared. Only upload it to a single customer's IBM MobileFirst Protect On-Premise installation.


Procedure


Contact IBM Support and provide the requested details to get the certificate and password.


Uploading the Certificate to the Instance

You must upload this certificate through IBM MobileFirst Protect On-Premise Administration Console to enable push notification to iOS devices.

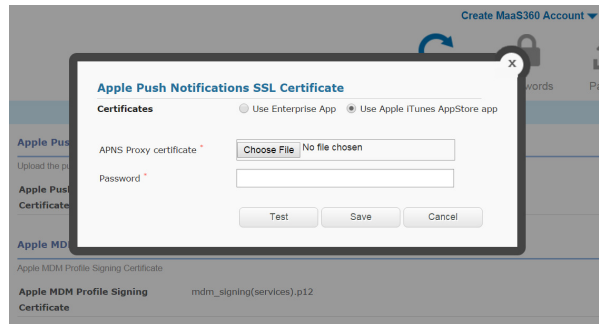
Procedure

1. Click the **Third Party Apps** tab.
2. Click the pencil icon  to edit your certificate choice.

Apple Push Notifications SSL Certificate 	
Upload the push notifications SSL certificate in order to directly use the MaaS360 App for iOS hosted on Apples iTunes Portal	
Apple Push Notifications SSL Certificate	APNS_PROXY_certificate.p12 (iOS AppStore)

Apple MDM Profile Signing Certificate 	
Apple MDM Profile Signing Certificate	
Apple MDM Profile Signing Certificate	mdm_signing(ervices).p12

3. Select Use Apple iTunes AppStore app.



4. Click **Choose File** to select the p12 format authentication certificate file.
5. Enter the password for the certificate as provided by IBM.
6. Click **Test** to test the validity of the certificate.
7. Click **Save** when you're finished.

Add an Apple MDM Profile Signing Certificate

About this task


Apple profile signing certificate is an SSL certificate used to sign the MDM profile that gets installed on Apple devices.

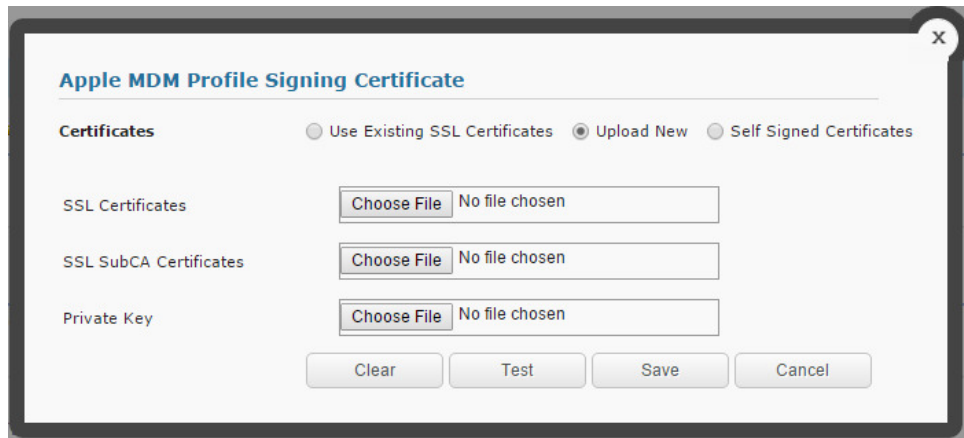
You can use the existing SSL certificate uploaded with the Services URL in the URL branding section, obtain a code signing certificate and upload it or choose to use a seeded self-signed certificate.

Note: For Reverse Proxy deployment with HTTP traffic routed to IBM MobileFirst Protect On-Premise you could choose to upload a new certificate with the Upload New option. Make sure the certificate uses 2048-bit keys or more.

If you do not upload a new certificate, by default the seeded self-signed certificate is chosen.

Procedure

1. Click the **Third Party Apps** tab.
2. Click the pencil icon  to edit your certificate choice.
3. To use an existing SSL Certificate, select it from the list of previously installed certificates.
4. To upload a new signing certificate, choose the new SSL Certificate, SSL SubCA Certificate, and Private Key files, and click **Save**.




5. To use a seeded self-signed certificate, select the certificate.
During MDM profile installation on the iOS device, the user is prompted to accept this certificate to continue with management.
6. Click **Save**.

Add the Microsoft Bing Maps Feature

About this task

IBM MobileFirst Protect On-Premise has device location tracking features that can integrate with Microsoft Bing Maps to show the physical location of a device. If you want to implement those features, you need a Bing Maps Key.

Procedure

1. Click the **Third Party Apps** tab.
2. Click the pencil icon .
3. Enter the key, and click **Save**.

Enable Android Notifications

About this task

There are two communication protocols used to communicate with Android devices.

Google Cloud Messaging (GCM) is the primary protocol for Android communication. You must set up a free GCM account and provide the **Sender ID** (also known as the *Project Number*) and **Google API Key** to the IBM MobileFirst Protect On-Premise server. For more information about GCM, see <http://developer.android.com/google/gcm/gs.html>.


Note: The Sender ID is not the email address associated with your GCM account.

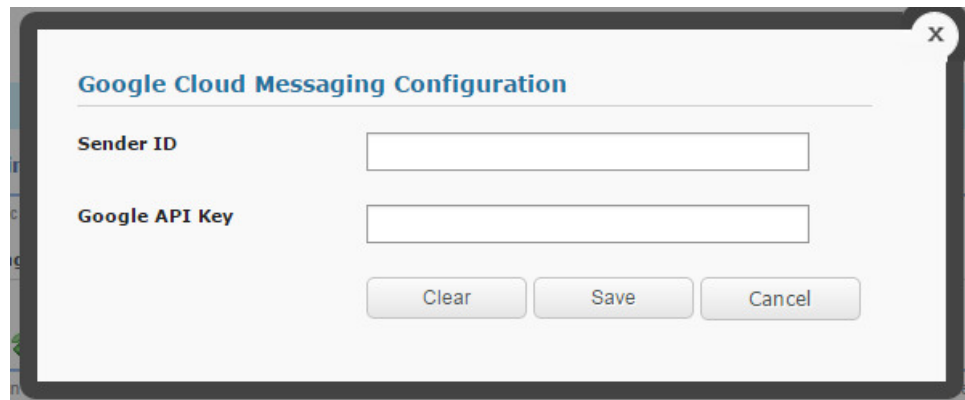
Message Queuing Telemetry Transport (MQTT) is an additional protocol for Android communication. It is necessary for integration with IBM® MessageSight product.

See the *IBM MessageSight Configuration for MaaS360* guide for information about configuring a MessageSight server for IBM MobileFirst Protect On-Premise Android notifications.

You must configure GCM or MQTT to enable communication with Android devices.

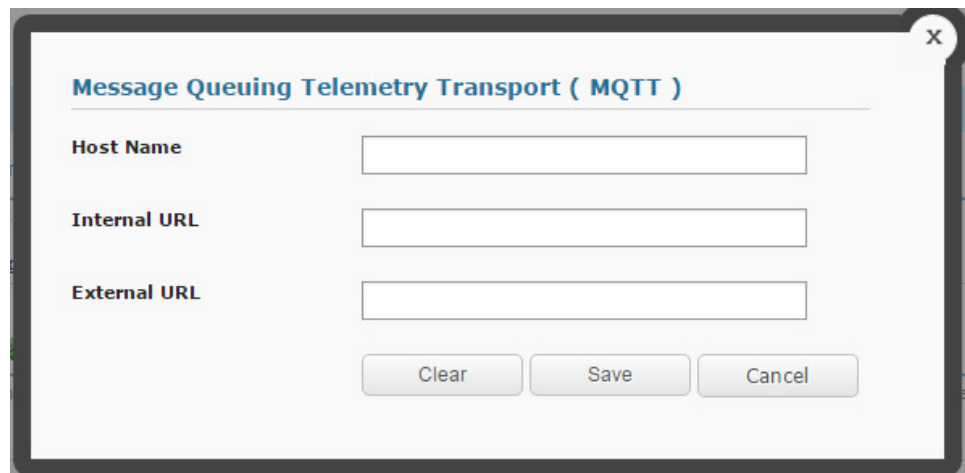
Procedure

1. Click the **Third Party Apps** tab.
2. Choose the GCM or MQTT radio button and click the pencil icon  .
3. If you chose GCM, enter the Sender ID and Google API Key.



The screenshot shows a dialog box titled "Google Cloud Messaging Configuration". It contains two text input fields: "Sender ID" and "Google API Key". Below the fields are three buttons: "Clear", "Save", and "Cancel".

4. If you chose MQTT, enter the host name, and URLs associated with MQTT server.



The screenshot shows a dialog box titled "Message Queuing Telemetry Transport (MQTT)". It contains three text input fields: "Host Name", "Internal URL", and "External URL". Below the fields are three buttons: "Clear", "Save", and "Cancel".

5. Click **Save**.

Enter SMS Gateway Account Details


About this task

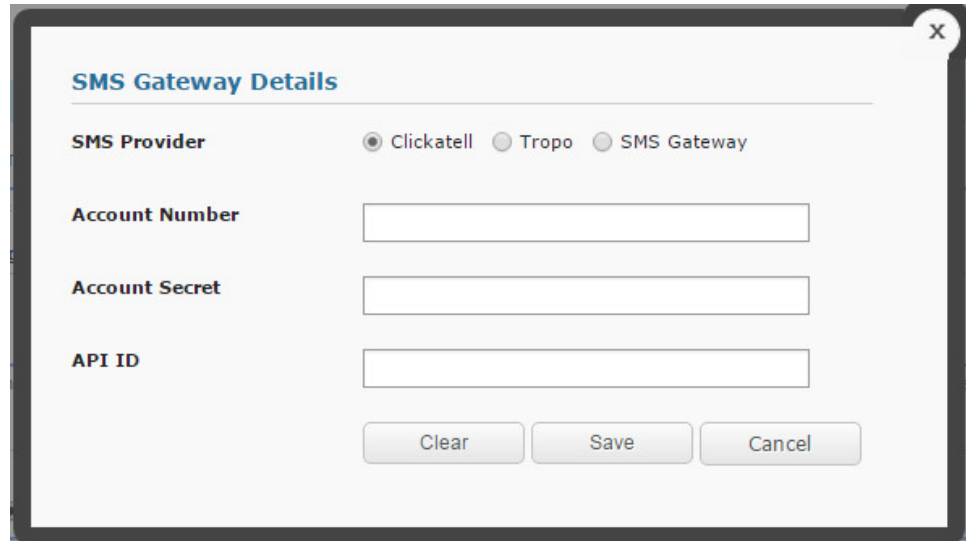
Device enrollment requests can be issued by email or SMS.

To enable SMS requests, set up an SMS Gateway account with a third-party provider. Currently, two SMS providers require less configuration: Clickatell and Tropo.

Alternatively, you can directly integrate with an SMS/SMPP Gateway which supports SMPP 3.4 protocol, as specified in the standards document - http://opensmpp.org/specs/smppv34_gsmumts_ig_v10.pdf

Procedure

1. Click the **Third Party Apps** tab.
2. Click the pencil icon  to designate an SMS provider.
3. If you select Clickatell or Tropo, enter the **Account Number**, **Account Secret**, and **API ID** provided by the SMS service provider.



4. If you select SMS Gateway, enter the service's configuration values, then click **Test** to ensure there are no errors connecting to the SMS Gateway Server.

Table 6. SMS Gateway Settings

Setting	Description
SMPP Hostname	IP Address / URL of the SMS Gateway Server Note: Please make sure Standalone Batch Jobs VM and Configuration VM have access to this Server
Port	Port number of the SMS Gateway Server Default value: 2775
Username	Username of the account created in the SMS Gateway
Password	Password for the account created in the SMS Gateway
Retype Password	Same as what was entered in Password field
Sender Type of Number (TON)	Type of Number Default value: 1
Sender Numbering Plan Identifier (NPI)	Number plan identifier Default value: 1

Table 6. SMS Gateway Settings (continued)

Setting	Description
Originator/Sender	Name of the sender as setup in the SMS Gateway Server
Priority	Priority of the message. Default value: 0

Refer to <https://docs.oracle.com/cd/E19142-01/819-0105/sms.html> to get more details on the values to be entered for the above fields.

5. Click Save.


Enter Network Time Protocol (NTP) Server Details

About this task

A NTP Server URL can be specified to synchronize the clocks of all the VMs in the vApp to a single time setting.

Important: Ensure the Database Server is also synchronized with the same NTP Server.

Procedure

1. Click the **Third Party Apps** tab.
2. Click the pencil icon  to designate an NTP provider

3. Enter the URL, then click **Save**.

Note: If the NTP server is configured, you can choose to disable configuration of time synchronization with the ESXi host(s) for each virtual machine in the vApp provided the ESXi host(s) are not synchronized with the same NTP server.

Integrate with an Application Reputation Engine


About this task

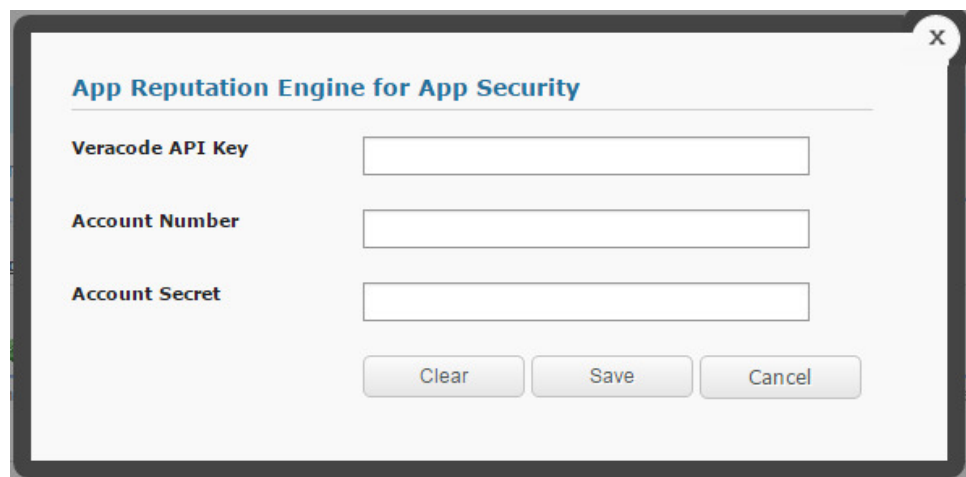
IBM MobileFirst Protect On-Premise provides integrates with an external application reputation provider, Veracode, to get the latest ratings for Android Applications hosted in Google Play Store.

You must set up an account with Veracode to obtain a Veracode API Key, Account Number, and Account Secret.

Note: Keep Internet connectivity for Veracode license key verification. If you notice verification failure errors, make sure the IBM MobileFirst Protect On-Premise vApp has outgoing access to the Internet. This verification is performed in IBM MobileFirst Protect On-Premise Portal in the Application Management workflow.

Procedure

1. Make sure the IBM MobileFirst Protect On-Premise vApp has outgoing access to the Internet.
2. Click the **Third Party Apps** tab.
3. Click the pencil icon  to enable Veracode integration.
4. Enter the **Veracode API Key**, **Account Number** and **Account Secret** from Veracode, then click **Save**.



The screenshot shows a dialog box titled "App Reputation Engine for App Security". It has a close button (X) in the top right corner. The dialog contains three input fields with the following labels: "Veracode API Key", "Account Number", and "Account Secret". Below the input fields are three buttons: "Clear", "Save", and "Cancel".

5. Click **Save**

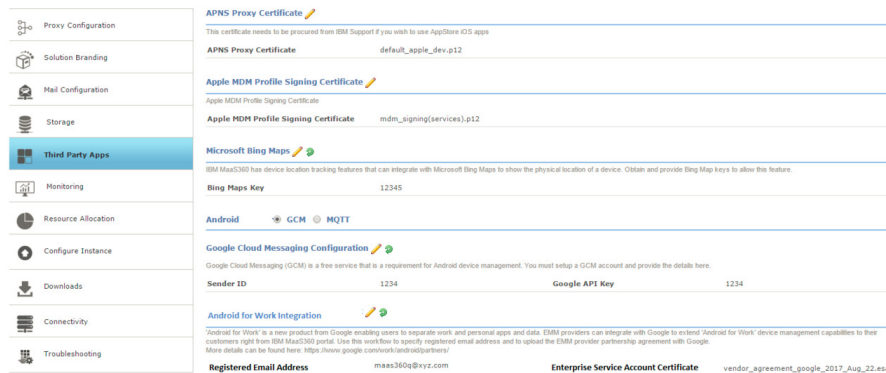
Integrating with Android for Work


About this task

Android for Work gives IT the ability to separate personal and work data from each other at the operating system level. This allows wide support for all Android apps and security controls built into the OS itself.

Procedure

1. Get an Enterprise Service Account (ESA) certificate from Google.
 - a. Log in to your Google apps admin account at <https://console.developers.google.com>.
 - b. Navigate to **API Manager > Credentials**
 - c. Click **Add Credential**, then select the service account.
 - d. Choose **p12** as the key type, then save the p12 file. This is the ESA certificate.
2. Click the **Third Party Apps** tab.



3. Next to **Android for Work**, click the pencil icon  .
4. Enter the registered email address and upload the p12 certificate file, and click **Save**.
5. To configure Android for Work for each customer, see the IBM MobileFirst Protect On-Premise Configuration Guide.


Setting up SNMP Monitoring

About this task

The **Monitoring** tab allows the configuration of the Simple Network Management Protocol (SNMP). Using SNMP is optional.

IBM MobileFirst Protect On-Premise supports SNMP v2c and v3.

Procedure

1. Select the **Monitoring** tab in the Administration Console.
2. Choose the SNMP version tab, then click the pencil icon  to configure the SNMP settings.



3. If you choose **SNMP Version 2c** (v2c), do the following:
 - a. For the **Allowed Host(s)**, enter a comma separated list of IP addresses or hostnames for those hosts that are authorized to monitor the seven IBM MobileFirst Protect On-Premise VMs.
 - b. Enter the Community String, then click **Save**.

4. If you choose **SNMP v3**, do the following:
 - a. Under **Allowed Host(s)**, enter a comma delimited list of IP addresses or hostnames for those hosts that are authorized to monitor the seven IBM MobileFirst Protect On-Premise VMs.
 - b. Enter the appropriate **User Name**, **Password**, and **Pass Phrase**, then click **Save**.

Setting up System Monitoring


In addition to SNMP monitoring, you can get email monitoring IBM MobileFirst Protect On-Premise instance's health for critical problems that can lead to loss of functionality or downtime.

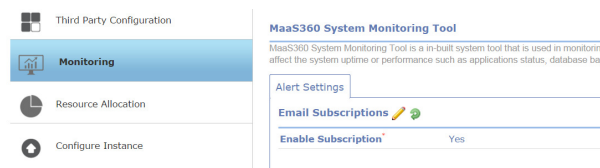
About this task

You receive email notifications for critical system health parameters, based on seeded threshold values, at regular intervals of time. You can use the system monitor either with or without SNMP monitoring to get comprehensive information on the health of MaasS360 On-Premise instance.

By default monitoring and alerting is turned off. However, it is recommended that you enable monitoring and alerting during initial configuration.

Procedure

1. Select the **Monitoring** tab in the Administration Console.
2. In the System Monitoring Tool section, click the pencil icon  to configure the notification settings.



3. Select **Enable** to turn it on.
4. Enter the email address in Mailing List field to enable subscription of alerts. This can be the email address of a group or individual.
5. Click on Save to activate system monitoring. You can select 'Disable' radio button and click on Save to deactivate system monitoring and alerting.
6. Use the VMware vSphere client to monitor and reduce resource overload on the VMs in the IBM MobileFirst Protect On-Premise app. This reduces the overhead of excessive alerts.

Monitoring Applications Using SNMP

About this task

SNMP clients can be used to monitor the IBM MobileFirst Protect On-Premise modules hosted in the seven IBM MobileFirst Protect On-Premise VMs.

OIDs or Object Identifiers are assigned to various IBM MobileFirst Protect On-Premise module level attributes representing Memory, Database Connections, Application State, CPU usage, Open Files, Uptime & Thread Count. These OIDs can be monitored through SNMP.

Procedure

Access the list of available OIDs at https://Configuration_VM:8443/static/MaaS360-OIDs.txt

You can also download this file from the Downloads page.
 This URL provides OID list for 1-0 virtual machines. The same set of OIDs work for 1-1 virtual machines of the same type.

Checking Server Connectivity

About this task

On the **Connectivity** tab of the Administration Console, you can see the network connectivity of the IBM MobileFirst Protect On-Premise VMs with external systems, Database, and within themselves. All port connections should show up as green checkmarks before you continue with the configuration of the instance.

External connectivity Monitoring				
	Portal VM	Services VM	Configuration VM	Standalone VM
Internal to Appliance				
Portal VM	✓	✓	✓	✓
Services VM	✓	✓	✓	✓
Setup VM	✓	✓		
Standalone VM	✓	✓	✓	
Environment Configuration				
Database	✓	✓	✓	✓
SMTP Server	✓	✓	✓	✓
Third Party Applications				
Google QR Code	✓	✓	✓	✓
SMS Gateway	✓	✓	✓	✓
Bing Maps	✓	✓	✓	✓
Messaging Services				
MQTT				
APNS Servers	✓	✓	✓	✓
GCM	✓	✓	✓	✓
Live.com				

[Export Results](#)

Database User Account Status ✓

Procedure

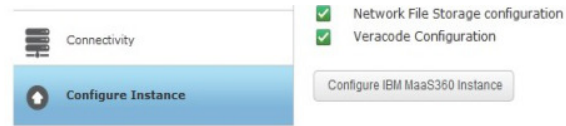
If you see a red X, hover over it to see the error message. Fix the reported errors and then refresh the page.

Note: Configuring the instance with pending errors may result in configuration failure or loss of functionality.

Chapter 11. Part 5: Configuring the Instance

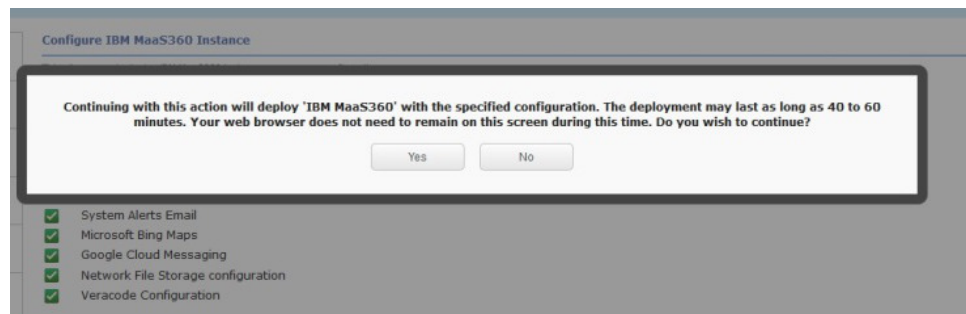
About this task

After all settings are configured, click the **Configure Instance** tab.

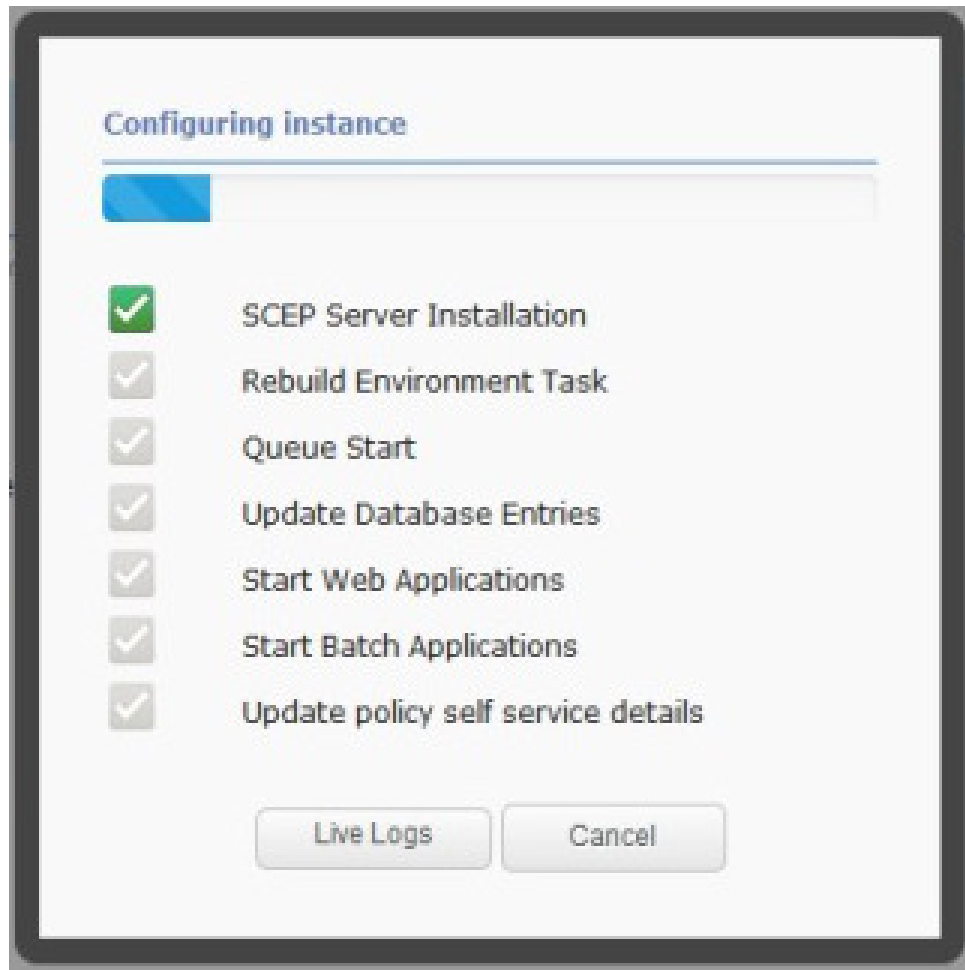


Procedure

1. Check each entry for a green checkmark, and If any item is not configured properly, correct the setting.
2. Once everything has a green checkmark, click **Configure MaaS360 Instance** to transfer your configured settings to the database and application modules. A confirmation window appears.
3. Click **YES** to continue.



A progress bar displays the configuration status. It takes several minutes before any progress is reflected, and the entire process can take up to an hour.



4. Select **Live Logs** to see a static snapshot of the configuration in progress. If you exit your browser, the configuration continues without it. You can log back in to the Administration Console and select the **Configure Instance** tab again to view the progress.

Chapter 12. Part 6: Checking Live Connectivity

About this task

After the instance has been successfully configured, check the network connectivity between the IBM MobileFirst Protect On-Premise VMs and external systems, the database and themselves. All port connections should have a green checkmark before you continue.

External connectivity Monitoring				
	Portal VM	Services VM	Configuration VM	Standalone VM
Internal to Appliance				
Portal VM	✓	✓	✓	✓
Services VM	✓	✓	✓	✓
Setup VM	✓	✓		
Standalone VM	✓	✓	✓	
Environment Configuration				
Database	✓	✓	✓	✓
SMTP Server	✓	✓	✓	✓
Third Party Applications				
Google QR Code	✓	✓	✓	✓
SMS Gateway	✓	✓	✓	✓
Bing Maps	✓	✓	✓	✓
Messaging Services				
MQTT				
APNS Servers	✓	✓	✓	✓
GCM	✓	✓	✓	✓
Live.com				

[Export Results](#)

Procedure

If you see a red X, hover over it to see the error message. Fix the reported errors, then refresh the page.

Note: Configuring the instance with pending errors may result in configuration failure or loss of functionality.

Chapter 13. Part 7: Creating an Organization Account

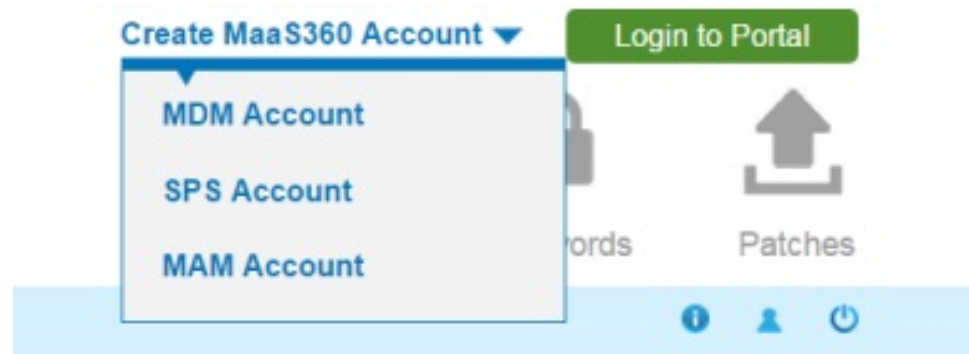
About this task

When configuration completes, you are prompted to create an account. Mobile devices and user accounts are tied to a single organization account.

Procedure

1. Click either **Create MDM Account**, **Create SPS Account**, **Create MAM Account** as needed. A new tab opens to the associated account creation portal. For more detailed information about creating an account, see IBM MobileFirst Protect On-Premise Configuration Guide.
2. Close this window to return to the Administration Console if you do not want to create an account at this time.

You can also create accounts from a menu at the top right corner of the Administration Console.



What to do next

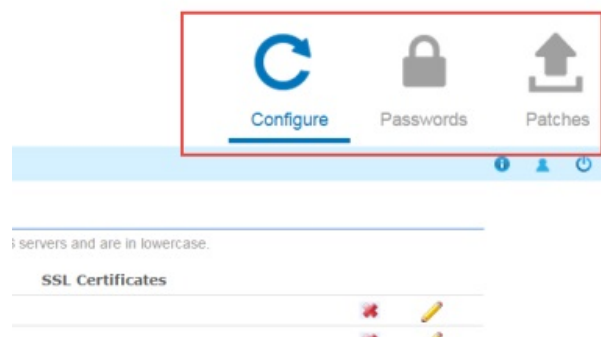
Note: Verify that there are no failures in application modules, using “Troubleshooting” page, before proceeding with the account creation.

Chapter 14. Continuing Maintenance

After the configuration has completed, look at the **Connectivity** and **Troubleshooting** tabs on the left side of the Administration Console to review the overall health of the system, and fix any errors that have been reported.

Using the Administration Console for Maintenance

Three tabs (in the upper-right corner of the user interface) show different configuration tasks and settings.



Configure

The bulk of your deployment configuration is performed using this tab.

Passwords

This tab provides password management for the operating systems of the seven virtual machines contained in the IBM MobileFirst Protect On-Premise virtual appliance.

You can grant remote access to your IBM MobileFirst Protect On-Premise environment to IBM support from the **Passwords** interface.

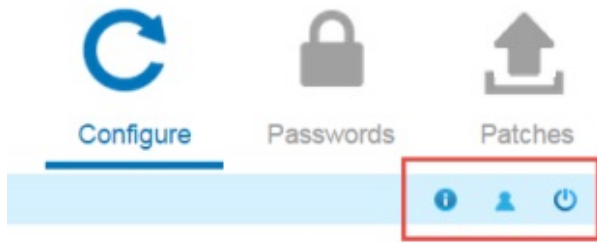
You can update the password applications used to connect to databases using the **Database Password** link in **Passwords** interface.

Note: Update the passwords for the databases before they expire.

Patches

You can apply new patches to fix issues with your instance. For more information, see “Applying Patches” on page 80.

There are three icons under those tabs.



Tab	Description
About	Displays version information for the various components of the deployment.
User	Displays the current user and allows that user's password to be changed. It also allows that user to log out of the configuration.
Logout	Logs the current user out of the configuration UI and shows the Administration Console.

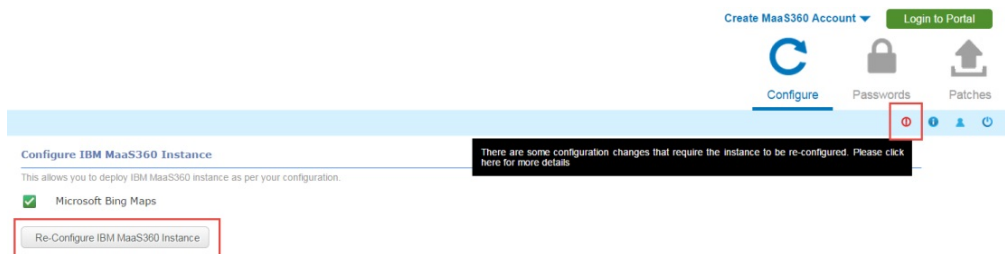
Last Login Information

The current user's last login time and date is displayed on the message bar at the bottom of IBM MobileFirst Protect On-Premise Administration Console.

Reconfiguring the Instance

After configuration is complete, you reconfigure your deployment to change settings. changes that are made in the Administration Console are not deployed instantly. Instead, you must reconfigure the instance using **Re-configure MaaS360 Instance** button.

After you configure your deployment, the **Configure Instance** tab displays a **Re-configure MaaS360 Instance** button.



This button is available only if a setting is changed. Any settings that have been changed since you last configured, are listed above the button. You can review any them and click **Re-configure MaaS360 Instance** to deploy the changes.

Any time a change is made in the Administration Console, a red icon displays near the **About**, **User**, and **Logout** buttons. If you hover over it, you receive a message that changes were made that are not yet deployed.

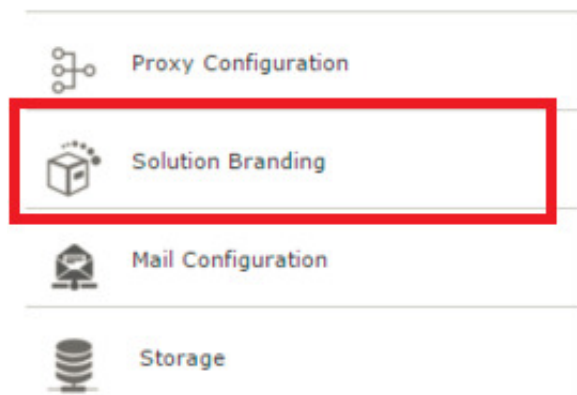
Reconfiguration takes several minutes to complete. As with the initial configuration, a snapshot of the logs can be viewed to verify that the process is active.

After reconfiguration completes, the system requires a 10-minute waiting period before access to the Administration Console is granted. This is reflected in the live logs.

Note: After a reconfiguration look at the Connectivity and Troubleshooting to review the overall health of the system and fix any errors that have been reported.

Replacing Certificates

You can change certificates for each component host in the **Solution Branding** tab of the Administration Console.



Backing Up and Restoring Your Service and Data

A robust backup and recovery mechanism for IBM MobileFirst Protect On-Premise is essential to recover from catastrophic failures and eliminate data loss. A complete backup policy should include full backup capabilities as well as incremental backups.

This content is provided as a guideline. You are expected to define your own Recovery Point Objective (RPO) and Recovery Time Objective (RTO) for IBM MobileFirst Protect On-Premise based on your requirements for uptime and data loss prevention.

Because the underlying technology used in IBM MobileFirst Protect On-Premise is VMware and Oracle, we recommend using the backup and recovery tools provided by these vendors. This is at your discretion; any tools you are comfortable with, or that meet your needs, are acceptable.

The components that should be part of your backup plan include:

- Virtual Appliance (vApp) and VMs
- Oracle databases: AGILINK, EDW, VPN2, and P03

- Content Delivery Network (CDN), NFS export directory
- IBM MobileFirst Protect Cloud Extender
- IBM MobileFirst Protect Mobile Enterprise Gateway

Backup Frequency

Determine a backup schedule that is appropriate to your deployment.

The following backup schedule is recommended. This schedule can be altered to fit your RPO and RTO requirements.

Table 7. Recommended backup frequency

Component	Full backup	Incremental backup
vApp and VMs	Weekly	Daily
Oracle Database	Weekly	Daily
Cloud Extender	Weekly	Daily
Mobile Enterprise Gateway	Weekly	Daily
CDN Content backup, NFS export directory	Weekly	Daily

For a High Availability deployment, an NFS server hosts the CDN content. The export directory in the NFS server that hosts CDN content for IBM MobileFirst Protect On-Premise has to be backed up and restored in case of failures.

For non-High Availability deployment, the CDN is part of the Services VM and is therefore backed up when the Services VM is backed up. However, it is possible to back up the content in the CDN independently, if desired, using a script. For more information, see “Backup the CDN” on page 71.

The IBM MobileFirst Protect Cloud Extender and IBM MobileFirst Protect Mobile Enterprise Gateway are optional components that might not be part of your deployment.

Backup the Virtual Appliance

When you back up the IBM MobileFirst Protect On-Premise VApp, be sure to include the backup and recovery of all aspects of the vApp environment.

Your chosen backup and recovery tools should have the capability to back up the entirety of the virtual appliance or every individual virtual machine. These include the Configuration, Portal, Standalone Batch Jobs, and Services & CDN virtual machines. The backup should capture both disk and memory data. In addition, your backup solution should allow full and incremental backups. Fast recovery by applying delta changes should also be supported. The ability to selectively restore individual files and folders within a virtual machine is also an advantage.

VMware vSphere Data Protection is the recommended tool to back up and restore your VMware environment. This tool meets all of the requirements listed. However, the choice of tool should be left to your VMware administrator based on the needs of your environment.

Backup the Oracle Database

A full backup solution should include backup of your Oracle database environment with all four databases that are part of your IBM MobileFirst Protect On-Premise deployment.

Your Oracle database backup solution should allow full and incremental backups of the four databases: AGELINK, EDW, VPN2, and P03. The backup should include data files, control files, and archived redo logs.

The recommended backup tool for your Oracle environment is Oracle's Recovery Manager or RMAN. RMAN is fully integrated with Oracle database and it supports full backup, incremental backup using change tracking, binary compression, encryption, and cross platform data conversion.

Archive Log Mode should be enabled for the four Oracle databases for RMAN to function properly. Be sure to enable Archive Log Mode during database installation. For more information see Chapter 7, "Part 1: Installing the Database," on page 21.

In addition, setting up a Flash Recovery Area, or FRA, is recommended. Using a FRA simplifies database backup by automatically naming recovery files, retaining them as long as they are needed for restore and recovery activities, and deleting them when they are no longer needed. The FRA should be sized according to your RPO and RTO policies.

Note: Incremental backup is not supported in Oracle Standard Edition or Standard Edition One.

Backup the CDN

About this task

The Content Delivery Network is used to store distributed apps, documents and agent versions. Be sure to include it in your backup plan.

The CDN is hosted in the Services VM and is at /u002. Because the Services VM should be part of your VMware backup plan, the CDN is automatically included. However, it is possible to back up CDN content separately with a utility.

Prepare the CDN backup utility by completing the following steps:

Procedure

1. Download the CDN backup script from the **Downloads** tab in the Administration Console.

For more information, see "Downloading Additional IBM MobileFirst Protect On-Premise Management Tools" on page 77.

Note: The Downloads tab might not be available within the Administration Console until you have configured your deployment.

2. Copy and run the script on the server where you want to back up the CDN content.

Specific CDN user credentials exist for this operation. The `cdn` user is the default user, and you are prompted for the password after the script runs:

User: *cdn*
Password: *MaaS360_Console*

Note: The user who runs this script must have permissions to create subdirectories under the directory where the script is run.

The *cdnbackup.sh* script can be used according to the following parameters to back up the CDN content:

```
cdnbackup.sh [-bbackup_dir] [-l remote_user] [-H remote_host] [-d remote_dir] [-D dir_list]
```

Where:

-h	Help
-b	Directory to back up. This parameter can be omitted if default value is used.
-l	User login name. This parameter can be omitted when you use the default <i>cdn</i> user.
-H	IP address of Services VM or host name, if a DNS entry can be added for the Services VM host name.
-d	Base directory to back up from, can be omitted if default value is to be used.
-D	List of directory names in CDN to be backed up, can be omitted if default value is to be used.

The following example command backs up the entire CDN to the backup server:

```
./cdnbackup.sh -Hservice_VM_IP_address
```

Note: When prompted for a password, enter the *cdn* user password. *MaaS360_Console* is the default password.

3. Check for errors, if any, after the script execution is completed.

Backup the IBM MobileFirst Protect Cloud Extender and IBM MobileFirst Protect Mobile Enterprise Gateway

IBM MobileFirst Protect Cloud Extender and IBM MobileFirst Protect Mobile Enterprise Gateway are optional, but if either one is part of your deployment they must be part of your backup and recovery plan.

The entirety of your deployment must be backed up. This is most easily accomplished by deploying them on virtual machines and including the VMs in your backup plan. VMware vSphere Data Protection is the recommended tool for managing your VM environment backup and restoration needs.

Learn About Data Retention

IBM MobileFirst Protect On-Premise stores several types of data that are rotated or purged. A retention policy must be defined to retain relevant data.

About Application Log Retention

Application logs are stored in the log directory. They are rotated after they reach 1 GB in size. Older logs are retained in the log directory and are not purged.

Application logs are accessible through the Administration Console. For more information, see “Collect Application Logs” on page 85.

About Database Table Retention

Tables that contain temporary transactional data are purged daily at midnight based on their individual predefined retention schedule.

The following table outlines the database tables that are purged during the daily cycle. The purge policy for each table is based on the nature of the data in the table. The number of retention days for each table is predefined. Data in other tables that are not listed are retained indefinitely. All the purged tables are located in the VPN2 database.

Table 8. Database tables that are purged during the daily cycle

Database Table Name	Retention Days	Table Description
SCHEMA2.USER_BULK_ENROLLMENT_OPTS	30	This table is a log of enrollment options selected by the customer during the bulk upload user workflow.
SCHEMA2.USER_BULK_ACTIVATION_OPTS	30	This table is a log of activation options selected by the customer in the bulk upload users model box.
SCHEMA2.USER_BULK_UPLOAD_OPTS	30	This table is a log of upload options used by the DB job to process the record as a part of bulk upload users workflow.
SCHEMA2.USER_BULK_UPLOAD_QUEUE	30	This table contains transient queue data used for the bulk upload users workflow. It stores a list of all users from the uploaded file in the bulk upload users workflow.
SCHEMA2.USERS_AUDIT	180	Audit of actions performed in user management.
SCHEMA2.DEVICE_LOCATION_HST	30	History of locations of device that come in through payload data.
SCHEMA2.APP_DEV_NOTIFICATION_ASSOC	30	Stores document notification sent per device.

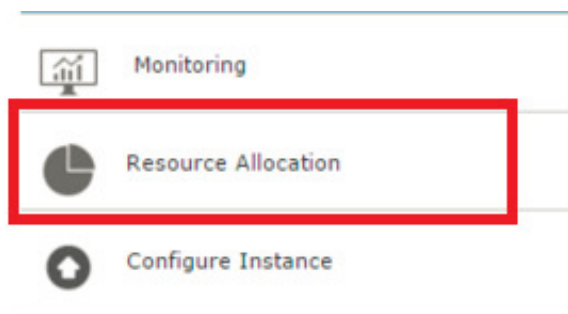
Table 8. Database tables that are purged during the daily cycle (continued)

Database Table Name	Retention Days	Table Description
SCHEMA2.APP_NOTIFICATIONS_STAGE_1	2	This table is staging table used for notification stage 1. For example, when a document is shared this would have information about a notification is to the group to which the information is being shared. Expansion of it to individual devices would be done in APP_NOTIFICATION_STAGE_2.
SCHEMA2.APP_NOTIFICATIONS_OBJECT_COUNT	2	The number of notification objects to be stored with a single notification ID.
SCHEMA2.EVT_GRP_RE_EVAL_QUEUE	15	Transient data. Stores the device and OOC group information for consumption of group evaluation hence making it faster.
SCHEMA2.APP_CATALOG_INSTALL_IOS_HST	30	Install history logs of app catalog.
DEVICE_VIEW_APP.AUTH_RESPONSE_ATTRIBUTE	30	Stores authentication tokens required for web services, etc..
DEVICE_VIEW_APP.SERVICE_AUDIT_LOG	30	Stores access logs of service URLs.

Managing Resource Allocation

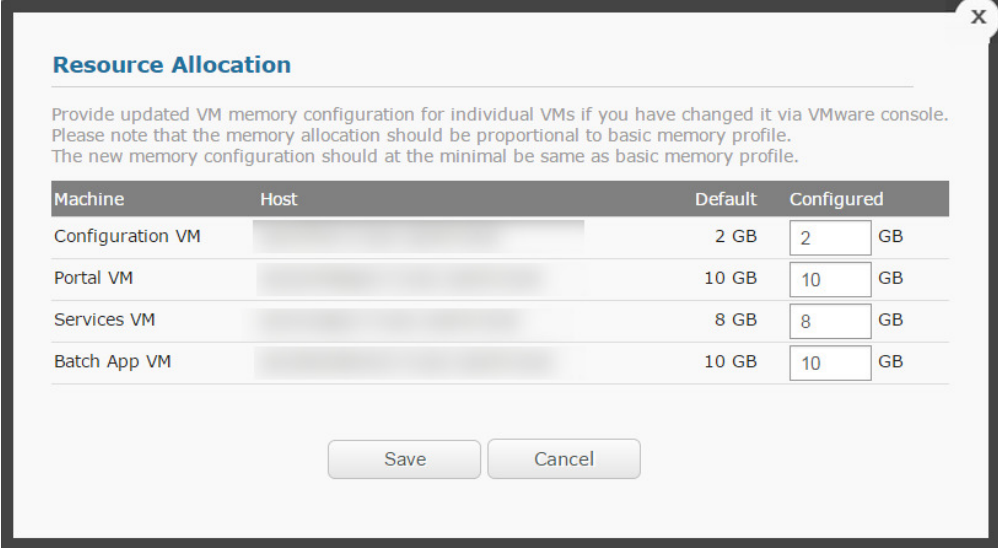
About this task

The **Resource Allocation** tab allows the configuration of memory allocated to the applications running in the IBM MobileFirst Protect On-Premise VMs. For increased scalability you have to allocate extra memory in addition to the predefined memory configuration of IBM MobileFirst Protect On-Premise VMs.



Procedure

Enter the updated VM memory value in the **Configured** field and click **Save**. You cannot enter values less than the default values.



The screenshot shows a dialog box titled "Resource Allocation" with a close button (X) in the top right corner. Below the title is a paragraph of instructions: "Provide updated VM memory configuration for individual VMs if you have changed it via VMware console. Please note that the memory allocation should be proportional to basic memory profile. The new memory configuration should at the minimal be same as basic memory profile." Below this is a table with four columns: "Machine", "Host", "Default", and "Configured". The "Configured" column has input fields for each VM. At the bottom of the dialog are "Save" and "Cancel" buttons.

Machine	Host	Default	Configured
Configuration VM		2 GB	<input type="text" value="2"/> GB
Portal VM		10 GB	<input type="text" value="10"/> GB
Services VM		8 GB	<input type="text" value="8"/> GB
Batch App VM		10 GB	<input type="text" value="10"/> GB

Note: Make sure you have already increased the memory of all VMs through VMware vCenter and then enter the new VM memory values here. The increase in memory for Portal, Services and Standalone VM pairs should be the same.

Manage Files and Downloads

After configuration, the **Downloads** tab is available in the Administration Console. It provides an interface where various apps and utilities are downloaded to support your deployment. Many of these downloads are discussed in more detail in the IBM MobileFirst Protect On-Premise Configuration Guide.



View IBM MobileFirst Protect On-Premise Apps and Agents

The **Apps and Agents** portion of the **Downloads** tab provides links to various agents and utilities. Several agents for Android and Windows Phone are available to download. In addition, the App Signing Utility for Windows Phone are available.

Note: Android apps do not require app signing.

The process of code-signing Android apps is discussed in detail in the IBM MobileFirst Protect On-Premise Configuration Guide.

The following apps and utilities are available:

Android

MaaS360 for Android

MaaS360 for Android Samsung

MaaS360 for Android LG

Secure Docs for Android

Secure Browser for Android

Secure Viewer for Android

Secure Email for Android

Secure Editor for Android

Windows Phone

MaaS360 Company Hub

Secure Docs for WP

Secure Browser for WP

Secure Email for WP 8.0+

Secure Email for WP 8.1+

Windows Phone App Signing

iOS (from the Apple iOS App Store)

MaaS360 for iOS

Secure Browser for iOS

Secure Editor for iOS

Provide the IBM MobileFirst Protect On-Premise App SDK

Applications SDKs for iOS and Android that can be integrated with enterprise apps are available. Details can be found in the IBM MobileFirst Protect On-Premise Configuration Guide.

Downloading IBM MobileFirst Protect On-Premise Optional Installers

Procedure

Use the **Downloads** tab to download these two optional installers.

- The IBM MobileFirst Protect Cloud Extender is a program that functions as a bidirectional communication portal that allows your deployment to communicate with third-party platforms such as Exchange Server. For more information, see the IBM MobileFirst Protect Cloud Extender Installation Guide.
- The IBM MobileFirst Protect Mobile Enterprise Gateway is a utility that allows behind-the-firewall access to your deployment without the need to change your network or firewall configuration. One or both of these utilities might be required depending on your deployment and the devices that are managed. For more information, see the IBM MobileFirst Protect Mobile Enterprise Gateway 2.0 Quick Start Guide.

Downloading Additional IBM MobileFirst Protect On-Premise Management Tools

Procedure

Use the **Downloads** tab to download these management tools that are available to help manage your IBM MobileFirst Protect On-Premise deployment:

Option	Description
Log Backup Tool	This utility backs up log files.
SNMP OIDs	This file contains the OIDs that can be used for SNMP monitoring.
Certificate Validation Tool	This utility allows the creation and verification of SSL certificates before deployment in your instance.
CDN Backup Tool	This utility allows the manual backup of the Content Delivery Network (CDN) content. The CDN content can be backed up separately from the Services VM backup that is part of the standard backup protocol.

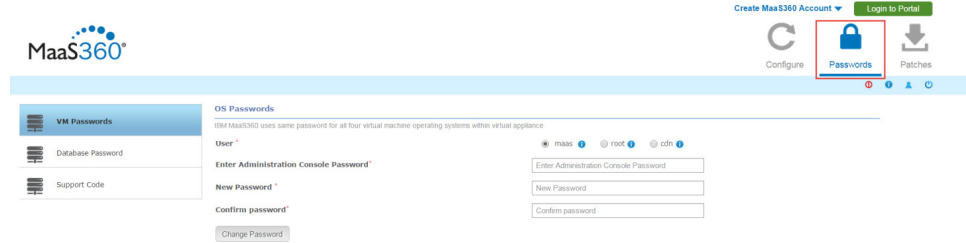
Managing Passwords

You should regularly change passwords to the VMs and the database.

Change VM Passwords

Procedure

1. Click the **Passwords** icon in the upper-right corner of the screen to manage the passwords for the operating systems of each virtual machine.
All seven of the virtual machines that are contained in the virtual appliance share the operating system password.



There are three user accounts:

- The **root** user cannot log in remotely.
- The **maas** user can log in remotely and can gain access to the root. For more information about accessing root remotely, see Chapter 19, “Appendix C: VM Shell Commands,” on page 99.
- The **cdn** user is used to back up the Content Delivery Network on the Services VM. For more information about backing up the CDN, see “Backup the CDN” on page 71.

2. Select the user whose password you want to change. Enter the new password, and click **Change Password** to update each virtual machine. You must enter your current Administration Console password as a security measure.

The default password for the root, maas, and cdn users is *MaaS360_Console*.

The operating system passwords can be changed at any time without the need to reconfigure the entire deployment.

Change the Database Password

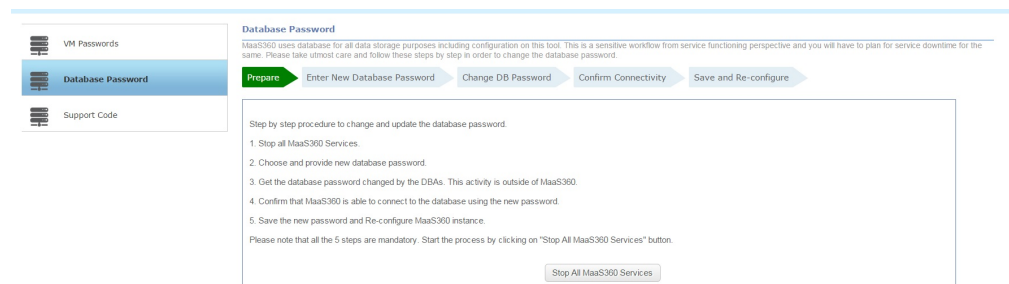
About this task

The **Database Password** wizard guides you to update the password required when connecting to IBM MobileFirst Protect On-Premise databases from IBM MobileFirst Protect On-Premise vApp.

Note: This workflow should be used whenever there is a need to update the database password. Ensure you execute this workflow before the existing database password expires.

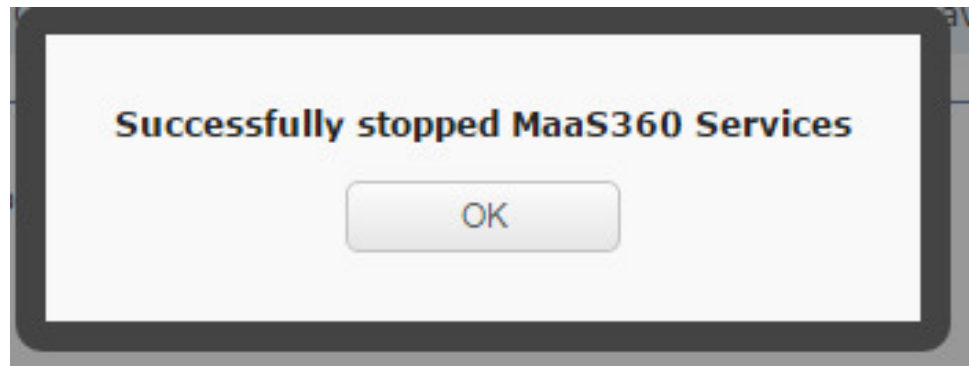
Important: This is a critical workflow and should be performed carefully. Note that this step requires restart of all application modules and has downtime implication. Plan for the downtime before executing this workflow.

The list of steps to be executed in this wizard is listed in **Prepare**. Make sure you review the steps and understand clearly what needs to be done.

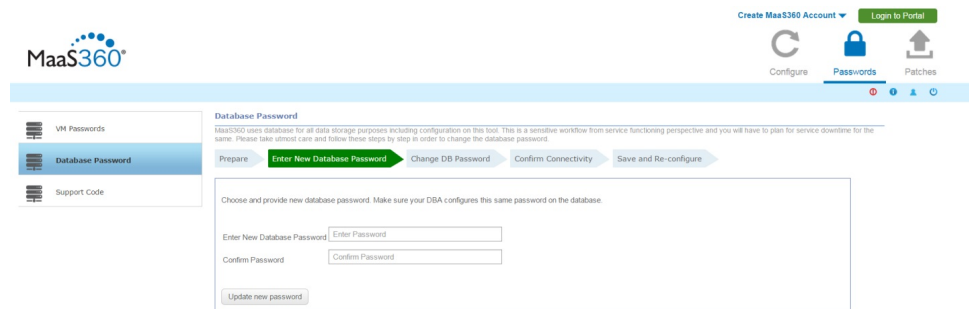


Procedure

1. Click **Stop All MaaS360 Services** to shut down all applications inside the vApp. This step takes time to complete. Please do not refresh the page till the process completes and you see the following response:

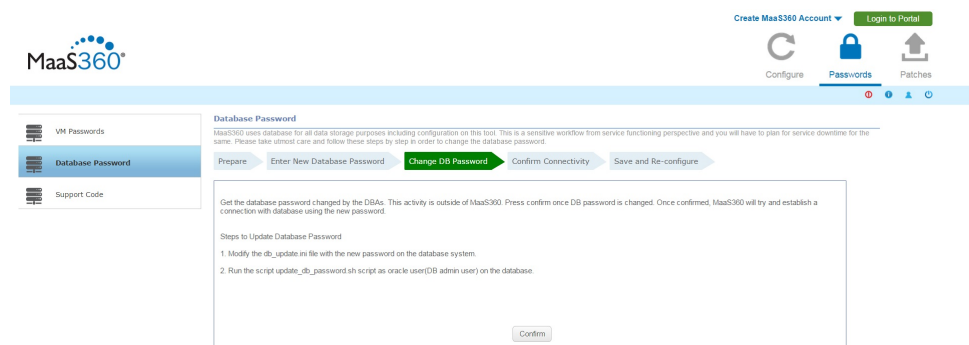


2. Click **OK** to continue.
3. Enter the new database password and click **Update new password**.



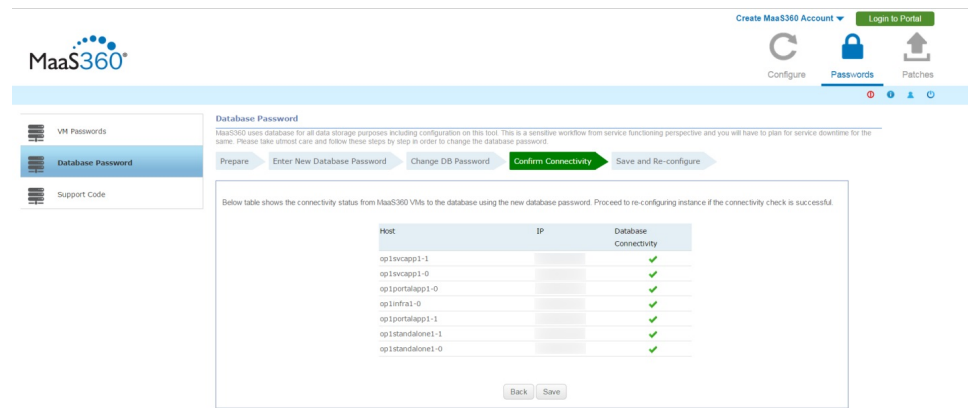
Attention: The next step must be performed outside of the IBM MobileFirst Protect On-Premise Administrative Console. Follow the steps outlined in this page to change the password for IBM MobileFirst Protect On-Premise databases. The files mentioned below are part of the database artifact. The script has to be executed on Oracle server.

4. After the password has been successfully changed at the database level click **Confirm**.



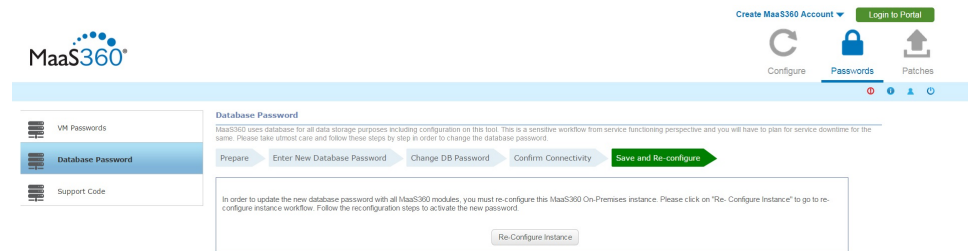
5. Confirm connectivity. A test is done to verify the database connection for all VMs in the vApp. A green checkmark indicates successful database connectivity test and a red X indicates a failure. Ensure all VMs have green checkmarks, and then click **Save**.

If there are any failures, click **Back** to go back and make corrections.



Do not refresh the page while the Save process is underway.

6. The last step applies the new database password to all the applications in the VMs, and reconfigures them to start using this new password.
7. Click **Re-Configure Instance**.



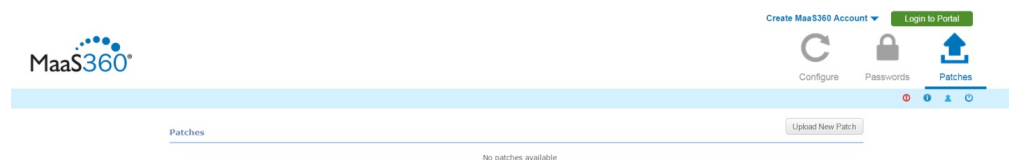
Applying Patches

FixPacks (large patches) and HotFixes (small or urgent patches) are found in the **Patches** section of the Administration Console.

About this task

Patches allow your IBM MobileFirst Protect On-Premise Mobile Device Management deployment to be modified between feature releases.

IBM can release security and functional fixes in the form of patches.



To see what patches have been applied to your deployment, do this:

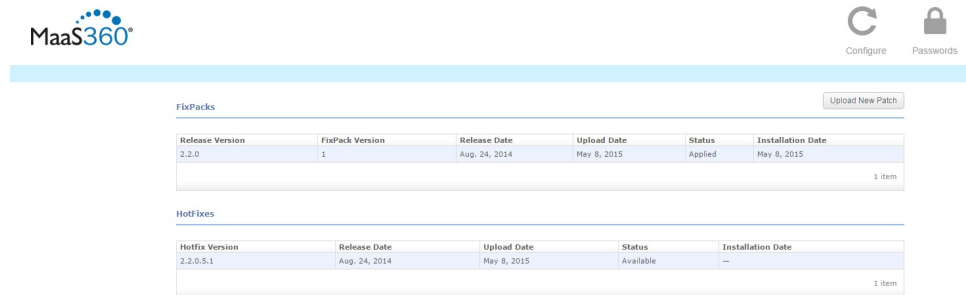
Procedure

Click the **Patches** icon in the upper-right corner of the Administration Console.

Applying patches smaller than 500MB

Procedure

1. Click the **Patches** icon in the upper-right corner of the Administration Console.
2. Click **Upload New Patch** and navigate to the location where the patch is located.
3. Select **Browser** mode, then navigate to the patch's RPM file and click **Upload**.
4. Enter the checksum provided with the patch and click **Upload**.

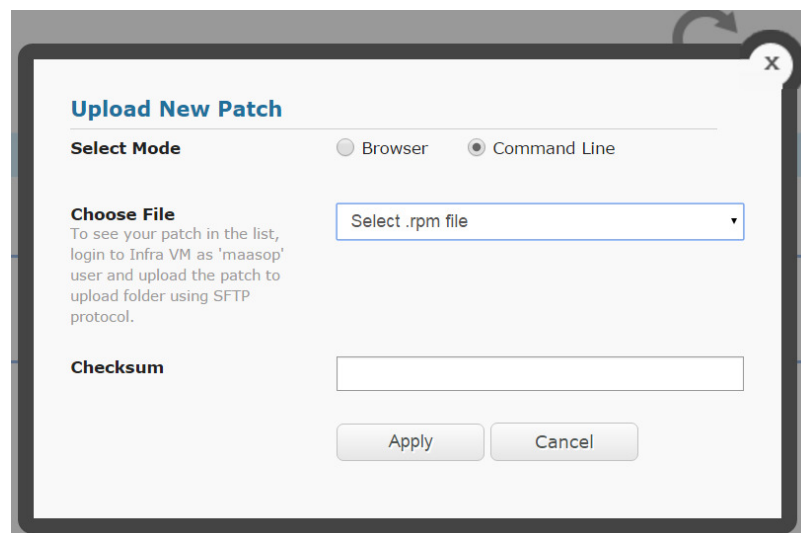


You can see the upload progress bar. The applied FixPacks and HotFixes are shown when applied.

Applying patches over 500MB

About this task

IBM MobileFirst Protect On-Premise FixPacks and HotFixes that exceed 500 MB in size should be uploaded via SFTP rather than the browser. This helps to avoid possible browser timeout errors while uploading the patch's RPM file to Configuration VM.



Procedure

1. Log in to the Configuration VM using any tool that supports the SFTP protocol.
 - Host name: Provide IP address of Configuration VM.
 - User name: maasop
 - Password: MaaS360_Console

2. Upload the patch RPM file to the /upload directory.
3. Click the **Patches** icon in the upper-right corner of the Administration Console.
4. Click **Upload New Patch** and navigate to the location where the patch is located.
5. Select **Command Line** mode, then navigate to the patch's RPM file using **Choose File**.
6. Enter the checksum provided with the patch and click **Upload**.

The screenshot shows the MaaS360 Administration Console interface. At the top left is the MaaS360 logo. At the top right are 'Configure' and 'Passwords' icons. Below the navigation bar is a table for 'FixPacks' with a '1 item' indicator. Below that is a table for 'HotFixes' with a '1 item' indicator.

Release Version	FixPack Version	Release Date	Upload Date	Status	Installation Date
2.2.0	1	Aug. 24, 2014	May 8, 2015	Applied	May 8, 2015

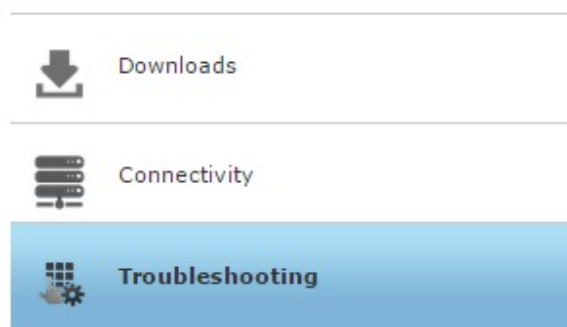
Hotfix Version	Release Date	Upload Date	Status	Installation Date
2.2.0.5.1	Aug. 24, 2014	May 8, 2015	Available	—

You can see the upload progress bar. The applied FixPacks and HotFixes are shown when applied.

Chapter 15. Troubleshooting Problems

About this task

The **Troubleshooting** tab is available after you have configured your instance. It provides an overall view of the health of your IBM MobileFirst Protect On-Premise deployment.



Audit Configuration Changes

Changes made to configuration values after initial configuration are tracked.

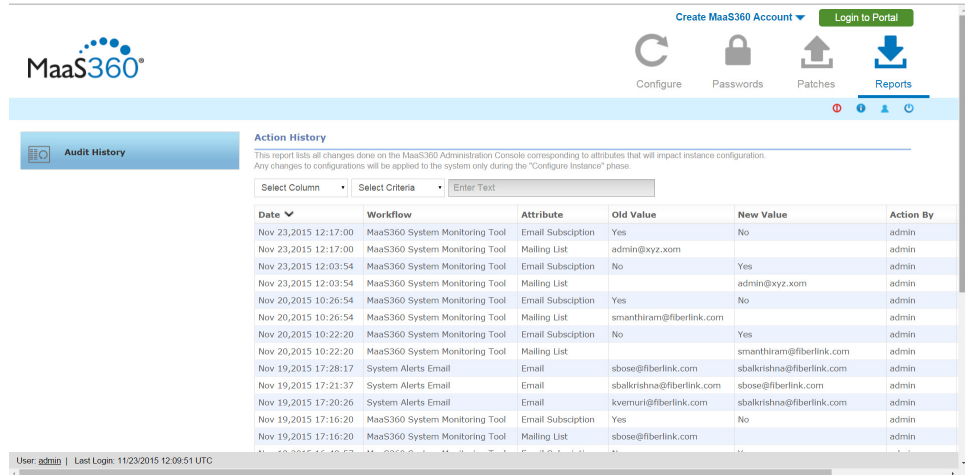
About this task

IBM MobileFirst Protect On-Premise maintains a history of all configuration changes made through the IBM MobileFirst Protect On-Premise Administration Console. The changes can be viewed as an audit report. The IP address of the computer that made the change is also displayed.

You can search and filter the data and customize the audit report for your needs. By default the audit information is sorted by date in descending order. You can sort the data by columns. Click the column header to sort by that column, and toggle ascending or descending order by clicking again.

Procedure

1. Click **Reports** in the top right corner of IBM MobileFirst Protect On-Premise Administration Console.



2. Select the desired column, criteria, and text value to filter the report.
Reset clears the filter and restores the default display.
3. Click **Customize Columns** to customize which columns are displayed.
The Status column indicates whether the changes that were made were applied or merely pending.
4. Click **Export** to download a CSV file of the audit history.

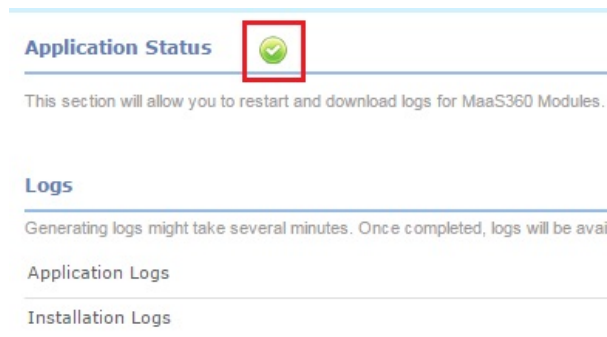
View Application Status

About this task

You can validate all the applications that are part of your IBM MobileFirst Protect On-Premise instance.

Procedure

When you access the **Troubleshooting** tab, the Administration Console conducts a health check of all web and batch applications that are part of your IBM MobileFirst Protect On-Premise deployment. This query is indicated by a spinning arrow icon.



After the health check completes, a green check mark icon is displayed showing that no problems were found. If any applications fail the health test, they are listed.

Failed applications can be handled as a group, or they can be interacted with individually in an advanced mode.

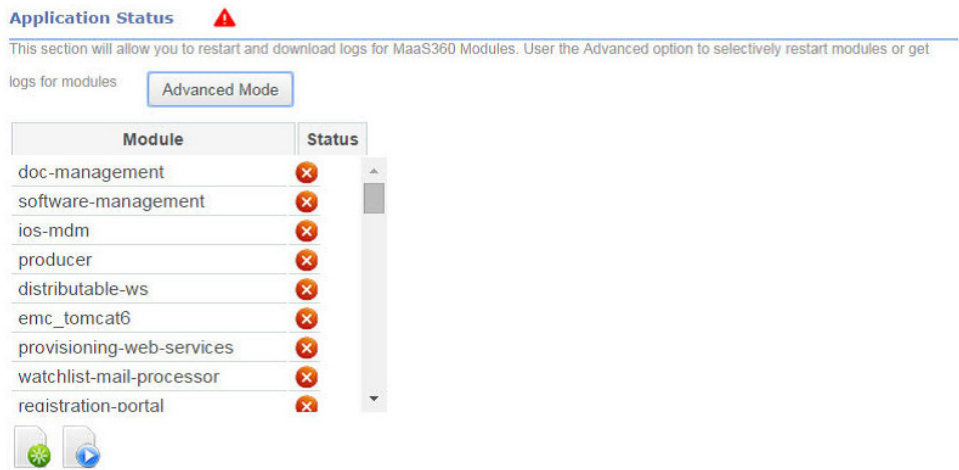
Troubleshoot in Basic Mode

About this task

Failed applications can be handled as a group when troubleshooting in basic mode:

Procedure

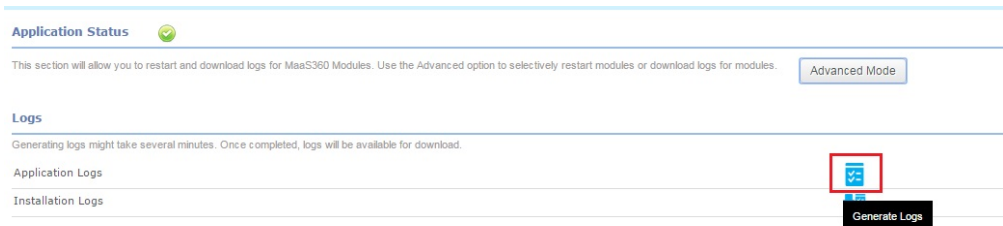
1. Generate the log files for the failed applications using the associated button. This step may take several minutes. See “Collect Application Logs” and “View Installation Logs” on page 86.
2. Use the link provided to download the generated logs and preserve them.
3. Restart the failed applications using the associated button. This process takes time. If necessary, navigate to a different tab and return to the **Troubleshooting** tab to query the applications again.
4. If applications continue to fail, generate the logs for the failed applications again, and preserve them.
5. Contact IBM Software Support.



Collect Application Logs

Procedure

Click **Generate Logs** to generate the logs.



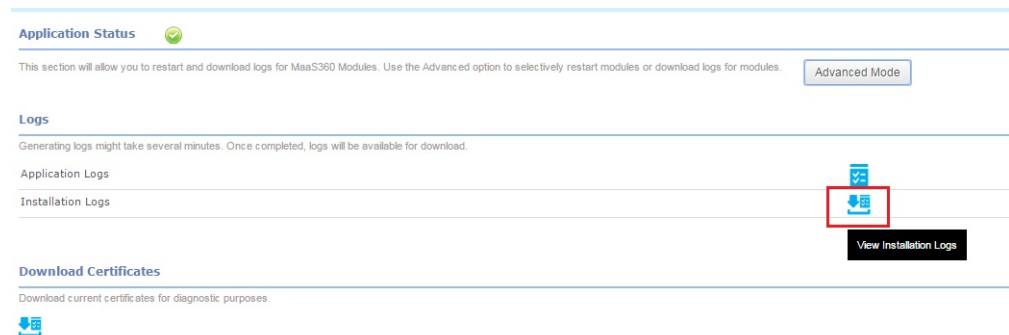


A pop-up box provides the download link.

View Installation Logs

Procedure

Click **View Installation Logs** to see them in a separate browser window.



Query the Oracle Database

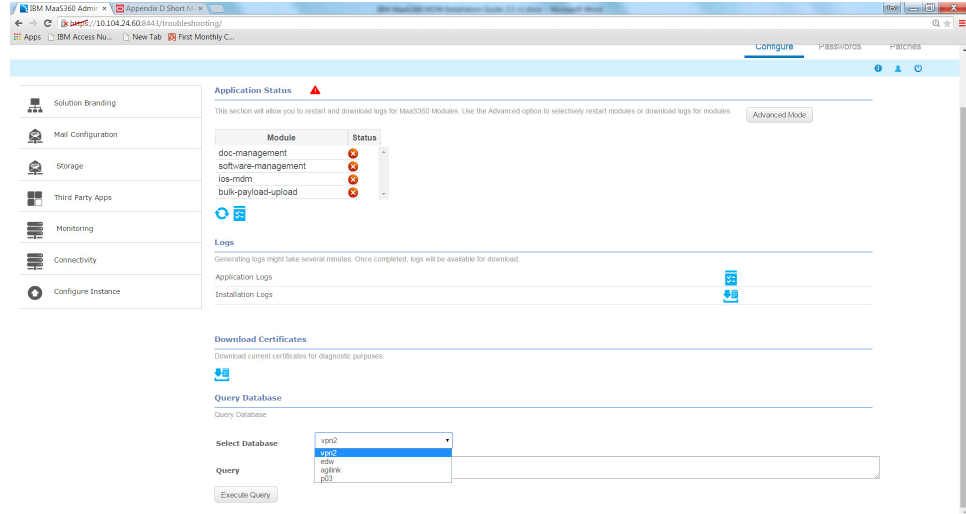
About this task

This is typically used as part of a troubleshooting session with customer support to get data that is used to debug a reported issue. The SQL queries are provided as part of the troubleshooting session.

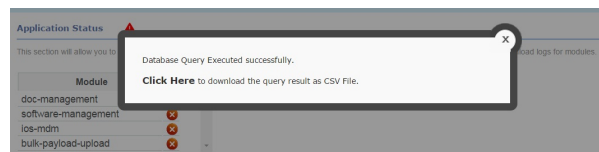
Do not run queries on your own since they may impact the system performance.

Procedure

1. Choose the database from the drop down.



2. Enter a read-only SQL query in the Query field, and click on Execute Query to execute the SQL in the database and return the results in CSV format.



Download Certificates

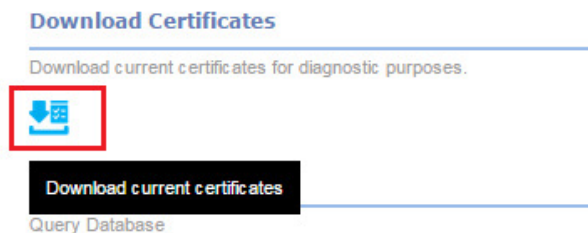
About this task

All of the certificates that are used to configure your IBM MobileFirst Protect On-Premise deployment can be downloaded for reference.

The ability to download the currently deployed certificates can be used to help determine whether the correct certificates were used.

Procedure

Select the **Troubleshooting** tab, and then click the **Download current certificates** icon.



A new browser window is opened that provides links to each certificate saved in the database.

Certificates saved in database (Download all)	
Scep Server Certificates	
Scep_Server_Root_Certificate	[blurred]
Scep_Server_Subordinate_Certificate	[blurred]
DNS Certificates	
Services	
[blurred]	[blurred]
[blurred]	[blurred]
Enrollment	
[blurred]	[blurred]
[blurred]	[blurred]
Portal	
[blurred]	[blurred]
[blurred]	[blurred]
Eup	
[blurred]	[blurred]
[blurred]	[blurred]
Security Certificates	
Apps	
[blurred]	[blurred]
Mdm	
[blurred]	[blurred]

Note: Private Key files for certificates cannot be downloaded for security reasons.

Download Configuration Summary File for Support

You can download a snapshot of the configuration information of a IBM MobileFirst Protect On-Premise instance.

About this task

The snapshot captures all the current configuration settings of the instance. It also includes:

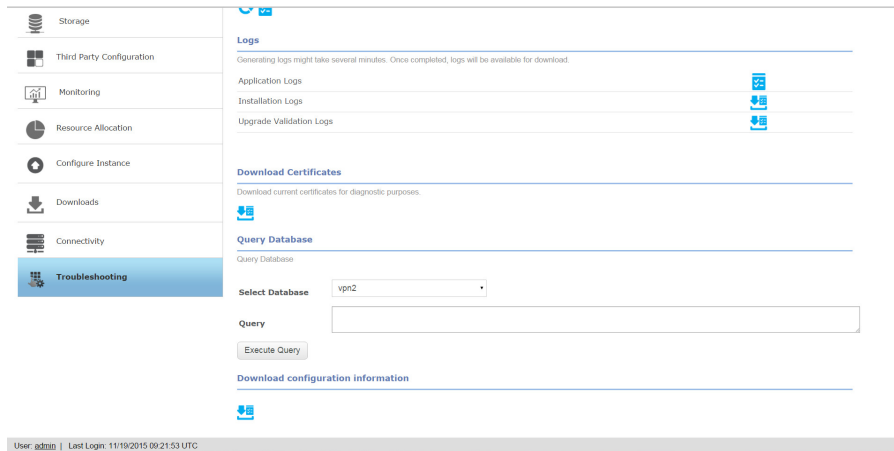
- Version numbers of the product and components
- Patch details
- System health reports

This information is used to troubleshoot issues reported to support and provides IBM with all the relevant information to initiate debugging of a reported problem.

Important: Download then provide this information to the PMR system whenever you report a problem with the IBM MobileFirst Protect On-Premise instance.

Procedure

1. Navigate to the Troubleshooting section of IBM MobileFirst Protect On-Premise Administration Console, and go to "Download configuration information" section.



2. Click the "Download configuration information." A new page opens to display the current snapshot of the configuration information.
3. Choose which sections to capture in the PDF file.
4. Click the "Generate PDF" button, then download the file from the specified URL.

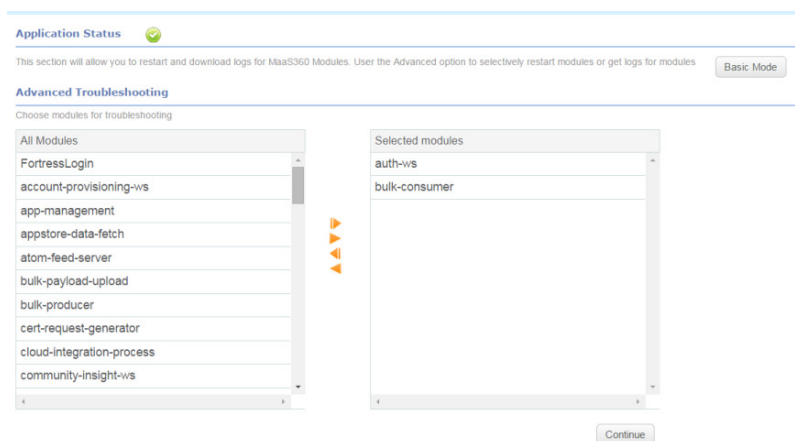
Troubleshoot in Advanced Mode

About this task

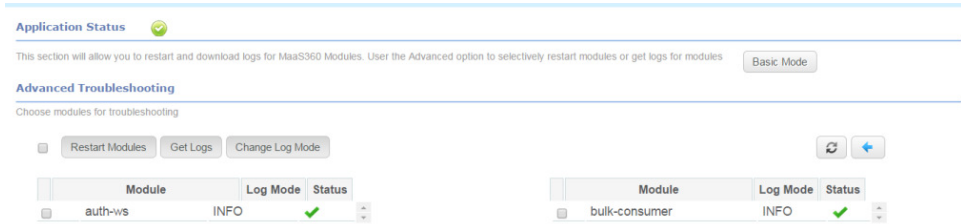
Troubleshooting in Advanced mode allows interaction with individual failed applications:

Procedure

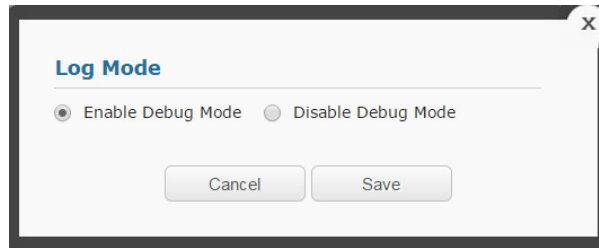
1. Select the applications that you want to troubleshoot with the arrow icons and click **Continue**.



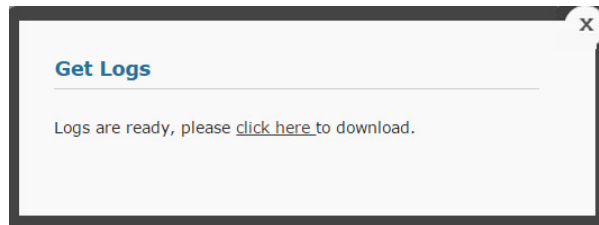
2. After the console queries the applications, select the appropriate applications by selecting the checkmark. All listed applications can be selected with the master checkbox at the top of the list.



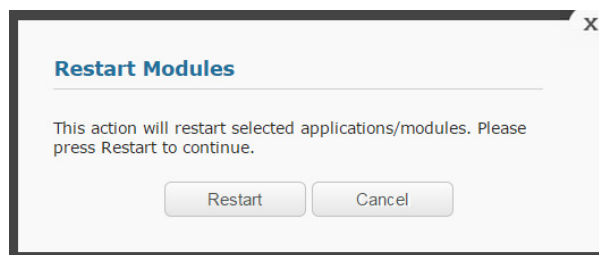
3. Click the **Change Log Mode** button and save your preference to enter or exit Debug mode.



4. Click **Get Logs** to generate the log files for the selected applications. You are prompted to download them. Save them for future reference.




5. Click **Restart Modules** to restart the selected applications.



Results

The refresh button  manually queries the applications to update their status.

The blue back button  can be used to go back a screen to select different applications.

If applications continue to fail, contact IBM Software Support and be prepared to provide the downloaded log files.

Create a Support Code

About this task

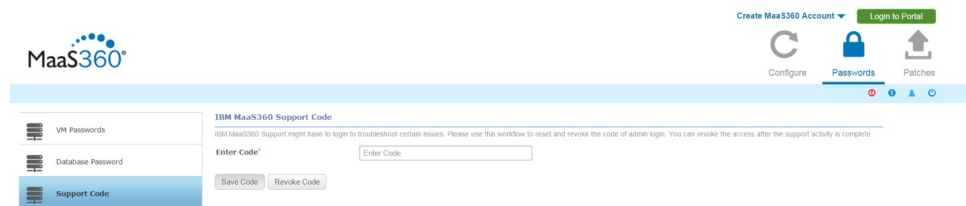
It may become necessary for IBM Support to gain access to your deployment to troubleshoot issues.

The IBM MobileFirst Protect On-Premise Support Code workflow allows you to grant temporary Portal Administration access to your IBM MobileFirst Protect On-Premise environment to IBM support. This access can be granted for a support session and can be revoked once the support session is over. The system automatically revokes the support code every hour for better security.

To enable or disable a support code, perform the following steps:

Procedure

1. From the Administration Console, access the **Passwords** tab in the upper-right corner of the UI and select **Support Code**.



2. Enter an access code provided by IBM Support in the **Enter Code** field.
3. Click **Save Code** to save and enable that access code. IBM Support can now access your IBM MobileFirst Protect On-Premise deployment.
4. After the need for remote access has passed, click **Revoke Code**. The entered code is no longer valid and IBM Support can no longer access your deployment.

Chapter 16. The Next Step

With your database deployed, the IBM MobileFirst Protect On-Premise vApp deployed, and your deployment configured using the Administration Console, you are ready to begin using the Portal to customize your deployment in preparation for managing devices.

The next step is to create an IBM MobileFirst Protect On-Premise Mobile Device Management account, if you have not done so already. This process and further steps are described in the IBM MobileFirst Protect On-Premise Configuration Guide.

Chapter 17. Appendix A: VM Internal Hostnames and IP Requirements

IBM MobileFirst Protect On-Premise is composed of seven virtual machines, which require their own static IP addresses.

The following IP entries are examples only. These examples should not be used, as is, for your environment.

Table 9. Virtual machine descriptions

Virtual Machine	Internal Hostname	Static IP	Description
Configuration VM	op1infra-0.op1.sysint.local	Static IP 1	This VM is used for deployment and administration.
Portal VM	op1portalapp1-0.op1.sysint.local op1portalapp1-1.op1.sysint.local	Static IP 2 Static IP 5	These VMs host the portal, end user portal, and enrollment URLs. These VMs run several applications and are the primary console for IBM MobileFirst Protect On-Premise administrators. These VMs also host the Enrollment service that devices use to enroll as well as the End User Portal that is accessible by users to manage their own devices.
Services and CDN VM	op1svcapp1-0.op1.sysint.local op1svcapp1-1.op1.sysint.local	Static IP 3 Static IP 6	These are the VMs through which end user devices connect. These VMs act as a gateway for device communication and API calls. They also host the Content Delivery Network that delivers content to devices.
Standalone Batch Jobs VM	op1standalone1-0.op1.sysint.local op1standalone1-1.op1.sysint.local	Static IP 4 Static IP 7	These VMs run scheduled batch jobs.

Chapter 18. Appendix B: Sample DNS Entries

Several DNS entries, Static IPs, and the natting between them must be set up.

IBM MobileFirst Protect On-Premise requires four DNS entries, one to four public IPs, and natting between the public IPs to the internal static IPs configured at the VM level.

The following DNS entries are examples only. These examples should not be used, as is, for your environment.

Note: The example below is for single-instance deployment. You have to do the correct natting when using a load balancer or reverse proxy.

Table 10. Sample DNS entries

DNS	Sample DNS	VM	Static IP	NATted Public IP	Description
Enrollments	mdm.company.com	Portal VM	Static IP 2	Public IP 1	Devices enroll into IBM MobileFirst Protect On-Premise using this URL
Portal	mdmportal.com	Portal VM	Static IP 2	Public IP 1	This URL hosts the primary portal console for device administration.
Services	mdmservices.com	Services and CDN VM	Static IP 3	Public IP 2	This URL acts as a gateway for device communication and all communications after enrollments.
EUP	mdmeup.com	Portal VM	Static IP 2	Public IP 1	This URL is the End User Portal that is accessible by users to manage their own devices.

Chapter 19. Appendix C: VM Shell Commands

IBM MobileFirst Protect On-Premise provides a command line interface (CLI) to execute frequently used commands in the virtual machines. This is a restricted shell where you can execute pre-defined commands needed for regular administration activities.

This secure shell is available in all IBM MobileFirst Protect On-Premise virtual machines, but available commands differ based on the virtual machine. You can type `help` or `?` to get a listing of available commands.

Important: Regular shell and root user access to IBM MobileFirst Protect On-Premise virtual machines is disabled.

Use an SSH client to access the secure shell with the username `maas` and corresponding password.

You see a `MaaS-SH $` prompt after you successfully log in.

To logout of secure shell type `Ctrl-D`.

Command: `startApp`

Name
startApp :: Start applications.

SYNOPSIS
startApp [OPTION]...

DESCRIPTION
This command is used to start one or more MaaS360 applications. This command needs the following mandatory arguments.

apps=[Application-Name | all]
Takes specific application name or all [Option "all" starts all MaaS360 applications]

-R [Role]
Takes a role name to execute a command on host.

-H [Hostname]
Provide IP address or hostname of a specific host to start applications deployed on that host.

Examples:

1. `$ startApp apps=dp -R dp`
This command starts dp application on respective host.
2. `$ startApp apps=all -H op1portalapp1-0.op1.sysint.local`
This command starts all applications on host op1portalapp1-0.op1.sysint.local.

Command: `stopApp`

Name
stopApp :: Stop applications.

SYNOPSIS
stopApp [OPTION]...

DESCRIPTION
This command is used to stop one or more MaaS360 applications. This command needs the following mandatory arguments.

apps=[Application-Name | all]
Takes specific application name or all [Option "all" stops all MaaS360 applications]

-R [Role]
Takes a role name to execute a command on host.

-H [Hostname]
Provide IP address or hostname of a specific host to stop applications deployed on that host

Examples:

1. `$ stopApp apps=dp -R dp`
This command stops dp application on respective host.
2. `$ stopApp apps=all -H op1portalapp1-0.op1.sysint.local`
This command stops all applications on host op1portalapp1-0.op1.sysint.local.

Command: restartApp

Name
restartApp :: Restart applications.

SYNOPSIS
restartApp [OPTION]...

DESCRIPTION
This command is used to restart one or more MaaS360 applications. This command needs the following mandatory arguments.
apps=[Application-Name | all]
Takes specific application name or all [Option "all" restarts all MaaS360 applications]
-R [Role]
Takes a role name to execute a command on host.
-H [Hostname]
Provide IP address or hostname of a specific host to restart applications deployed on that host

Examples:

1. `$ restartApp apps=dp -R dp`
This command restarts dp application on respective host.
2. `$ restartApp apps=all -H op1portalapp1-0.op1.sysint.local`
This command restarts all applications on host op1portalapp1-0.op1.sysint.local.

Command: uninstallScep

This command should only be performed during the first time deployment of the instance. Performing this step on an existing instance requires re-enrollment of all existing devices.

Name
uninstallScep :: Uninstall SCEP server or client

SYNOPSIS
uninstallScep [OPTION]...

DESCRIPTION
This command is used to uninstall the scep server or client. This command needs the following mandatory arguments.
ejbcamaster
This option uninstalls scep server.
ejbcaslave
This option uninstalls scep client.

Examples :

1. `$ uninstallScep ejbcamaster`
This command uninstalls scep server from respective host.

Command: installScep

This command should only be performed during the first time deployment of the instance. Performing this step on an existing instance requires re-enrollment of all existing devices.

Name
installScep :: Install SCEP server or client.

SYNOPSIS
installScep [OPTION]...

DESCRIPTION
This command is used to install the SCEP server or client. This command needs the following mandatory arguments.
ejbcamaster
This option installs scep server.
ejbcaslave
This option installs scep client.

Examples :
1. \$ installScep ejbcamaster
This command installs scep server on respective host.

Command: restartScep

Name
restartScep :: Restart SCEP server or client.

SYNOPSIS
restartScep [OPTION]...

DESCRIPTION
This command is used to restart the SCEP server or client. This command needs the following mandatory arguments.
ejbcamaster
This option restarts scep server.

Examples :
1. \$ restartScep ejbcamaster
This command restarts Scep scep server on respective host.

Command: startQueue

Name
startQueue :: Start message queue server.

SYNOPSIS
startQueue [OPTION]...

DESCRIPTION
This command is used to start messaging server. This command needs the following mandatory arguments.

Examples :
1. \$ startQueue
This command starts messaging server.

Command: stopQueue

Name
stopQueue :: Stop message queue server.

SYNOPSIS
stopQueue [OPTION]...

DESCRIPTION
This command is used to stop messaging server. This command needs the following mandatory arguments.

Example :
1. \$ stopQueue
This command stops messaging server.

Command: listPatches

Name
listPatches :: List all patches.

SYNOPSIS
listPatches

DESCRIPTION
This command is used to list all installed patches. This command does not take any arguments.

Example:
1. \$ listPatches

Command: getPatchLogs

Name
getPatchLogs :: Gather all patch logs.

SYNOPSIS
getPatchLogs

DESCRIPTION
This command is used to gather all patch logs. The output is placed in the /download folder under file name "patch_log.zip"

Example:
\$ 1. getPatchLogs

Command: listLogs

Name
listLogs :: List installation or upgrade or application logs.

SYNOPSIS
listLogs

DESCRIPTION
This command is used to all log files including install logs, application logs and any other validation logs.

Example:
1. \$ listLogs
This command shows list of all files from /download directory.

Command: getAppLogs

Name
getAppLogs :: Gather application logs.

SYNOPSIS
getAppLogs [OPTION]...

DESCRIPTION
This command is used to gather logs for one or more applications. This command needs the following mandatory arguments.

apps=[Application-Name | all]
Takes specific application name or all [Option "all" gathers logs for all MaaS360 applications]

-R [Role]
Takes a role name to execute a command on host.

prompt_type=[auto_dont_delete]
Turn off delete confirmation prompt

Note: Logs are available in /download directory.

Examples:
1. \$ getAppLogs apps=all -H op1portalapp1-0.op1.sysint.local
This command collects all applications logs from host op1portalapp1-0.op1.sysint.local.

2. \$ getAppLogs apps=dp -d dp
This command collects dp application logs.

Command: purgeLogs

Name
purgeLogs :: Delete logs.

SYNOPSIS
purgeLogs [OPTION]...

DESCRIPTION
This command is used to delete logs prior to a specific number of days. This command needs following arguments.

Number of days in integer
-1 : -1 option deletes all logs files.

Command: checkSysCfg

Name
checkSysCfg :: Validate and fix environment health.

SYNOPSIS
checkSysCfg [OPTION]...

DESCRIPTION
This command is used to validate the environment. This command needs the following mandatory arguments.

false
Validate environment and output result.

true
Validate environment and fix any errors.

Examples:
1. checkSysCfg true

Command: executeCfgAgent

Name

executeCfgAgent :: Execute or run configuration agent.

SYNOPSIS

executeCfgAgent [OPTION]...

DESCRIPTION

This command is used to run or execute configuration agent on all IBM MobileFirst Protect hosts. This command does not take any arguments.

Command: pingDB

Name

pingDB :: Ping database server.

SYNOPSIS

pingDB

DESCRIPTION

This command is used to ping database server. This command does not take any argument.

Chapter 20. Appendix D: SSL Certificate Password Removal

About this task

You can use commands to generate an SSL key without a password from an SSL key containing a password.

Procedure

Run the following command:

```
#old.key is SSL key with password  
#new.key is SSL key without password  
openssl rsa -in old.key -out new.key
```

Chapter 21. Appendix E: High Availability Environment

High Availability / Reverse Proxy Requirements

Some applications in IBM MobileFirst Protect On-Premise VMs send requests to each other by using the external DNS URLs.

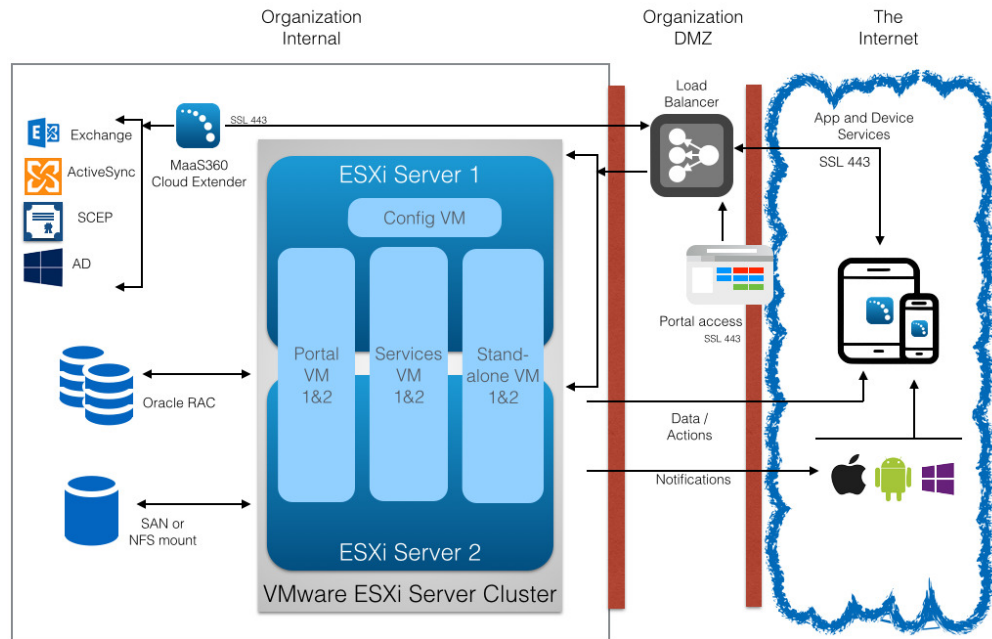
If IBM MobileFirst Protect On-Premise is integrated with an external load balancer or reverse proxy server, then IBM MobileFirst Protect On-Premise VMs need to be able to route requests to applications through the load balancer or reverse proxy. Ensure the VMs can send outgoing requests to the load balancer or reverse proxy at port 443. The IBM MobileFirst Protect On-Premise vApp should have access to the DNS Gateway needed for looking up the external DNS URL entries.

High Availability Architecture

IBM MobileFirst Protect On-Premise has the ability to configure the instance for native Active/Active High Availability. This configuration option offers customers the ability to deploy IBM MobileFirst Protect On-Premise to support environments where critical Enterprise Mobility Management services must be available at all times.

IBM MobileFirst Protect On-Premise Active/Active High Availability (HA) is achieved by leveraging inherent resilience within the architecture of IBM MobileFirst Protect On-Premise. IBM MobileFirst Protect On-Premise can support Application, Database and Server/OS resilience. Application resilience is achieved by deploying two Portal VMs, two Services VMs and two Standalone VMs and utilizing a load balancer to direct traffic to the running VMs or to a single VM in the case of a failure. Hardware resilience is achieved by deploying the IBM MobileFirst Protect On-Premise Virtual Machines across ESXi Servers in an ESXi cluster running on disparate hardware. Database resilience is achieved by deploying Oracle across at least two nodes using Real Application Clusters (RAC).

High Availability Deployment Architecture



Please refer to the *IBM MobileFirst Protect On-Premise High Availability Overview* document for more details.

Notes

- In case of non-native High Availability deployment (with four VMs), VMware High Availability (HA) and VMware Distributed Resource Scheduler (DRS) products can be utilized to provide Active/Passive high availability for IBM MaaS30.
- In addition to software license requirements, the backbone of your HA deployment is one or more ESXi servers. Each server must meet the hardware requirements described in Chapter 4, "Hardware Requirements," on page 9.
- Multiple ESXi servers must have a shared storage solution (SAN or NFS) that is part of the HA cluster. The IBM MobileFirst Protect On-Premise vApp must be deployed on this shared storage.
- The IBM MobileFirst Protect On-Premise High-Availability configuration requires familiarity with the standalone installation process and the various aspects of a successful installation including IP addressing, DNS, certificates, URLs and sizing of the instance.

Deploy the vApp in a VMware Cluster

About this task

The vApp has seven virtual machines as follows:

VM Description	VM Host Name
----------------	--------------

Configuration VM	op1infra1-0.op1.sysint.local
Portal VM	op1portalapp1-0.op1.sysint.local op1portalapp1-1.op1.sysint.local
Services and CDN VM	op1svcapp1-0.op1.sysint.local op1svcapp1-1.op1.sysint.local
Standalone Batch Jobs VM	op1standalone1-0.op1.sysint.local op1standalone1-1.op1.sysint.local

Procedure

- For a native High Availability deployment you should deploy the vApp across ESXi Servers in an ESXi cluster.

There should be a minimum of two ESXi Servers in the cluster.

Note: VMware Distributed Resource Scheduler (DRS) module is required to complete the setup explained below.

- Ensure the following are placed in the first ESXi host or host group:

- *Configuration VM*
- *Portal VM* - op1portalapp1-0.op1.sysint.local
- *Services and CDN VM* - op1svcapp1-0.op1.sysint.local
- *Standalone Batch Jobs VM* - op1standalone1-0.op1.sysint.local

- Ensure that the following are placed in the second host or host group:

- *Portal VM* - op1portalapp1-1.op1.sysint.local
- *Services and CDN VM* - op1svcapp1-1.op1.sysint.local
- *Standalone Batch Jobs VM* - op1standalone1-1.op1.sysint.local

This ensures uninterrupted availability of the VMs in case of failure of VMs on a single host or failure of the entire host.

- Ensure no 1-0 VM coexists with its corresponding 1-1 VM on the same host or host group.

To achieve this you should:

- Create a DRS-enabled VMware cluster and deploy the vApp on this cluster.
- Create two DRS cluster VM groups and place the 1-0 VMs in the first group and 1-1 VMs in the second group.
- Create two DRS cluster Host groups containing one or more distinct ESXi hosts.
- Create Rules to assign the first VM group to first host group and the second VM group to second host group.

This configuration ensures there is no single point of failure and is the recommended configuration for IBM MobileFirst Protect On-Premise native High Availability deployment.

Here is a sample configuration showing the 1-0 and 1-1 VMs placed on different ESXi hosts.

VM Name	Power State	Health
op1infra1-0.op1.sysint.local	Powered On	Normal
op1portalapp1-0.op1.sysint.local	Powered On	Normal
op1standalone1-0.op1.sysint.local	Powered On	Normal
op1svcapp1-0.op1.sysint.local	Powered On	Normal
op1portalapp1-1.op1.sysint.local	Powered On	Normal
op1standalone1-1.op1.sysint.local	Powered On	Normal
op1svcapp1-1.op1.sysint.local	Powered On	Normal

Refer to VMware's *vSphere Resource Management* for details.

Configure Network File System (NFS) Service

About this task

An NFS server used for Content Data Network (CDN) storage is mandatory for native high availability deployment.

The NFS server should be configured as follows:

Procedure

- Default NFS version should be 3 File - /etc/nfsmount.conf [Defaultvers=3]
- Export Directory/Path should have ownership as follows:
UID : 1011
GID : 1026
e.g., drwxrwxr-x 8 1011 1026 4096 Dec 2 23:58 /export/directory/path/
- In /etc/exports file, permissions should be (rw,sync,no_root_squash) for the IP addresses of Services and Standalone VMs.
e.g., /export/directory/path/ xx.xx.xx.xx(rw,sync,no_root_squash)

Note: For high availability deployment, make sure you add IP addresses of the two Services VMs and two Standalone VMs.

- IP tables/Firewall changes should be done to have Services and Standalone VMs access the NFS server at the configured port.

Note: For high availability deployment, make sure you allow access to NFS server and port for the two Services VMs and two Standalone VMs.

- Reserve minimum of 100 GB in the NFS server for each customer account created in IBM MobileFirst Protect On-Premise.

Based on actual utilization, this size is likely to vary.

Important: If the NFS server is not accessible from IBM MobileFirst Protect On-Premise for some reason, uploading and downloading applications and documents is likely to fail. After connection is reestablished please allow up to 20 minutes for applications and documents upload/download to work properly.

Chapter 22. Appendix F: System Monitoring Alerts

Alert Reference

Once the alert condition is detected, a mail alert with remediation steps is sent to subscribers within 15 minutes. Repeat alerts are sent out twice and then temporarily suspended for some time. Threshold values and alerting frequency are fixed and cannot be changed.

Note: System monitoring and alerting is suspended while patches are applied to the IBM MobileFirst Protect On-Premise instance to avoid false positives. They resume after the patch is successfully applied.

Application Alerts

Name	Description
Application Status	Alert if applications are down.
Application Memory	Alert if application memory consumption greater than 80%.

Database Alerts

Name	Description
Database Connection (number)	Alert if database connections from the virtual appliance exceed 80% capacity.
Database Connection (connectivity)	Alert if the VMs lose connectivity to the database.
Time Difference	Alert if difference in time stamp between the VMs and database exceeds 2 minutes.

Virtual Appliance Alerts

Name	Description
Disk Space Usage	Alert if disk space usage of VMS exceeds 80%.
Certificate Expiry	Alert when expiry of domain certificates occurs in 30 days.

Notices

This information was developed for products and services that are offered in the USA.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

*IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
United States of America*

For license inquiries regarding double-byte character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

*Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan*

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM websites are provided for convenience only and do not in any manner serve as an endorsement of those

websites. The materials at those websites are not part of the materials for this IBM product and use of those websites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

*IBM Corporation
2Z4A/101
11400 Burnet Road
Austin, TX 78758 U.S.A.*

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

This information is for planning purposes only. The information herein is subject to change before the products described become available.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to

IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS", without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.

Each copy or any portion of these sample programs or any derivative work, must include a copyright notice as follows:

Portions of this code are derived from IBM Corp. Sample Programs.

© Copyright IBM Corp. 2016. All rights reserved.

Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at www.ibm.com/legal/copytrade.shtml.

BYOD360™, Cloud Extender™, Control360®, E360®, Fiberlink®, MaaS360®, MaaS360® and device, MaaS360 PRO™, MCM360™, MDM360™, MI360™, Mobile Context Management™, Mobile NAC®, Mobile360®, Secure Productivity Suite™, Simple. Secure. Mobility.®, Trusted Workplace™, Visibility360®, and We do IT in the Cloud.™ and device are trademarks or registered trademarks of Fiberlink Communications Corporation, an IBM Company.

Linux is a trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.



Java™ and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Terms and conditions for product documentation

Permissions for the use of these publications are granted subject to the following terms and conditions.

Applicability

These terms and conditions are in addition to any terms of use for the IBM website.

Personal use

You may reproduce these publications for your personal, noncommercial use provided that all proprietary notices are preserved. You may not distribute, display or make derivative work of these publications, or any portion thereof, without the express consent of IBM.

Commercial use

You may reproduce, distribute and display these publications solely within your enterprise provided that all proprietary notices are preserved. You may not make derivative works of these publications, or reproduce, distribute or display these publications or any portion thereof outside your enterprise, without the express consent of IBM.

Rights

Except as expressly granted in this permission, no other permissions, licenses or rights are granted, either express or implied, to the publications or any information, data, software or other intellectual property contained therein.

IBM reserves the right to withdraw the permissions granted herein whenever, in its discretion, the use of the publications is detrimental to its interest or, as determined by IBM, the above instructions are not being properly followed.

You may not download, export or re-export this information except in full compliance with all applicable laws and regulations, including all United States export laws and regulations.

IBM MAKES NO GUARANTEE ABOUT THE CONTENT OF THESE PUBLICATIONS. THE PUBLICATIONS ARE PROVIDED "AS-IS" AND WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE.



Product Number: 5725-R11

Printed in USA