



MobileIron Cloud 74 Connector Installation Guide

October 14, 2020

For complete product documentation, see:
[MobileIron Cloud Documentation Home Page](#)

Copyright © 2009 - 2020 MobileIron, Inc. All Rights Reserved.

Any reproduction or redistribution of part or all of these materials is strictly prohibited. Information in this publication is subject to change without notice. MobileIron, Inc. does not warrant the use of this publication. For some phone images, a third-party database and image library, Copyright © 2007-2009 Aeleeeta's Art and Design Studio, is used. This database and image library cannot be distributed separate from the MobileIron product.

“MobileIron,” the MobileIron logos and other trade names, trademarks or service marks of MobileIron, Inc. appearing in this documentation are the property of MobileIron, Inc. This documentation contains additional trade names, trademarks and service marks of others, which are the property of their respective owners. We do not intend our use or display of other companies' trade names, trademarks or service marks to imply a relationship with, or endorsement or sponsorship of us by, these other companies.



Contents

Important information about this release	1
Installing and Configuring the Connector OVA	2
Requirements	2
Installing the OVA	2
System properties and SSH admin account setup	3
Final configuration settings	5
Troubleshooting a failed installation	5
Deploying MobileIron Connector in AWS	6
Obtaining the Connector AMI	6
Deploying the EC2 instance	6
Connector Requirements	8
Installing the Connector ISO Package	9
Using the Configuration Wizard	10
System Properties and SSH Admin Account Setup	10
Network Setup	11
Final Configuration Settings	12
Maintenance and Troubleshooting	14
Troubleshooting Connector registration failure	14
Starting and Stopping the Connector	14
Displaying Connector Status	15
Displaying Connector Version	15
Collecting Logs	15



Important information about this release

Important notes about MobileIron Cloud Connector version 74:

- Customers using MobileIron Cloud Connector versions earlier than version 74 **must manually install** MobileIron Cloud Connector version 74.
- After installation of MobileIron Cloud Connector version 74, MobileIron Cloud Connector automatically upgrades to new versions.
- MobileIron Cloud Connector version 74:
 - Uses CentOS 7, a change from CentOS 6.
 - **Increases the minimum disk space requirement from 20 GB to 50 GB** for the MobileIron Cloud Connector version 74 virtual machine. Attempts to install MobileIron Cloud Connector version 74 with disk space less than 50 GB will fail.

MobileIron Cloud Connector uses the increased disk capacity to add a second disk partition and to accommodate CentOS 7. The second partition makes more robust the MobileIron Cloud Connector upgrade process.



Installing and Configuring the Connector OVA

If you are **not** installing and configuring the MobileIron Cloud Connector OVA:

- Skip ahead to [Deploying MobileIron Connector in AWS on page 6](#) if you are deploying Connector in AWS.
- Skip ahead to [Connector Requirements](#) if you are **not** installing the Connector OVA and you are **not** deploying Connector in AWS.

Requirements

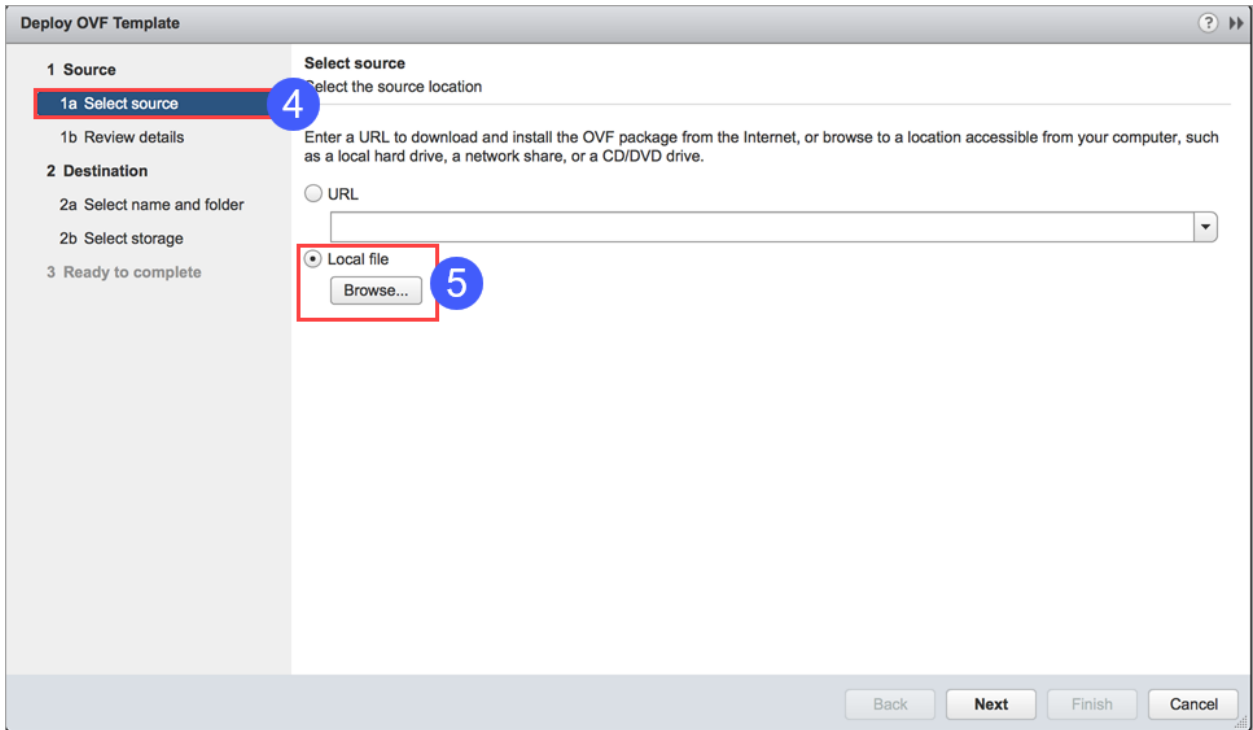
- For VMWare ESX/ESXi, use one of the following:
 - VMware ESX/ESXi 5.x, with datastore created (Do not install a host OS; boot from the Connector ISO.)
 - VMware ESX v6.5
- For Hyper-V, use one of the following:
 - Microsoft Hyper-V Server 2012
 - Microsoft Hyper-V Server 2012 R2
- 64-bit VM
- 4 GB Memory
- 50 GB Disk
- Two CPUs of 2GHz
- Network adapter (use E1000)
- VM OS Type: Red Hat Linux 5 64 bit. The OS is CentOS v7 and CentOS is a selectable option in ESX v6.0 and 6.5.
- CPU Settings: - Shares: Normal - Reservation: 900MHz - Limit: Unlimited (maximum assigned)
- Memory Settings: - Shares: Normal - Reservation: 1.5GB - Limit: Unlimited (maximum assigned)

Installing the OVA

To install the OVA:

1. Download the Connector OVA package from <https://support.mobileiron.com/cloud-connector-vm>.
2. Login into VM client.
3. Navigate to **Deploy OVF template**.
4. Select **1a Select source**.





5. Select **Local file** and browse to the ova file you downloaded in step 1.
6. Once the VM is ready, then use **launch console** to configure the following:
 - System properties/admin account settings. See [System properties and SSH admin account setup](#) for guidance.
 - Network settings. See [System properties and SSH admin account setup](#) for guidance.
 - Configuration settings. See [Final configuration settings](#).

During the configuration, you will be prompted to set the following credentials:

- privileged access: provides access to the more important Connector CLI commands
- SSH administrator: provides access to the Connector CLI basic commands

You will also need to provide the Tenant Admin credentials you received when you signed up for the device management service.

System properties and SSH admin account setup

Prompt	What to Do
End User Licensing Agreement/Terms of Use	Enter yes to accept.
Enter a privileged access password	Set a password for privileged access (6-20 alphanumeric characters).
Confirm password	Re-enter the password you just set.
Administrator user name	Enter the admin name



Prompt	What to Do
Enter administrator password	Enter the password
Confirm password	Re-enter the password you just set.
Fully qualified domain name for this system (ex: myhost.myserver.com):	Enter the fully-qualified domain name for this system.
Default domain:	Enter the default domain for this system.
Skip ip address settings. If you skip this step DHCP will be user. (yes/no)	Press <Enter>
IP Address	Enter the IP address for this system.
Netmask:	Enter the subnet mask associated with the IP address you just entered.
Skip dns server setting. If you skip this step default DNS servers will be used. (yes/no) [no]:	Press <Enter>
Default gateway address:	Enter the default gateway address for this system
DNS name server 1 address:	Enter the IP address for a DNS name server.
DNS name server 2 address:	Enter the IP address of another name server, or press Enter "none" and go to step 9 if you have finished entering name servers.
DNS name server 3 address:	Enter the IP address of another name server, or press Enter if you have finished entering name servers.
Enable remote shell access via SSH (yes/ no):	Enter yes to enable SSH access.
Enable the NTP service (yes/no):	Enter yes to enable the optional NTP service and begin specifying time sources.
NTP server 1 hostname or address:	Enter the hostname or IP address of a time source.
NTP server 2 hostname or address:	Enter the hostname or IP address of another time source, or press Enter and go to step 15 if you are finished entering time sources.



Prompt	What to Do
NTP server 3 hostname or address:	Enter the hostname or IP address of another NTP server, or press Enter "if you are finished entering NTP servers
Specify an HTTP proxy (yes/no):	Enter yes to set up an HTTP proxy or enter no to skip this step.
Enter a time in 24 hour format in UTC timezone to	Enter the time at which you would like the service to check for Connector software updates. Example, to specify 2 pm as the time to check for updates, enter 14:00. If updates are found, they will be applied automatically.

Final configuration settings

Prompt	What to do
Apply this configuration?	Enter yes. The settings you entered are applied. After several minutes, a SUCCESS message indicates that Connector installation is complete. Next, the Connector registration process begins.
Enter your Tenant Admin Username:	Enter the Tenant Admin username you received when you signed up for the device management service.
Password:	Enter the Tenant Admin password.

Troubleshooting a failed installation

If Connector registration fails, the following message displays:

You must register this Connector. You may do this at any time by running the following command (You will be prompted for your Tenant Admin Credentials): Confirm your Tenant Admin credentials and restart the registration process with the following steps: 1. Enter the following command: 2. enable 3. Enter the privileged password you set. 4. Enter the following command if you are ready to register your Connector: connector register

See [Maintenance and Troubleshooting](#) for useful troubleshooting commands and techniques.



Deploying MobileIron Connector in AWS

If you are not installing the MobileIron Cloud Connector on AWS, skip ahead to [Connector Requirements](#).

Deploying the MobileIron Connector in AWS involves the following steps:

- [Obtaining the Connector AMI](#)
- [Deploying the EC2 instance](#)

Obtaining the Connector AMI

To obtain the Connector AMI, contact your MobileIron Support representative with the following AWS information:

- AWS Account
- AWS Region

MobileIron will share the Connector AMI with your AWS account and notify you through your Support representative.

Deploying the EC2 instance

Note: AMI must be shared with customer before performing this step.

To deploy the EC2 instance:

1. Open the Amazon EC2 console at <https://console.aws.amazon.com/ec2/>.
2. From the console dashboard, choose **Launch Instance**.
3. Choose the Amazon Machine Image (AMI) you obtained as described in [Obtaining the Connector AMI on page 6](#).
4. On the **Choose an Instance Type** page, select the **t2.medium** type.
5. Choose **Review and Launch** to let the wizard complete the other configuration settings for you.
6. On the **Review Instance Launch page**, under **Security Groups**, you'll see that the wizard created and selected a security group for you. You can use this security group, or alternatively you can select the security group that you created when getting set up using the following steps:
 - a. Choose **Edit security groups**.
 - b. On the **Configure Security Group** page, ensure that **Select an existing security group** is selected.
 - c. Select your security group from the list of existing security groups, and then choose **Review and Launch**.
7. On the **Review Instance Launch** page, under **Tags**:
 - a. Choose **Edit Tags**.
 - b. Choose **Add Tag**.
 - c. In the Key field, type **Name**.
 - d. In the Value field, type **Mobileiron-connector**.
 - e. Choose **Review and Launch**.
8. On the **Review Instance Launch** page, choose **Launch**.



9. When prompted for a key pair, select **Choose an existing key pair**, then select the key pair that you created earlier.
Alternatively, you can create a new key pair. Select **Create a new key pair**, enter a name for the key pair, and then choose **Download Key Pair**.
10. This is the only chance for you to save the private key file, so be sure to download it. Save the private key file in a safe place. You'll need to provide the name of your key pair when you launch an instance and the corresponding private key each time you connect to the instance.

Note: Don't select the Proceed without a key pair option. If you launch your instance without a key pair, then you can't connect to it.

11. When you are ready, select the **acknowledgement** check box, and then choose **Launch Instances**. A confirmation page lets you know that your instance is launching.
12. Choose **View Instances** to close the confirmation page and return to the console.
On the Instances screen, you can view the status of the launch. It takes a short time for an instance to launch. When you launch an instance, its initial state is pending. After the instance starts, its state changes to running and it receives a public DNS name. (If the Public DNS (IPv4) column is hidden, choose **Show/Hide Columns** (the gear-shaped icon) in the top right corner of the page and then select **Public DNS (IPv4)**.)
13. It can take a few minutes for the instance to be ready so that you can connect to it. View the **Status Checks** column to see if your instance has passed its status checks.
14. SSH to the newly-created instance using the user name: operations.
Setup starts and displays the End User License Agreement (EULA).
15. Accept the EULA and proceed.
A privileged access password is required for protected access to privileged commands.
16. Enter a privileged access password.
17. Confirm the password.
18. Enter the Administrator user name: miadmin
19. Enter an administrator password.
20. Confirm the password.
21. Skip the IP address settings so that DHCP is used.

Note: Do not skip to provide DNS servers info.

22. On following screen, enter the DNS servers information, making sure not to use the default settings.

For more information about the configuration wizard, see: [Using the Configuration Wizard](#).



Connector Requirements

- For VMWare ESXi, use:
 - VMWare ESXi v 6.0 and 6.5
- For Hyper-V, use one of the following:
 - Microsoft Hyper-V Server 2012
 - Microsoft Hyper-V Server 2012 R2
- 64-bit VM
- 4 GB Memory
- 50 GB Disk
- Two CPUs of 2GHz
- Network adapter (use E1000)
- VM OS Type: Red Hat Linux 5 64 bit. The OS is CentOS v7 and CentOS is a selectable option in ESXi v6.0 and 6.5
- CPU Settings:
 - Shares: Normal
 - Reservation: 900MHz
 - Limit: Unlimited (maximum assigned)
- Memory Settings:
 - Shares: Normal
 - Reservation: 1.5GB
 - Limit: Unlimited (maximum assigned)



Installing the Connector ISO Package

After the VM environment is set up, you can install the Connector ISO package.

1. Log in to the VM Client.
2. In the directory tree on the left, right-click the device on which you want to install the package.
3. Select Edit Settings from the drop-down menu.
4. Select CD/DVD Drive 1.
5. Make sure that Datastore ISO File is selected.
6. Click Browse and navigate to the directory where the ISO package is kept.
7. Select the ISO package.
8. Click Open to return to the VM Properties screen.
9. Click OK to return to the previous screen.
10. Right-click the device on which the package is to be installed.
11. Select Power, then Reset.
12. Click Yes to reset the virtual machine.
13. Observe the status messages at the bottom of the screen.
14. Click the Console tab.

The following screen appears after the ISO package is installed:

```
Welcome to the Connector Installation Program
```

To install the Connector, type:

```
install<ENTER>
```

To boot from your local hard disk, type: <ENTER>

Note: System will boot from the local hard disk if no key is pressed.

15. Type install.
16. Press Enter.
17. The CentOS installation begins and might take several minutes.
18. When prompted, press Enter to log in.

The Configuration Wizard starts.



Using the Configuration Wizard

The Configuration Wizard starts after the ISO package is installed. Use the Configuration Wizard to set the following:

- system properties/admin account
- network settings
- final configuration settings

During the configuration, you will be prompted to set the following credentials:

- privileged access: provides access to the more important Connector CLI commands
- SSH administrator: provides access to the Connector CLI basic commands

You will also need to provide the Tenant Admin credentials you received when you signed up for the device management service.

System Properties and SSH Admin Account Setup

	Prompt	What to Do
1	Welcome to the MobileIron Configuration Wizard Use the “-“ character to move back to a previous field. Proceed with system configuration (yes/no):	Enter yes.
2	End User Licensing Agreement	Enter yes to accept.
3	Enter a privileged access password:	Set a password for privileged access (6-20 alphanumeric characters).
4	Confirm password	Re-enter the password you just set.



Network Setup

	Prompt	What to Do
1	Fully qualified domain name for this system (ex: myhost.myserver.com):	Enter the fully-qualified domain name for this system.
2	Default domain:	Enter the default domain for this system.
3	IP address:	Enter the IP address for this system.
4	Netmask:	Enter the subnet mask associated with the IP address you just entered.
5	Default gateway address:	Enter the default gateway address for this system
6	DNS name server 1 address:	Enter the IP address for a DNS name server.
7	DNS name server 2 address:	Enter the IP address of another name server, or press Enter "none" and go to step 9 if you have finished entering name servers.
8	DNS name server 3 address:	Enter the IP address of another name server, or press Enter if you have finished entering name servers.
9	Enable remote shell access via SSH (yes/no):	Enter yes to enable SSH access.
10	Enable the NTP service (yes/no):	Enter yes to enable the optional NTP service and begin specifying time sources.
11	NTP server 1 hostname or address:	Enter the hostname or IP address of a time source.
12	NTP server 2 hostname or address:	Enter the hostname or IP address of another time source,



	Prompt	What to Do
		or press Enter and go to step 15 if you are finished entering time sources.
13	NTP server 3 hostname or address:	Enter the hostname or IP address of another NTP server, or press Enter "if you are finished entering NTP servers
14	Specify an HTTP proxy (yes/no):	Enter yes to set up an HTTP proxy or enter no to skip this step.
15	Enter a time in 24 hour format in UTC timezone to check for software updates daily	<p>Enter the time at which you would like the service to check for Connector software updates.</p> <p>Example, to specify 2 pm as the time to check for updates, enter 14:00.</p> <p>If updates are found, they will be applied automatically.</p>

Final Configuration Settings

The settings you just entered are displayed.



	Prompt	What to Do
1	Apply this configuration?	Enter yes. The settings you entered are applied. After several minutes, a SUCCESS message indicates that Connector installation is complete. Next, the Connector registration process begins.
2	Enter your Tenant Admin Username:	Enter the Tenant Admin username you received when you signed up for the device management service.
3	Password:	Enter the Tenant Admin password.
4	Registration Successful!	



Maintenance and Troubleshooting

Troubleshooting and maintenance involves such activities as:

- [Troubleshooting Connector registration failure](#)
- [Starting and Stopping the Connector](#)
- [Displaying Connector Status](#)
- [Displaying Connector Version](#)
- [Collecting Logs](#)

Troubleshooting Connector registration failure

If Connector registration fails, the following message displays:

```
You must register this Connector. You may do this at any time by running the following command (You will be prompted for your Tenant Admin Credentials):
```

Confirm your Tenant Admin credentials and restart the registration process with the following steps:

1. Enter the following command:

```
enable
```

2. Enter the privileged password you set.
3. Enter the following command if you are ready to register your Connector:

```
connector register
```

Starting and Stopping the Connector

To stop the Connector service:

1. Enter the following command:

```
enable
```
2. Enter the privileged password you set.
3. Enter the following command:

```
connector stop
```

To start the Connector service:

1. Enter the following command:

```
enable
```
2. Enter the privileged password you set.
3. Enter the following command:

```
connector start
```



Displaying Connector Status

To display Connector status, enter the following command:

```
status connector
```

Displaying Connector Version

To display the version of the Connector, enter the following command:

```
show version
```

Collecting Logs

If your Support Representative requests Connector logs, use the following command:

```
connector log upload <user> <server>
```

where

<user> is the name of a user with access to the specified host.

<server> is the IP address (such as 10.10.10.10) or host name of a server (myserver.mycompany.com) that can receive the log via SCP.

The log is placed in the home directory of the specified host.

