



Ivanti Neurons for MDM Connector 80 - 95 Installation Guide

February 2024

Contents

Revision history	3
Latest available versions	4
New features summary	5
Related information from previous releases	5
Resolved issues	6
Related information from previous releases	6
Known issues	7
Related information from previous releases	7
Limitations	8
Related information from previous releases	8
Installing and Configuring the Connector OVA	9
Requirements	9
Installing the OVA	10
Troubleshooting a failed installation	13
Deploying Connector in AWS	14
Deploying the EC2 instance	14
Connector Requirements	17
Installing the Connector ISO Package	19
Using the Configuration Wizard	21
System Properties and SSH Admin Account Setup	22
Network Setup	23
Final Configuration Settings	25
Upgrading the Connector	26
OVA and AMI-based Connector	26
ISO-based Connector	27
Maintenance and Troubleshooting	28
Troubleshooting Connector registration failure	28
Starting and Stopping the Connector	28
Displaying Connector Status	29
Displaying Connector Version	29
Collecting Logs	29

Revision history

TABLE 1. REVISION HISTORY

Date	Revision
February 9, 2024	Updated for Ivanti Neurons for MDM Connector 95: <ul style="list-style-type: none"> • "Latest available versions" on the next page • " New features summary" on page 5 • "Resolved issues" on page 6 • "Limitations" on page 8 • "Upgrading the Connector" on page 26
December 18, 2023	Updated for Ivanti Neurons for MDM Connector 93: <ul style="list-style-type: none"> • " New features summary" on page 5 • "Resolved issues" on page 6
July 18, 2023	Updated for patch release 87.0.0.81
June 2, 2023	Updated for Ivanti Neurons for MDM Connector 87: <ul style="list-style-type: none"> • " New features summary" on page 5 • "Limitations" on page 8
March 8, 2023	Added information about "Latest available versions" on the next page.
July 9, 2022	Re-branded Cloud as Ivanti Neurons for MDM.
April 22, 2022	<ul style="list-style-type: none"> • Updated for Ivanti Neurons for MDM 83. Ivanti Neurons for MDM 81 and 82 Connectors were not released for general availability. • Added Microsoft Hyper-V Server 2016.
December 9, 2021	Updated for Ivanti Neurons for MDM 81, including instructions for T3 instance support.

Latest available versions

- **AWS AMI:** mobileiron-kocab-95.0.0-2.us-east-1 ami
Available on the **Images > AMIs** page of the AWS EC2 Management Console by searching Public Images for "mobileiron-kocab." For example, [this link](#).
- **ISO:** 95.0.0.2
Available at <http://support.mobileiron.com/cloud-connector/current/connector-LATEST.zip>. This site requires credentials available from Ivanti Support.
- **OVA:** 95.0.0.2
Available at <https://support.mobileiron.com/cloud-connector-vm>. This site requires credentials available from Ivanti Support.

New features summary

These are cumulative release notes. If a release does not appear in this section, then there were no associated new features and enhancements.

Ivanti Neurons for MDM Connector 95 - New features summary

- **Security fix:** The current release provides important security features and is recommended for all users.

Related information from previous releases

Click [here](#) to see the HTML version of this guide which contains related new features information from previous releases, if any.

Resolved issues

These are cumulative release notes. If a release does not appear in this section, then there were no associated resolved issues.

Ivanti Neurons for MDM Connector 95 - Resolved issues

- **AW-70957:** Starting with this release, the error notifications will now display for Connector registration failures from CLI.

Related information from previous releases

Click [here](#) to see the HTML version of this guide which contains related resolved issues information from previous releases, if any.

Known issues

These are cumulative release notes. If a release does not appear in this section, then there were no associated known issues.

Related information from previous releases

Click [here](#) to see the HTML version of this guide which contains related known issues information from previous releases, if any.

Limitations

These are cumulative release notes. If a release does not appear in this section, then there were no associated limitations.

Ivanti Neurons for MDM Connector 95 - Limitations

Previous Connector version limitation: The update includes security fixes that require a reboot to apply Kernel patches when the Connector upgrades to 95.0.0.x. For more information, see "[Upgrading the Connector](#)" on page 26.

Related information from previous releases

Click [here](#) to see the HTML version of this guide which contains related limitations information from previous releases, if any.

Installing and Configuring the Connector OVA

If you are **not** installing and configuring the Ivanti Neurons for MDM Connector OVA:

- Skip ahead to "[Deploying Connector in AWS](#)" on page 14 if you are deploying Connector in AWS.
- Skip ahead to "[Connector Requirements](#)" on page 17 if you are **not** installing the Connector OVA and you are **not** deploying Connector in AWS.

Requirements

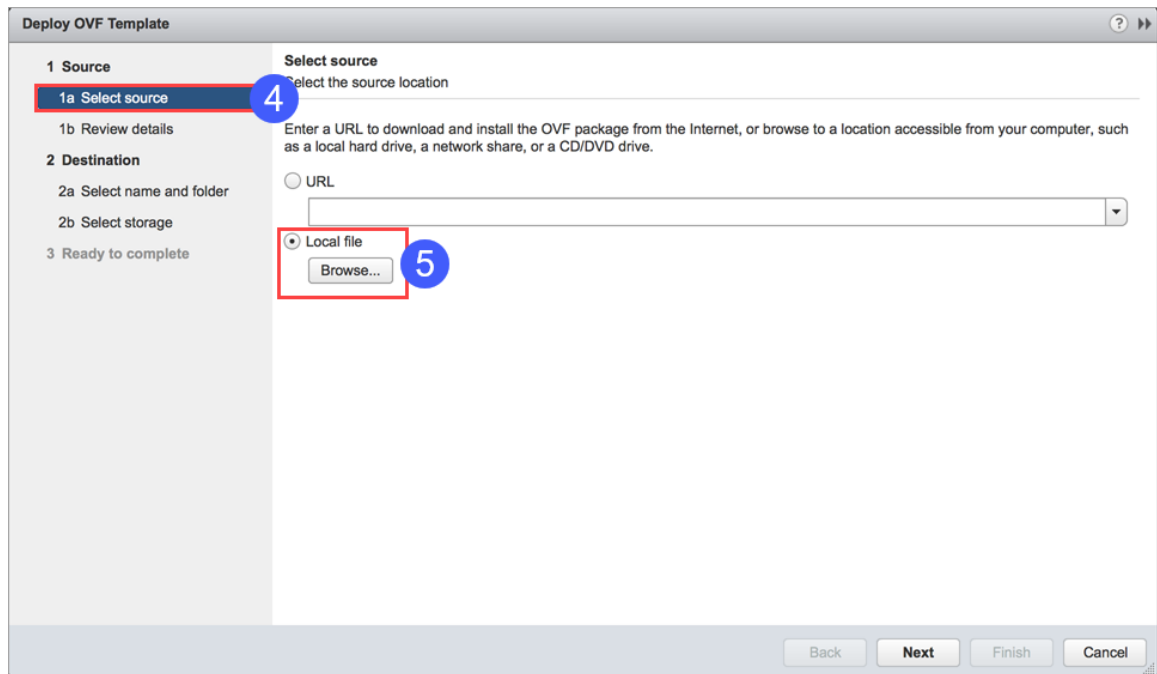
- For VMware ESX/ESXi, use one of the following:
 - VMware ESX/ESXi 5.x, with datastore created (Do not install a host OS; boot from the Connector ISO.)
 - VMware ESX v6.5 or 7.0.
- For Hyper-V, use one of the following:
 - Microsoft Hyper-V Server 2012
 - Microsoft Hyper-V Server 2012 R2
 - Microsoft Hyper-V Server 2016
- 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, 6.5, and 7.0.
- CPU Settings: - Shares: Normal - Reservation: 900MHz - Limit: Unlimited (maximum assigned)
- Memory Settings: - Shares: Normal - Reservation: 1.5GB - Limit: Unlimited (maximum assigned)

Installing the OVA

Install the OVA as follows:

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](#)" below for guidance.
- Network settings. See "[System properties and SSH admin account setup](#)" below for guidance.
- Configuration settings. See "[Final configuration settings](#)" on page 13.

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
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.

Prompt	What to Do
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.
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 in24 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](#)" on page 28 for useful troubleshooting commands and techniques.

Deploying Connector in AWS

If you are not installing the Ivanti Neurons for MDM Connector on AWS, skip ahead to "[Connector Requirements](#)" on page 17.

Deploying the EC2 instance

To deploy the EC2 instance:

1. Log in to AWS with administrator credentials.
2. On the AWS services page, select **EC2** under **Compute**.
3. Expand Images and select **AMIs** in the left pane.
4. Select **Public Images** from the drop-down list in the right pane.
5. Search for the Ivanti Neurons for MDM Connector using keywords such as "MobileIron," "Cloud Connector."
6. Select the latest version of the connector from the list.
7. From the console dashboard, choose **Launch Instance**.
8. On the **Choose an Instance Type** page, select the **t2.medium** or **t3.medium** type. t3 type supported with Connector version 81 and later.
9. Choose **Review and Launch** to let the wizard complete the other configuration settings for you.
10. 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:
11. Choose **Edit security groups**.
12. On the **Configure Security Group** page, ensure that **Select an existing security group** is selected.

13. Select your security group from the list of existing security groups, and then choose **Review and Launch**.
 - a. On the **Review Instance Launch** page, under **Tags**:
 - b. Choose **Edit Tags**.
 - c. Choose **Add Tag**.
 - d. In the Key field, type **Name**.
 - e. In the Value field, type **Mobileiron-connector**.
14. Choose **Review and Launch**.
15. On the **Review Instance Launch** page, choose **Launch**.
16. When prompted for a key pair, select **Choose an existing key pair**, then select the key pair that you created earlier.
17. 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**.
18. 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.



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

19. 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.
20. Choose **View Instances** to close the confirmation page and return to the console.
21. 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)**.)

22. 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.
23. SSH to the newly-created instance using the user name: operations.
Setup starts and displays the End User License Agreement (EULA).
24. Accept the EULA and proceed.
A privileged access password is required for protected access to privileged commands.
25. Enter a privileged access password.
26. Confirm the password.
27. Enter the Administrator user name: miadmin
28. Enter an administrator password.
29. Confirm the password.
30. Skip the IP address settings so that DHCP is used.



Do not skip to provide DNS servers info.

31. 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" on page 21](#).

Connector Requirements

These are the requirements:

- For VMware ESXi, use:
 - VMware ESXi v6.0, 6.5, and 7.0
- For Hyper-V, use one of the following:
 - Microsoft Hyper-V Server 2012
 - Microsoft Hyper-V Server 2012 R2
 - Microsoft Hyper-V Server 2016
- 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, 6.5, and 7.0.
- 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.

	Prompt	What to Do
12	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.
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	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

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!	

Upgrading the Connector

The update includes security fixes, which require a reboot to apply kernel patches if the Connector is upgraded to 95.0.0.4. To check the Connector version in the **Admin Console**, navigate to **Admin > Infrastructure > Connector**.

Prerequisite: The suggested minimum version of the Connector is 95.0.0.4.

Procedure:

If you have configured DHCP and have manually specified DNS server settings during the initial setup, a Connector reboot following the update to 95.0.0.4 will discard the manually specified DNS server settings. It results in an unrecoverable state caused by the unresolvable DNS settings. Create a new Connector to resolve this with the following steps:

1. ["Installing and Configuring the Connector OVA" on page 9](#)
2. ["Deploying Connector in AWS" on page 14](#)
3. ["Installing the Connector ISO Package" on page 19](#)

If you have configured DHCP but have not manually specified the DNS server addresses, or if you have not used DHCP at all and have manually configured the IP address and DNS servers during the initial setup, follow the steps to update the Kernel after the Connector auto-upgrades to v95.0.0.4:

OVA and AMI-based Connector

1. SSH to the Connector instance using the Connector administrator user.
2. Enter the following command:

```
enable
```

3. Enter the privileged password that was set previously to configure the Connector.
4. Enter the following command to stop the Connector:

```
connector stop
```

5. Enter the following command to start the Connector:

```
connector start
```

6. Enter the following command to reboot the Connector:

```
reload
```

ISO-based Connector

1. SSH to the Connector instance using the Connector administrator user.

2. Enter the following command:

```
enable
```

3. Enter the privileged password that was set previously to configure the Connector.

4. Enter the following command to reboot the Connector:

```
reload
```



If you want to re-configure the Connector, you should wait for an hour after reboot. Repeat the steps for each Connector as required.

Maintenance and Troubleshooting

Troubleshooting and maintenance involves such activities as:

- ["Troubleshooting Connector registration failure" below](#)
- ["Starting and Stopping the Connector" below](#)
- ["Displaying Connector Status" on the next page](#)
- ["Displaying Connector Version" on the next page](#)
- ["Collecting Logs" on the next page](#)

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:
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.