Ivanti Neurons for MDM Connector 100 Installation Guide

December 2024

Contents

Revision history

TABLE 1. REVISION HISTORY

Date	Revision
December 13, 2024	Updated for Ivanti Neurons for MDM Connector 100: • "Latest available versions" on page 5 • " New features summary" on page 6 • "Deploying Connector in AWS" on page 10 • "Connector Requirements" on page 14 • "Installing the Connector ISO Package" on page 16 • "Using the Configuration Wizard" on page 19
June 12, 2024	Updated for Ivanti Neurons for MDM Connector 99: • "Latest available versions" on page 5 • " New features summary" on page 6 • Upgrading the Connector
February 9, 2024	Updated for Ivanti Neurons for MDM Connector 95: • "Latest available versions" on page 5 • " New features summary" on page 6 • "Resolved issues" on page 7 • "Limitations" on page 9 • Upgrading the Connector
December 18, 2023	Updated for Ivanti Neurons for MDM Connector 93: • " New features summary" on page 6 • "Resolved issues" on page 7

TABLE 1. REVISION HISTORY (CONT.)

Date	Revision
July 18, 2023	Updated for patch release 87.0.0.81
June 2, 2023	Updated for Ivanti Neurons for MDM Connector 87: • " New features summary" on page 6 • "Limitations" on page 9
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	• 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-100.0.0-14.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**: mobileiron-kocab-100.0.0-14.iso
  Available at http://support.mobileiron.com/cloud-connector/current/connector-LATEST.zip. This site requires credentials available from Ivanti Support.

The **OVA** package format is not available for this release and it will available in the future releases.

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 100 - New features summary

- **Fresh installation**: Do a fresh installation of Ivanti Neurons for MDM Connector since CentOS 7 is end of life (EOL) and will use Oracle Linux 8.
- **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.

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.

Ivanti Neurons for MDM Connector 100 - Known issues

- **1495642**: During new LDAP configuration, administrators may experience issues with User Search and LDAP sync.

  Workaround: Reconfigure the LDAP in Ivanti Neurons for MDM Admin Portal.

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.

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.

Deploying Connector in AWS

If you are not installing the Ivanti Neurons for MDM Connector on AWS, skip ahead to "Connector Requirements" on page 14.

Onboarding to Oracle Linux 8 based Connector

Follow the steps to onboard the Oracle Linux 8 based connector:

1. Install the latest Ivanti Cloud Connector.

   To deploy the Oracle Linux 8 based Connector on AWS, follow the steps in **Deploying the EC2 instance**.

   > Register the new Ivanti Cloud Connector in the Ivanti Neurons for MDM Admin portal.

2. To disable the existing Ivanti Cloud Connector, log in to the Ivanti Neurons for MDM Admin Portal.
3. Navigate to **Infrastructure** > **Connector** and click the **Actions** drop-down option from the **Actions** column.
4. Select, **Disable**.

   > Make sure to verify the LDAP connectivity with the new Ivanti Cloud Connector after disabling the existing Ivanti Cloud Connector.

5. To remove the old Connector when the new Connector is stable, click the **Actions** drop-down option from the **Actions** column.
6. Select, **Remove**.
7. Select **Yes** from the **Remove this connector** dialog box to remove the old Connector.

Deploying the EC2 instance

Following the steps 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 filed, type **Mobileiron-connnector**.
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 19.

Connector Requirements

These are the requirements:

- For VMware ESXi, use:

  VMware ESXi v6.7U and later versions

- 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)
- Oracle Linux 8 supported on ESXi 6.7U and later versions.
- 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

Onboarding to Oracle Linux 8 based Connector

Follow the steps to onboard the Oracle Linux 8 based connector:

1. To perform a fresh installation of the Ivanti Cloud Connector, click the **Download Connector** button.

   It will download the latest connector package on your local system.

2. Install the latest Ivanti Cloud Connector.

   To deploy the Oracle Linux 8 based Connector on VMs, follow the steps in **Installing the Connector ISO Package**.

   > Register the new Ivanti Cloud Connector in the Ivanti Neurons for MDM Admin portal.

3. To disable the existing Ivanti Cloud Connector, log in to the Ivanti Neurons for MDM Admin Portal.
4. Navigate to **Infrastructure** > **Connector** and click the **Actions** drop-down option from the **Actions** column.
5. Select, **Disable**.

   > Make sure to verify the LDAP connectivity with the new Ivanti Cloud Connector after disabling the existing Ivanti Cloud Connector.

6. To remove the old Connector when the new Connector is stable, click the **Actions** drop-down option from the **Actions** column.
7. Select, **Remove**.
8. Select **Yes** from the **Remove this connector** dialog box to remove the old Connector.

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 Oracle Linux 8 installation begins.

    The installation might take several minutes. Once the installation is complete, the VM client will auto-reboot to the Configuration Wizard window.

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	This Connector will now be registered. Your Tenant credentials are required to perform the registration. Onboard LDAP or PKI connector app using UEM device authorization flow. (yes/no):	To proceed with the Ivanti Connector registration, enter 'no'.
3	Enter your Tenant Admin Username:	Enter the Tenant Admin username you received when you signed up for the device management service.
4	Password:	Enter the Tenant Admin password.
5	Registration Successful!	

Maintenance and Troubleshooting

Troubleshooting and maintenance involves such activities as:

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.