Ivanti Neurons for MDM - FedRAMP Secure Configuration Guide

April 2026

Version 1.0

Prepared by

Identification of Organization that prepared this document		
	Organization Name	Ivanti, Inc
	Street Address	10377 South Jordan Gateway
	Suite/Room/Building	Suite 400
	City, State ZIP	South Jordan, Utah 84095

Prepared for

Identification of Cloud Service Provider		
	Organization Name	Ivanti Neurons for MDM
	Street Address	10377 South Jordan Gateway
	Suite/Room/Building	Suite 400
	City, State ZIP	South Jordan, Utah 84095

Contact us

For questions about the Ivanti Neurons for MDM - FedRAMP Secure Configuration Guide, or for technical questions related to this document, including usage guidance, contact us by email at : FedRAMPAuditandCompliance@ivanti.com.

Contents

Revision history

TABLE 1. REVISION HISTORY

Date	Revision
Apr 15, 2026	Updated for Version 1.0

Introduction and Purpose

From the **Federal Risk and Authorization Management Program (FedRAMP)** website regarding the **Secure Configuration Guide (SCG) Mandatory Balance Improvement Release (BIR):**

Executive Order 14144, *Strengthening and Promoting Innovation in the Nation's Cybersecurity, Section 3(d), as amended by Executive Order 14306, Sustaining Select Efforts to Strengthen the Nation's Cybersecurity and Amending Executive Order 13694 and Executive Order 14144, Section 3(b), states that "the Administrator of General Services, acting through the Director of the Federal Risk and Authorization Management Program (FedRAMP), in coordination with the Secretary of Commerce, acting through the Director of NIST, and the Secretary of Homeland Security, acting through the Director of CISA, shall develop FedRAMP policies and practices to incentivize or require cloud service providers in the FedRAMP Marketplace to produce baselines with specifications and recommendations for agency configuration of cloud based systems in order to secure Federal data based on agency requirements*."

As a result of these Executive Orders, the **FedRAMP Project Management Office (PMO)** has issued additional requirements for all **Cloud Service Providers (CSPs)** in the form of the **Mandatory Secure Configuration Guide (SCG) Balance Improvement Release (BIR)**.

To comply with the requirements listed in the SCG BIR, Ivanti has created this document. This guide explains, in simple and clear steps, how to manage administrator accounts in Ivanti Neurons for MDM in environments that follow **Federal Risk and Authorization Management Program (FedRAMP)** security requirements.

This document is intended to help customers using the Ivanti Neurons for MDM **FedRAMP** environment to:

- Set up and configure administrator accounts.
- Access administrator accounts and understand the types of administrator accounts available.
- Use and manage administrator accounts.
- Decommission (delete) administrator accounts securely when they are no longer needed.

Default Tenant Admin and Accounts

By default, the following accounts are created for Ivanti Neurons for MDM tenant:

Admin Type	Format	Roles/Permissions	Details
Super Admin	<username>-emmadmin@<domain>	All	A **Super Admin** is the primary user who can create new admin accounts with full permissions. By default, newly added space permissions are not automatically assigned to these admins. However, the Super Admin can manually grant access to any new spaces later.
Nobody User	nobody-<number>-<tenant-id>@<domain>	Device App & Content Read, Device Registration	A **Nobody User** is a default account that cannot be deleted. The service assigns this user to devices that have no associated users, such as retired devices.

Admin Type	Format	Roles/Permissions	Details
Guest User	guest-<number>-<tenant-id>@<domain>	None	By default, the guest user created by Ivanti Neurons for MDM is disabled. When a guest user signs in, the device is not assigned to any user, and the guest user is not managed. To manage a guest user, the default guest account created by Ivanti Neurons for MDM must be enabled. After enabling the default guest account, any device that a guest user signs into, is assigned to the default guest user, allowing the user to be managed.

Roles Management

Roles are packaged groups of permissions that allows granting a set of permissions to an administrative user, while limiting their access to control specific areas of functionality. Ivanti Neurons for MDM provides a set of system roles that can be assigned (or edited) and a facility to create custom roles. You can search for specific permission based on the category and all the options that are associated with the specific role or permission in the UI are displayed. A tool tip is displayed for the permissions that are added as dependent permissions.

The Roles Management page and the associated options are hidden for converged tenants who have access to both Ivanti Neurons for UEM and Ivanti Neurons for MDM.

There are two kinds of permissions available, and therefore two kinds of roles:

- **Space-specific roles** - The permissions are Space-specific, and therefore apply in a specific Space only. Examples are Device Management, App Management in a Space.
- **Cross-Space roles** - The permissions are, by nature, applicable to all roles. Examples are tenant-level settings such as MDM Certificates, App Catalog Settings.

Creating a custom role

You can create a custom cross-Space or Space-specific roles. When you select a permission, the dependent permissions will be selected automatically. Accordingly, a user assigned with a custom role can only perform the specific actions (such as retire, wipe) that are available when the user visits the Devices page or the Device Details page.

When you apply the View User Registration PIN custom role, users can view the PIN of other users that have the same access level or with lesser privileges and the users cannot create PINs for other users.

The newly created custom role can not be assigned to anyone automatically. The tenant super admin needs to assign it to the required admin users who can later assign the same to other users as needed.

Procedure

1. Go to **Admin** > **Roles Management**.
2. Click **+Add Custom Role**.

3. In the **Create Role** page, enter the **Name** of the new role.
4. (Optional) add a description for the new role.
5. Under **Role Type**, select one of the following role types:
   - **Cross-Space Role**
   - **Space-Specific Role**
6. Under **Permissions**, select the required granular permissions.

   See the following table for Admin and User permissions.
7. Click **Save**.

The following table lists the permissions, roles, and attributes you can use to create a custom role:

Role Type	Permissions Category	Granular Permissions
Cross-Space Role		
Admin		
	Manage Custom Attributes	• Add Custom Attribute • Delete Custom Attribute • Edit Custom Attribute • View Custom Attribute
	Support Administrators	• Add Support Admins • Delete Support Admins • Disable Support Admins • View Support Admins and Show Login History
	Certificate Authority	• Add Certificate Authority • Delete Certificate Authority
	Connector	• Add Connector Logs • Delete Connector Logs • View Connector • Update Connector

Role Type	Permissions Category	Granular Permissions
	LDAP Management	• Add User/Group/OU • Add Server • Browse Server • Delete Server • Search Server • Sync Server • Remove User/Group/OU • View Serve All LDAP permissions in this section require View Connector permission. It will be automatically selected in the Connector section when you select any of these LDAP permissions.
	Licensing Management	View Licenses
Users		

Role Type	Permissions Category	Granular Permissions
	User Management Actions	• View User • Update User • Send Message to User • Append/Assign Roles to User • Create User • Delete User • Invite User • View User Registration PIN
	Assign Custom User Attribute	• Delete Attribute • View Attribute • Add/Edit Attribute
	User Groups	• View User Group • Edit User Group • Append/Assign Roles to User Group • Create User Group • Delete User Group

Role Type	Permissions Category	Granular Permissions
	Report Management	• Create Report • Edit Report • Run Report • Delete Report Record • View Report • Delete Report • Download Report Record
Devices		
	Bulk Enrollment	• Create Bulk Enrollment • Update Bulk Enrollment • Assign User to Bulk Enrollment • View Bulk Enrollment • Delete Bulk Enrollment
Space-Specific Role		
Devices		

Role Type	Permissions Category	Granular Permissions
	Device Actions	• Assign Device to User • Clear Device Activation Lock • Delete Device • Disable Device Lost Mode • Enable Device Lost Mode • Device Force Checkin • Lock Device • Unlock Device • Device Force Logout • Reinstall Device System Apps • Restart Device • Schedule iOS Device Updates • Relinquishing Device Ownership • Retire Device • Cancel Retire Device • Shutdown Device • View Device • Wipe Device • Cancel Wipe Device • Update Device OS Version

Role Type	Permissions Category	Granular Permissions
		• Bulk Assign Via Upload • Start TeamViewer Session
	Assign Custom Device Attributes	• Add/ Edit Device Custom Attribute • Delete Device Custom Attribute • View Device Custom Attribute All Assign Custom Device Attribute permissions in this section require Device Read permission. It will be automatically selected in the Device Actions section when you select any of these Assign Custom Device Attribute permissions.
	Device Configurations	• Exclude Profile • Push Profile • Push Excluded Profile • Retry Install on Error
	Device Groups	• Add Device Group • Delete Device Group • Edit Device Group • View Device Group

Role Type	Permissions Category	Granular Permissions
	Bulk Enrollment	• Create Bulk Enrollment • Update Bulk Enrollment • Assign User to Bulk Enrollment • View Bulk Enrollment • Delete Bulk Enrollment
	App Inventory	• View App Inventory
Configurations		
	Configurations	• View/ Export Configs • Edit/ Prioritize Configs • Add/ Clone Configs • Delete Configs
Policies		
	Policies	• View Policies • Edit/ Prioritize Policies • Add/ Clone Policies • Delete Policies

To edit a role, go to **Admin**, **Roles Management** page and click the edit icon under **Actions** against the name of the role. A user cannot edit a cross-space role to a space-specific role and vice versa.

Account / User Management

Add a user

Procedure

1. Click **Add** (top right).
2. Select **Single User** .
3. Complete the form with the user's information:
   - Email Address
   - First Name
   - Last Name

   The **Username** field displays the email address you entered.
4. If you want to change the display name for this user, edit the default text in the **Display Name** field.
5. Assign a password in the **Password** field.
6. Enter the password again in the **Confirm Password** field.
7. Click **Done** to add the user.
8. Communicate the password to the person who will help manage devices.

Assign Roles to users

You can give users access to Ivanti Neurons for MDM data and features by assigning roles. You can assign roles directly to users or to user groups. Assigning a role to a user group gives that role to all users in that group.

Procedure:

1. Go to:
   - **Users > Users** *or*
   - **Users > User Groups.**
2. Select one or more users or user groups.
3. Click **Actions**.
4. From the Users details page or User Groups details page, click **Assign Roles** *or* From the User list or User Group list page, select **Append Roles**.
5. Select one or more of the following roles you want to assign:
   - System Management | Cross-Space
   - System Read Only | Cross-Space
   - User Management | Cross-Space
   - User Read Only | Cross-Space
   - LDAP User Import and Invite | Cross-Space
   - Device Management | Space-Specific
   - Device Read Only | Space-Specific
   - App & Content Management | Space-Specific
   - App & Content Read Only | Space-Specific
   - Device Actions | Space-Specific
   - Cisco ISE Operations | Cross-Space
   - Scheduled Task Management | Cross-Space
   - Common Platform Services (CPS) | Cross-Space
   - Low User Impact Migration Management | Cross-Space
   - Custom Device Enrollment | Cross-Space

- Edit Microsoft Graph | Cross-Space
- Send/Cancel Wipe | Cross-Space
- View Microsoft Graph | Cross-Space
- Manage Access Integration | Cross-Space

6. Click **Next**.
7. If the selected roles are Space bound, then select Spaces for all the Space bound roles.

   > If there is only one Space (Default Space), the Specify Space step is skipped when assigning a Space-bound role.

   The summary page displays the Space name for Space bound round as Default Space.
8. Review the summary of the roles to be assigned and click **Done**.

Edit a user

Procedure:

1. Go to **Users** > **Users**.
2. Click any user from the displayed list.
3. Under the **Overview** tab, click **Edit**.
4. Enter the password and click **Authenticate**.
5. Edit/Modify the applicable fields.

Delete a user

Procedure:

1. Go to **Users** > **Users**.
2. Select the entry for the user.

3. Click **Actions** (upper-right).
4. Select **Delete**.

When an Ivanti Neurons for MDM Administrator or Partner Administrator attempts to delete a Partner Administrator, Ivanti Neurons for MDM displays a message conveying that a Partner Administrator must perform this operation on the Service Provider Portal.

If a user has some devices associated with their account, first the user must retire and delete the devices and then delete the user. If user has no devices the user information can be deleted when the user is deleted.

Additional Recommendations from FedRAMP

Ivanti is currently reviewing the additional recommendations outlined in the SCG and will determine their implementation in future versions of this document based on the environment's security requirements and the feasibility of each recommendation.

Additional Recommendations from **FedRAMP**:

- Clear Instructions on how the product sets all settings to their recommended secure defaults for top-level administrative accounts and privileged accounts when initially provisioned.
- Clear Instructions on how the product offers the capability to compare all current settings for top-level administrative accounts and privileged accounts to the recommended secure defaults.
- Clear Instructions on how the product offers the capability to export all security settings in a machine-readable format.
- Clear Instructions on how the product offers the capability to view and adjust security settings via an API or similar capability.

References

- *Ivanti Neurons for MDM Administrator Guide*

  Contains information for getting started, registering users and devices, adding, configuring, and managing apps, creating and managing configurations and policies for apps, security, certificates, device and user licenses, package licenses, and license upgrades, and device use self-service portal for managing devices.

The preceding link was the most recent at the time of publication. To ensure that you are getting the latest Ivanti Neurons for MDM documentation, visit this link.