Ivanti Neurons for ITSM - Secure Configuration Guide

Document Home

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 ITSM
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 ITSM Secure Configuration Guide, or for technical questions related to this document, including usage guidance, contact us by email at : FedRAMPAuditandCompliance@ivanti.com.

Revision History

Date	Revision
April 15, 2026	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 ITSM 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 ITSM 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.

Secure Configurations - Ivanti Neurons for ITSM

This page details the Neurons for ITSM content related to the Administrator role, their tasks pertaining to secure configuration and administration and all security components in ITSM that are required to be aligned with the FedRAMP guidelines.

User roles in ITSM

In ITSM, the user roles are broadly defined under three user categories –

Administrators – are users managing the overall administration of Neurons for ITSM and monitoring its operational health. Administrators have access to all modules and configuration of workspaces.

For most configuration tasks, you must log in as an administrator and work in the Configuration console.

Common administrator tasks include the following:

Defining the security structure.

Add users to roles to control access to the system.

Constructing business objects used to capture and display data in the environment.

Designing the workflows required to process information.

Defining the schedule of escalation for processing incidents, tasks, and service requests.

Users – are the IT support staff who manage service requests, problems, and incidents, for example, Service Desk Analyst, Service Desk Manager, and Change Manager.

Self Service Users – Employees and external customers who use the Self-Service portal to request IT business services, such as reporting a service interruption or ordering a computer. Users in the Self-Service portal can also create incidents and check the status of existing incidents.

For more information, refer to Types of Users.

Adding Users to the System and Assigning Roles

The Administrator manages user access by adding new users to the system and assigning roles to ensure required permissions and responsibilities are set for users to function and carry on with their responsibilities.

For more information, refer to Adding Users to the System and Assigning Roles to Users and Setting up Roles.

Secure Login

The Administrator ensures secure login to the application by managing authentication settings, enforcing strong password policies, managing session timeouts, and more.

The following topics have in-depth information regarding assigning user roles, setting up users, accessing URLs securely,

- Setting Up User Login
- Logging in or Accessing Records Using URLs
- Configuring Anonymous User
- Application Security
- Role-Based Security
- Controlled Access

Provisioning and Decommissioning of Tenants

The following topics have in-depth information regarding provisioning and decommissioning of tenants:

- Deploying Neurons for ITSM
- Using Development Project
- Decommissioning of tenants – To decommission a tenant, raise a ticket to the Ivanti Operations team.

Administrator-Only Security Controls

Administrators ensure application security by configuring authentication settings restricted to top-level accounts, with clear security implications.

The following topics have in-depth information regarding authentication methods and security settings:

- Authentication
- About external authentication configuration
- Setting up ITSM users for authentication via the Neurons Platform
- Setting Up External Authentication with LDAP
- Working with Single Sign-On authentication
- Working with ADFS/SAML
- About Windows Integrated Security
- Setting Up Authentication for OpenID Connect with Google
- Setting Up authentication for OpenID Connect with Microsoft Azure
- Neurons for ITSM OpenID Connect Configuration

- Setting Up Authentication for OpenID Connect with Yahoo
- Setting Up Authentication for OpenID

Recommended Secure Default Settings for Administrative Accounts and Privileged Accounts

This capability is currently not available, but it's tentatively planned to be delivered by the end of 2026.

Compare Current Settings to Default Settings for Administrative Accounts and Privileged Accounts

This capability is currently not available, but it's tentatively planned to be delivered by the end of 2026.

Export Security Settings in a Machine-Readable Format

There are currently no plans on the one-year roadmap to provide this capability due to other innovations taking priority. It may be considered in future releases.

View and Adjust Security Settings using API or any other integration

There are currently no plans on the one-year roadmap to provide this capability due to other innovations taking priority. It may be considered in future releases.

Version History for the Recommended Default Secure Settings

This capability is currently not available, but it's tentatively planned to be delivered by the end of 2026.

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

Neurons for ITSM Administer and Configure help

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 ITSM documentation, visit Neurons for ITSM Administrator and User help and Self Service help.