10ZiG Manager V6 User Guide

Document and Version Control			
Version	Created by	Date	Authorised & Checked
1.0	Zachary Flanagan	6/18/26	Chris Hayes

Table of Contents

1. About this document

This document introduces the 10ZiG Manager Web Console.

It explains key features of the Web Console and covers the main areas of device and operating system management. This guide focuses on managing 10ZiG Linux-based Thin Clients and Zero Clients.

In this guide, client devices may also be called **Platforms**. Different Platforms may have different management options. Where this applies, the guide notes the difference and provides examples. Some options apply to all Platforms, and those are also identified to avoid confusion.

2. Definition of terms

This guide references several hardware types and 10ZiG Manager Web Console features. Some terms have changed between releases. The definitions below explain how these terms are used in this guide.

10ZiG Linux Clients – Refers to 10ZiG NOS, PeakOS, and RepurpOS Linux-based clients.

Secure Connector – Refers to the Secure Connector in 10ZiG Manager version 6 and later. In versions earlier than 6, this feature was called Cloud Connector.

Secure Agent – Refers to the Secure Agent included with 10ZiG NOS, PeakOS, and RepurpOS firmware version 16.5.37 and later. In firmware versions earlier than 16.5.37, this feature was called Cloud Agent.

Organization – A logical tenant or administrative boundary in 10ZiG Manager. Organizations can be used to separate devices, groups, users, roles, and access permissions by customer, department, region, or business unit.

Root user – The top-level administrator account for the 10ZiG Manager environment. The root user can manage global settings and create or administer Organizations.

Organization user – A user account created within, or assigned to, a specific Organization. Organization users can only access the resources and actions allowed by their assigned role.

Entra ID – Microsoft Entra ID, previously Azure Active Directory. Entra ID can be configured through User Management as an external identity provider for Web Console authentication.

Active Directory – A directory service that is planned for support in a future 10ZiG Manager release. When available, its integration settings will be documented under User Management.

Licensing – Refers to the 10ZiG Manager license information and license status shown in the Web Console Licensing tab.

3. What is the 10ZiG Manager Web Console and what can it do for your 10ZiG Linux Clients?

The 10ZiG Manager Web Console is an enterprise device management tool for 10ZiG Linux Clients. It allows administrators to manage devices, configurations, firmware, templates, tasks, and remote access from a single web-based interface.

The Web Console can be used to perform the following actions:

- Create device groups and subgroups to organize devices by operating system, device type, business area, region, test group, or other criteria.
- Use auto-naming to automatically rename devices when they register with 10ZiG Manager. Device names can follow your organization's naming standards.
- Connect 10ZiG Linux Clients directly to the 10ZiG Manager Server or through the 10ZiG Manager Secure Connector.
- Remotely power devices on, power them off, or reboot them.
- Retrieve, edit, and send client-specific hardware and software configuration settings.
- Create, manage, and apply templates to individual Linux clients or groups of Linux clients.
- Import, export, and deploy Linux firmware or addon releases. For example, newly registered devices can automatically receive a firmware update, so they meet your organization's required firmware level.
- Use the built-in Task Scheduler to create scheduled actions for individual devices or groups. These tasks can include actions such as rebooting devices, powering them off, or applying Linux firmware updates.
- Use Organizations to support multi-tenant management. Organizations can separate devices, groups, users, and permissions for different customers, departments, regions, or business units.
- Assign users and roles through User Management so administrators only have access to the features and Organizations required for their responsibilities.

- Use supported directory and identity provider integrations under User Management, including Entra ID, to centralize sign-in and user access control.
- Use the Recovery, User Management, and Licensing tabs to access additional V6 management functions from the same Web Console.
- Remotely control and administer 10ZiG Linux Clients through VNC.

4. Which Linux endpoint devices can the 10ZiG Manager Web Console control?

The 10ZiG Manager Web Console can manage 10ZiG Linux-based hardware and software platforms, including the following device types.

10ZiG Linux Clients

NOS Zero Clients

All 10ZiG NOS operating systems running on 10ZiG hardware are supported. This includes:

- NOS-M for Microsoft environments.
- NOS-O for Omnissa environments, previously VMware.
- NOS-C for Citrix environments.

PeakOS Thin Clients

PeakOS is the 10ZiG Linux-based thin client operating system that runs on 10ZiG hardware.

RepurpOS Thin Clients

RepurpOS is based on the same operating system as PeakOS. It is designed for customers who run the OS on reused or repurposed non-10ZiG hardware.

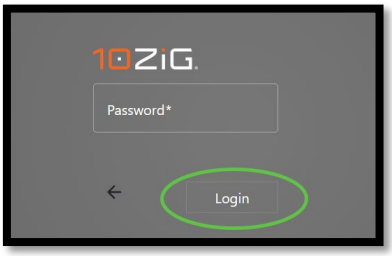
NOTE: Screenshots and references to PeakOS, RepurpOS, and NOS devices in this guide are based on the latest OS releases available when this guide was published.

5. Signing in to the 10ZiG Manager Web Console for the first time

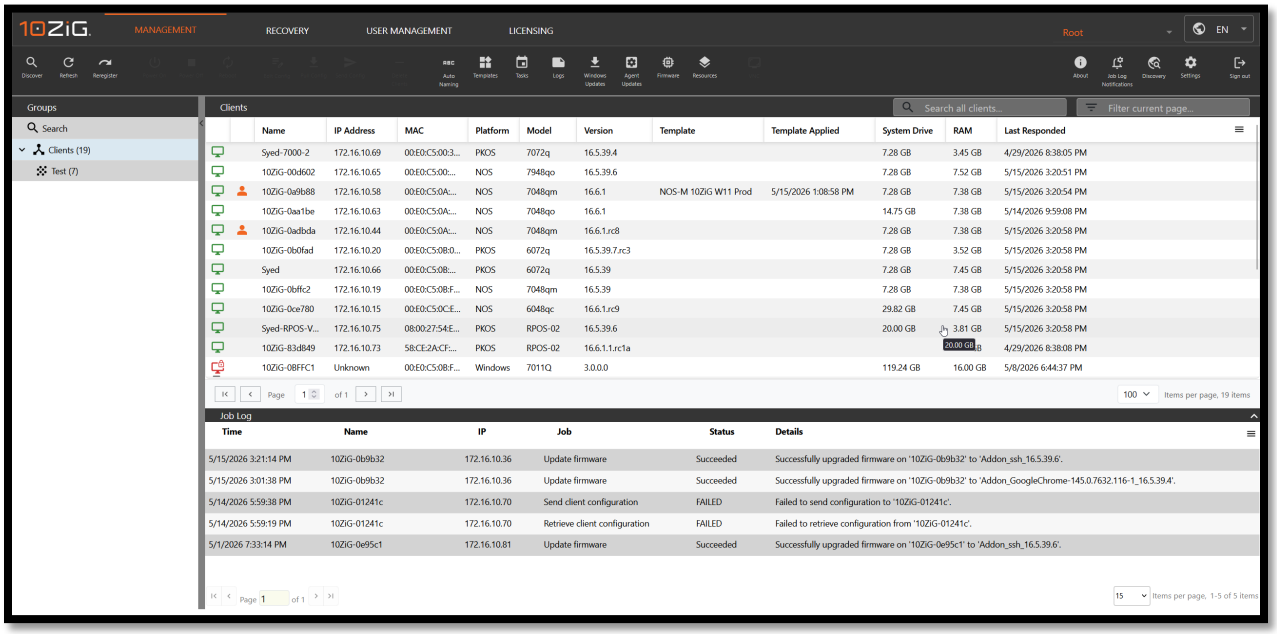
The 10ZiG Manager Web Console runs in a supported web browser. Microsoft Edge and Google Chrome are the preferred browsers.

To sign in for the first time:

1. Ask your 10ZiG Manager Administrator for the Web Console server address or IP address.
2. Enter the address in your browser's address bar.
3. When the login screen appears, enter your domain, username, and password.



4. Click **Login**.
5. The window you see once logged in is the 10ZiG Manager Web Console



6. Welcome to the 10ZiG Manager Web Console

The 10ZiG Manager Web Console provides access to 10ZiG Manager features from one browser window.

The console is divided into several panes. These panes show thin clients, device properties, device groups, group properties, and Job Log information. The Job Log pane displays updates for actions performed throughout the console.

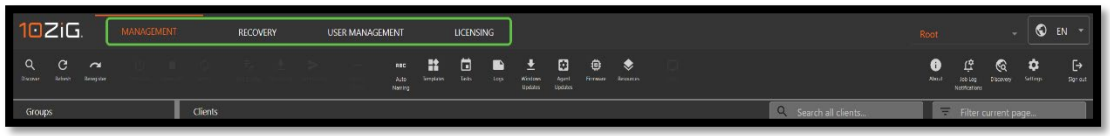
Different device Platforms may have different management options. Where platform-specific options apply, this guide identifies them and provides examples. Options that apply to all Platforms are also noted.

Navigating the Web Console Menus

The main menu tabs appear near the top-left side of the Web Console. These tabs group related management tasks together.

The main tabs are:

- **Management**
- **Recovery**
- **User**



Management

- **Licensing**

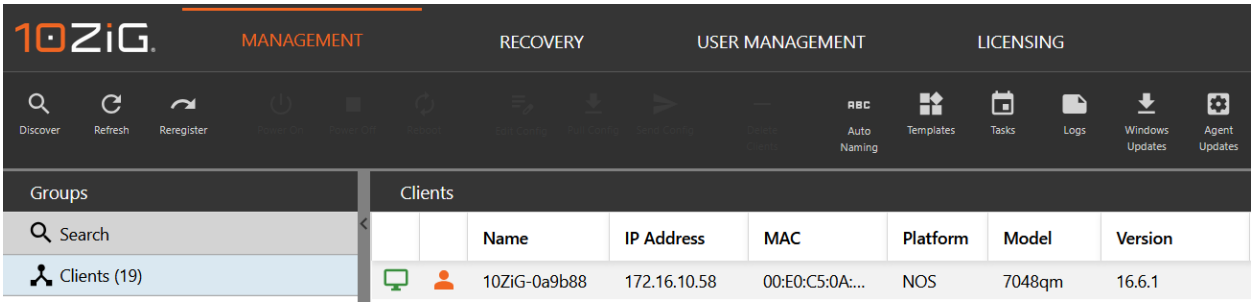
When you select a tab, the available options below it change.

The main tabs are used as follows:

Management – Used for day-to-day client management, including groups, templates, firmware, configuration, tasks, and VNC access.
Recovery – Used for recovery-related tools and workflows for supported 10ZiG clients.
User Management – Used to manage local users, roles, Organizations, and authentication-related access. This is also where administrators manage access boundaries for multi-tenant environments.
Licensing – Used to view and manage 10ZiG Manager license information and license status.

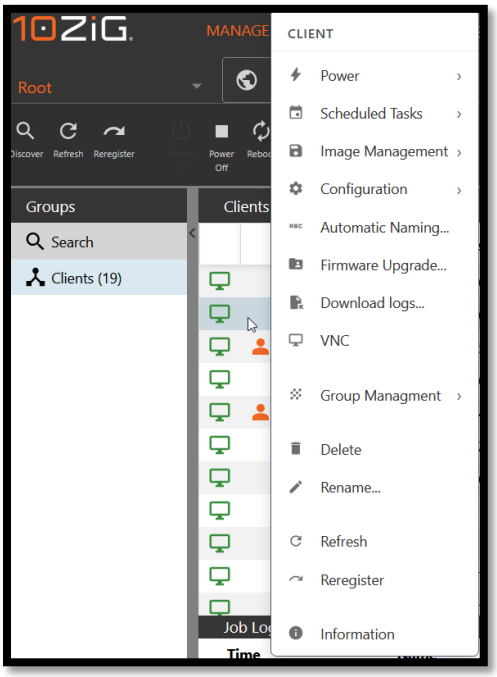
If a tab or option is not visible, confirm that the signed-in user has the required role and Organization access.

The **Management** tab opens by default when the Web Console launches. It displays registered clients in the **Clients** window.



In the **Clients** window, devices are listed by platform. For example, a device may appear as **NOS** or **PKOS**.

When you right-click on a device, additional management options become available. For example, selecting a NOS device gives access to options for power control, configuration management, and VNC remote control.



7. Connecting your 10ZiG Linux Clients to the 10ZiG Manager Server

There are several ways to discover thin clients or point them directly to the 10ZiG Manager Server. This section explains how to manually configure 10ZiG Linux Clients to connect to the server.

This process uses the local 10ZiG Linux Client application called **Secure Agent** on OS version 16.5.37 and later. On earlier OS versions, this application is called **Cloud Agent**.

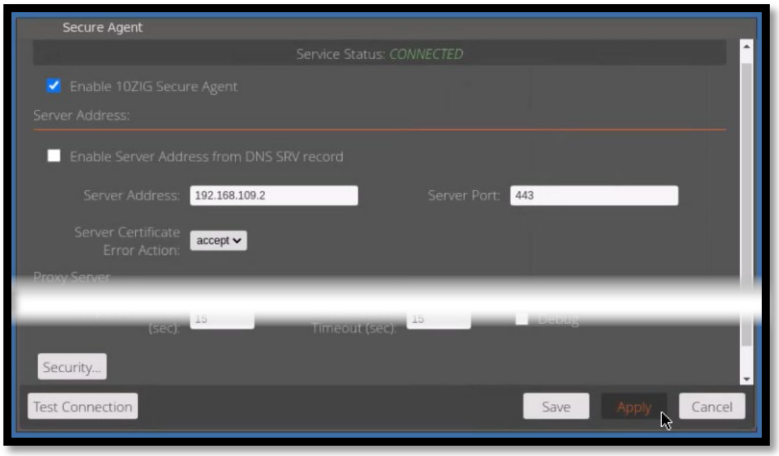
1. On the local 10ZiG Linux Client, open **Control Panel** by selecting the gears icon.

2. Select **Cloud Agent** or **Secure Age**
3. When the applet opens, choose one of the following registration options:
    - Leave **Enable Server Address from DNS SRV record** selected.
    - Clear the checkbox and manually enter the server address or FQDN.

If you use the DNS SRV option, your network infrastructure must be configured to support it. The DNS record must also be visible to the clients. Contact your Network Administrator if this discovery method is required.

Connecting Directly to the 10ZiG Manager Server

In this example, the 10ZiG Manager Server uses the IP address **`192.168.109.2`**. You can also use an FQDN.



1. Enter the server IP address or FQDN in the server address field.

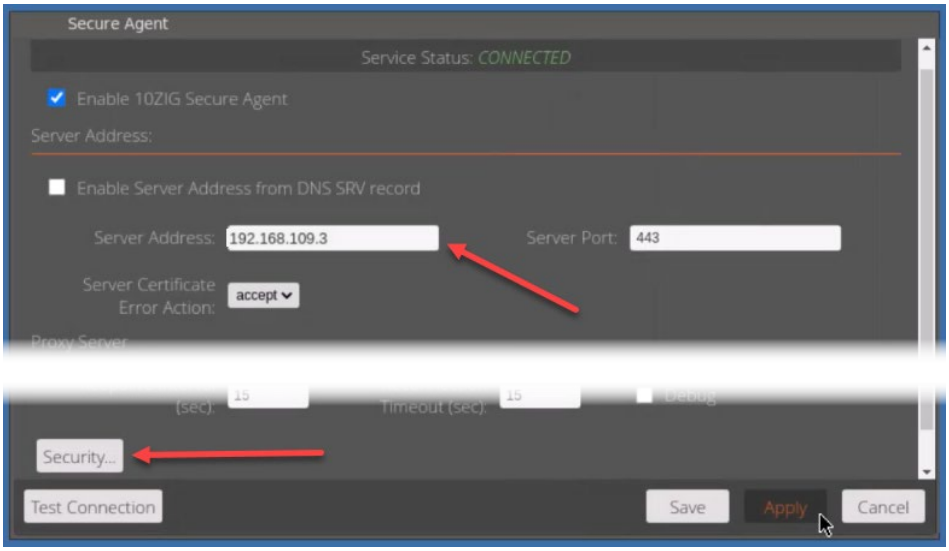
2. Click **Apply**.
3. The client attempts to connect to the 10ZiG Manager Server.
4. When the connection succeeds, **Service Status** displays **CONNECTED** in green.

Connecting to 10ZiG Manager via the 10ZiG Manager Secure Connector

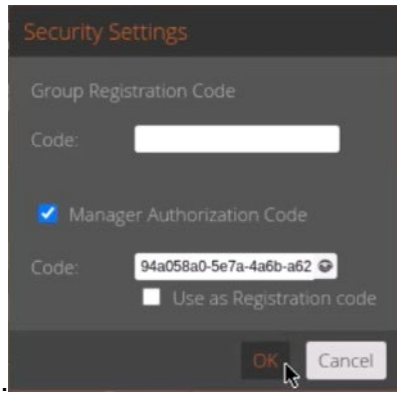
If your organization uses the Secure Connector, remote users will usually connect their 10ZiG clients through it.

The Secure Connector is configured to point to the 10ZiG Manager Server. In most environments, the client only needs to point to the Secure Connector address. A 10ZiG Manager Authorization Code is not required simply to connect through the Secure Connector. The authorization code is used when Secure Agent authorization is enabled or when a client must be registered into a specific Organization.

1. Open the **Secure Agent** settings.
2. Change the server address to the Secure Connector address. In this example, the Secure Connector uses `192.168.109.3`.



3. Click Security only if you need to enter an authorization code for Secure Agent authorization or Organization registration.



4. Enter the authorization code provided by the 10ZiG Manager administrator or Organization administrator.
5. Click **OK**.

The client connects to the 10ZiG Manager Server through the Secure Connector. If an Organization authorization code was entered, the client is registered into the matching Organization according to the Manager configuration.

Note: Use an FQDN for the server address when possible. If the server IP address changes, clients can still connect by using the hostname.

After these settings are configured, they can be retrieved and added to a device template. That template can then be used to replicate the client configuration across other devices in your organization.

Secure Agent Authorization and Organizations

Secure Agent authorization can be enabled from the 10ZiG Manager settings interface. This settings interface is accessed through the Configuration Service address, typically using port 10219 on the 10ZiG Manager Server.

Use Secure Agent authorization when you want clients to provide an authorization code before they are accepted by the Manager or when clients must register directly into a specific Organization.

To use Secure Agent authorization:

Open the 10ZiG Manager Configuration Service in a supported browser. The address is typically https://<manager-address>:10219/.
Sign in with an administrator account that has access to Manager settings.
Locate the Secure Agent authorization settings.
Enable Secure Agent authorization if your deployment requires authorization codes.

Create or confirm the authorization code that clients will use.
Save the settings.

After this setting is enabled, provide the appropriate authorization code to the administrator configuring the client Secure Agent.

Registering a client to a specific Organization

If Organizations are enabled, a client can be registered into a specific Organization by using that Organization's authorization code during Secure Agent configuration.

Use this workflow when clients must be separated by customer, department, region, or other administrative boundary.

Confirm that the Organization exists in User Management.
Confirm that the Organization has the correct authorization code or registration settings configured.
On the client, open Secure Agent.
Enter the Manager Server or Secure Connector address.
Open Security and enter the Organization authorization code.
Apply the settings and confirm that the client appears under the intended Organization in the Web Console.

If the client appears in the root environment or in the wrong Organization, verify the authorization code and the Organization registration settings before re-registering the client.

---

8. Creating 10ZiG Manager Device Groups

This section explains how to create a 10ZiG Manager Device Group so you can register, manage, and maintain 10ZiG Linux Clients.

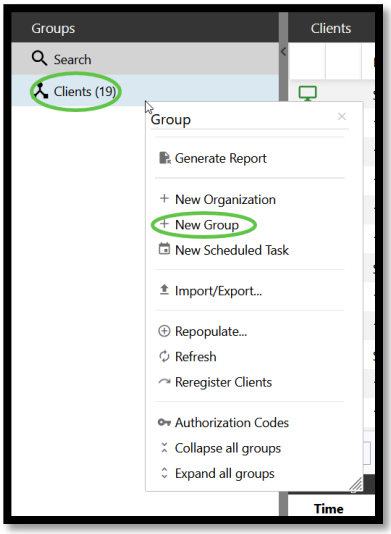
In this example, you will create a group for a specific platform and model. Additional configuration options are added later in the section.

The **Groups** window includes a default group called **Clients**. All discovered clients appear in this group. If you create subgroups, selecting **Clients** still displays all available devices.

8.1 Creating a New Device Group with Filters for Platform and Model

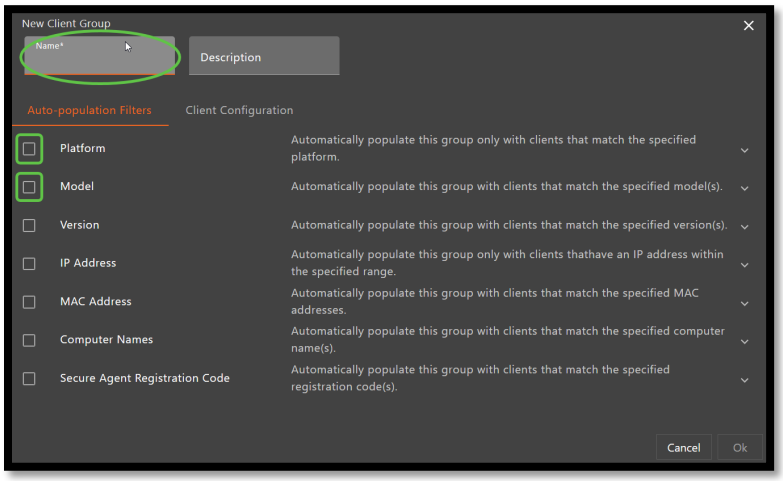
This example creates a group for **Linux 16.4 and later** devices. It also filters by model using **6148M** as the target NOS-M client model.

1. Right-click **Clients**.

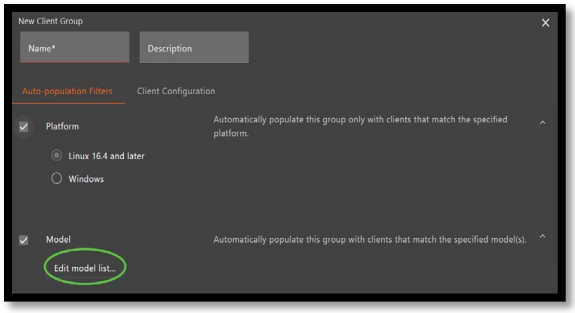


2. Select **New > Group**.
3. In the **New Thin Client Group** window, enter a clear group name. This example uses **NOS-M-DEVICES**.
4. In **Auto-population Filters**, select **Filter by Platform**.

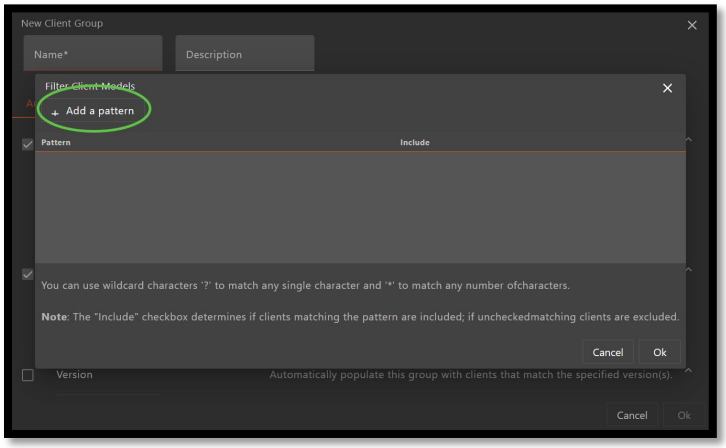
5. Choose **Linux 16.4 and later**.
6. Select **Filter by Model**.



7. Click **Edit model list**.



8. In the **Filter Client Models** window, click **Add a pattern**.



9. Enter the pattern `??48M`.
10. Click **OK**.

You can use `?` and `*` as wildcards in filters:

- `?` matches any single character.
- `*` matches any number of characters.

The example `??48M` matches any first two characters, followed by `48M`.

Note: If **Include** is selected, devices that match the filter are added to the group. If **Include** is cleared, matching devices are excluded from the group.

After creating the group:

1. Confirm that the new group appears under **Thin Clients**.
2. Right-click the new group.
3. Select **Repopulate**.
4. Click **Yes** when prompted.

After the group is populated, matching clients appear in the **Thin Clients** window.

8.2 Additional Examples of Group Filters

Group filters can be used to include or exclude devices based on model, IP address, computer name, or MAC address.

Filter	Example Filter Value	Example Matched Value	Include / Exclude	Description
Model	`??48*`	`4648QV`, `6148C`	Include	Matches models containing `48`, ignoring the first two characters and anything after `48`. Useful for NOS Zero Clients.
Model	`*72*`	`4672Q`, `6072Q`	Include	Matches models containing `72`. Useful for PeakOS Thin Clients.
IP Address	`192.168.110.1-192.168.110.254/24`	`192.168.110.100`	Exclude	Can be used to group externally deployed devices, such as home workers connecting through the Cloud Connector.
Computer Names	`SALES*`	`SALES-0001`	Include	Matches hostnames that start with `SALES`.
MAC Address	`00E0C5*`	`00E0C56D771F`	Include	Matches NOS or PeakOS 10ZiG hardware clients.
MAC Address	`00E0C5*`	`00E0C56D771F`	Exclude	Excludes NOS or PeakOS 10ZiG hardware clients while allowing other clients running a 10ZiG OS, such as RepurpOS clients.

8.3 Set your Group to Auto Configure your 10ZiG Linux Clients with Templates

10ZiG Manager can assign templates to groups so related Linux clients are automatically configured when they register with the 10ZiG Manager Server.

This section explains how to:

- Create a base template after a factory reset.
- Modify and save the template.

- Copy the template.
- Modify the copy.
- Assign the updated template to a group.

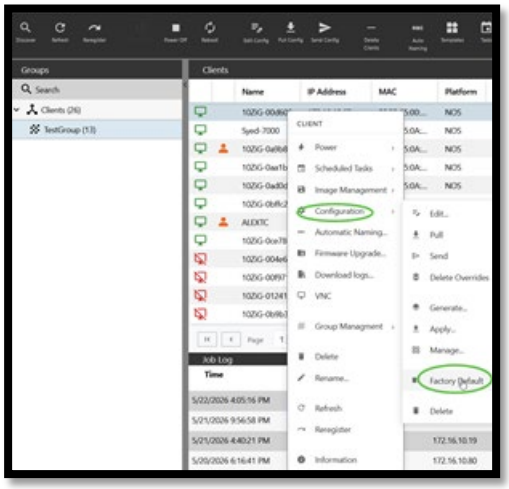
Before creating the template, this example resets the client to factory defaults. This helps ensure the template does not include unwanted settings.

Note: A factory reset is not required if you are creating a golden image. If the master device already contains all required settings, configure the device as needed and then create the template from that device.

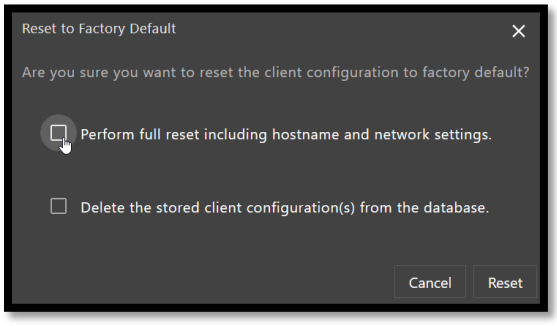
8.3.1 Resetting your device to Factory Defaults using the 10ZiG Manager Web Console

You can reset a device locally or from the 10ZiG Manager Web Console. This example uses the Web Console.

1. In the Web Console, right-click the 10ZiG Linux Client.



2. Select **Configuration > Factory Default**.
3. When prompted, review the following options:
    - **Perform full reset including hostname and network settings**
    - **Delete the stored client configuration(s) from the database**



4. Select the full reset option if you want to start from a clean base image.

5. Select **Delete the stored client configuration(s) from the database** if you want the base template to use a clean configuration.
6. Click **Reset**.

The client resets to factory defaults. Progress appears in the **Job Log** window.

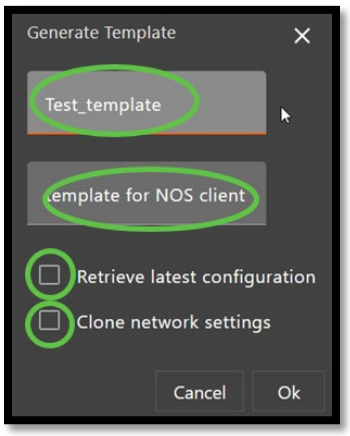
Note: Use caution when resetting remote endpoints. A full reset removes device-specific settings, including imported certificates and Secure Agent or Cloud Agent settings. If the client connects through a proxy or uses the agent to reach the 10ZiG Manager Server, the reset may remove those settings and disconnect the client from the server.

A full reset also changes VNC service startup settings back to **On Demand** if they were previously set to **On Boot**.

8.3.2 Building your first 10ZiG Linux Client Template

Follow these steps to create a Linux client template.

1. Right-click the Linux client.
2. Select **Configuration > Generate**.
3. In the **Configuration Template** window, enter a template name.



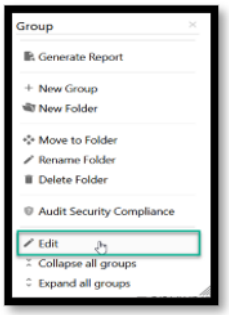
4. Add a clear description.
5. Choose whether to retrieve the client's current configuration before creating the template:
   - Click **Yes** to retrieve the latest configuration from the client.
   - Click **No** to use the configuration already stored on the 10ZiG Manager Server.
6. Click **Ok**.

Retrieving the latest configuration is recommended. This ensures the template includes the client's current settings.

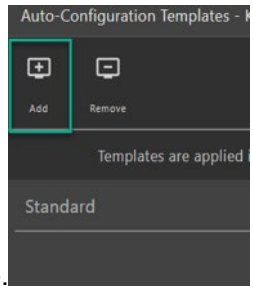
When the template is created successfully, the result appears in the **Job Log** window.

8.3.3 Adding Template(s) to the Group to Auto-Configure your 10ZiG Linux Clients

After creating a template, assign it to the group that should receive the configuration. The assigned template is applied to matching 10ZiG Linux Clients when they check in.



1. Right-click the group that should receive the template.
2. Select Edit.



3. Open the Client Configuration tab.
4. Select Automatic Client Configuration.
5. Click Edit Configuration. The Auto Configuration Templates window opens.
6. Click Add.
7. When the Stacking Configuration Templates message appears, click OK.
8. Select the template that should be applied to the group.
9. Click OK. The template is added to the Auto Configuration Templates list.
10. Confirm that the correct template is listed before closing the window.

11. Click OK in the Auto Configuration Templates window.
12. Click OK again in the Edit Thin Client Group window to save the group settings.

Warning: After the Auto Configuration settings are saved, any 10ZiG Linux Client in the group receives the assigned template the next time it checks in.

Before closing the group settings, verify that the template appears in the Auto Configuration Templates list. If the template is not listed, it will not be applied to clients in the group.

Verification

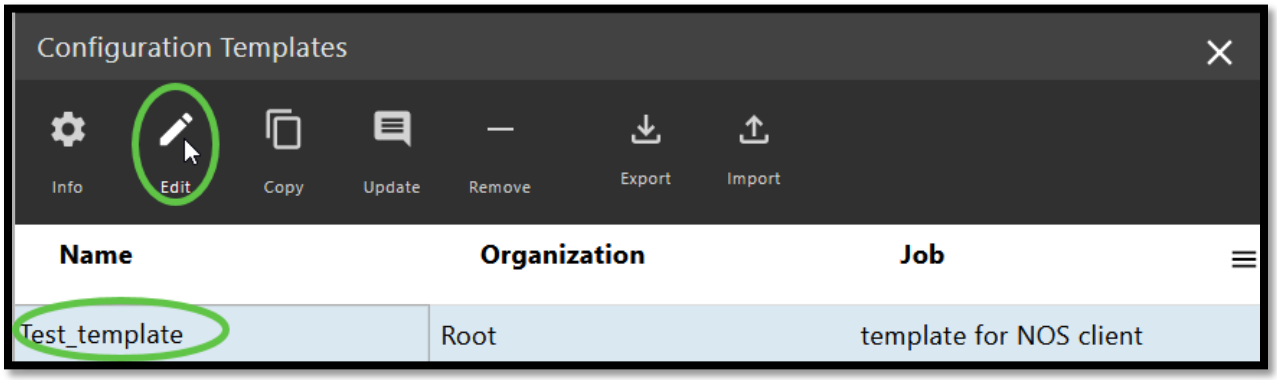
After the client checks in, confirm the result in the Job Log window and verify that the Template or Template Applied value is updated in the Clients list.

8.3.4 Editing an existing template that is assigned to an Auto-Config Group

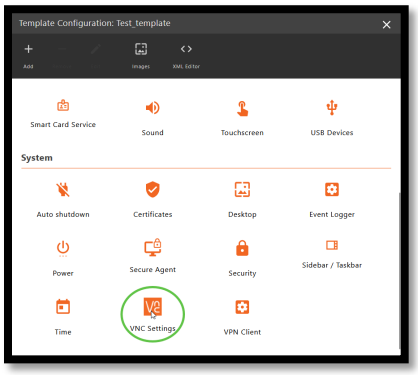
This example edits an assigned template and changes the VNC service startup setting.

The change sets **VNC Server Startup** to **On Boot** instead of **On Demand**. This allows VNC connections without waiting for an on-demand session.

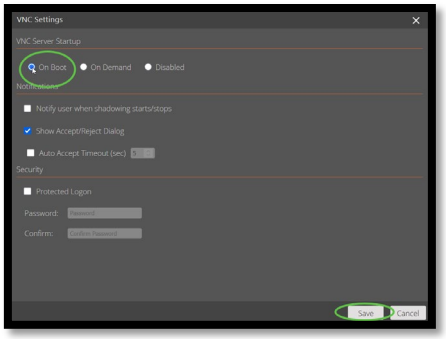
1. Click **Templates** in the **Management** menu.
2. Select the template.



3.
4. Click **Edit**.
5. In the **Configuration** window, open **VNC Settings**.



6. Locate **VNC Server Startup**.



7. Select **On Boot**.
8. Click **Save**.
9. Click **OK** in the **Configuration** window.
10. Click **OK** in the **Configuration Template** window to save the template.

The next time the client checks in, the updated template settings are applied. The **Job Log** window shows the update, and the template status appears next to the client in the **Thin Clients** list.

Testing: Test template changes thoroughly before deployment. This is especially important for changes that may restart the client, reset the client, or refresh the desktop.

When possible, apply disruptive template changes outside business hours or notify users before the changes are applied. Production changes should be tested in a lab or UAT environment before being deployed live.

8.3.5 Copying an existing template, modifying it, and assigning it to an Auto-Config Group

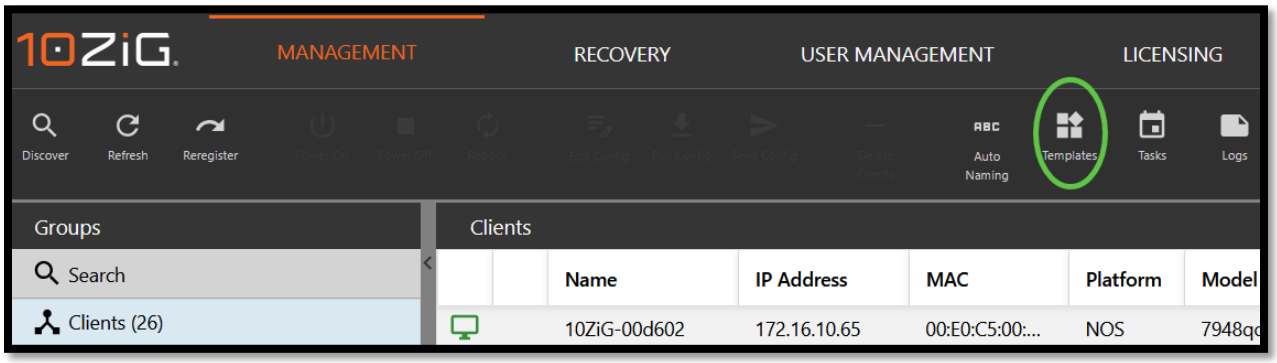
This section explains how to copy an existing template, modify the copy, and assign the new template to an Auto-Config group.

In this example, the copied template keeps the existing VNC settings and adds a change that disables the onboard speaker. The updated template then replaces the previous template assigned to the **NOS-M-DEVICES** group.

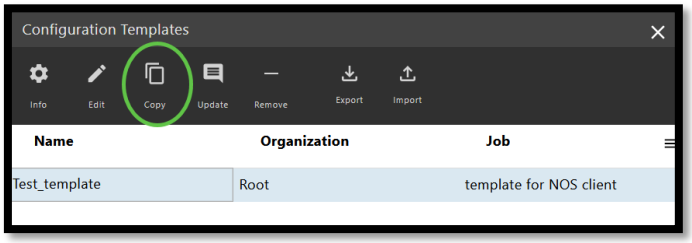
NOTE: Copying and updating templates is recommended. It allows you to maintain a single template that contains the required settings, which is easier to manage than several layered templates.

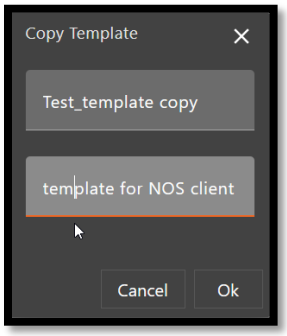
Copying an existing template to a new one and updating its description

1. Open the **Configuration Templates** screen.



2. Select the existing template.
3. Click **Copy**.





4. Rename the copied template with a clear name.
5. Select the new template.
6. Click **Edit**.
7. Enter a clear comment that explains what the template does.
8. Click inside the template dialog box again.
9. When prompted, click **Yes** to save the updated comment.

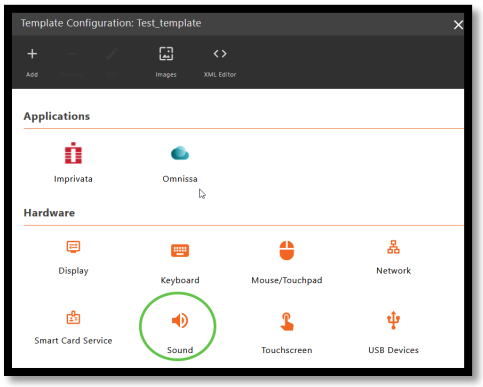
Use meaningful template names and comments. Include dates, version numbers, and a short description of the changes.

Editing the copied template

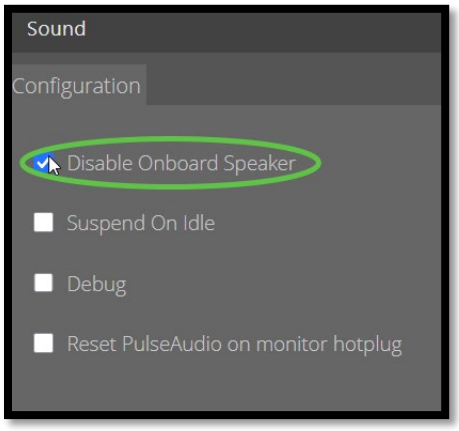
This example disables the onboard speaker.

1. Select the copied template.
2. Click **Edit**.

3. In the **Configuration** window, select **Sound** by double clicking.



4. Select **Disable Onboard Speaker**.



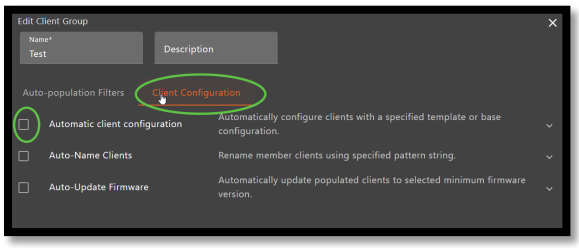
5. Click **Save**.
6. Click **OK** in the **Configuration Template** window to save the template.

Assigning the new template to the group "NOS-M-Devices" to replace the existing "Auto-config" template

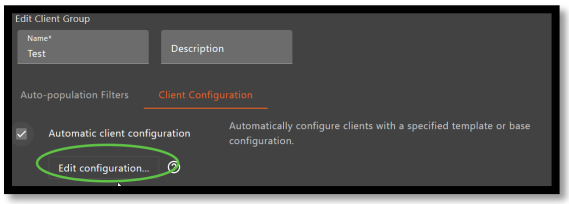
This example replaces the existing Auto-Config template assigned to **NOS-M-Devices**.

1. Right-click the group.
2. Select **Edit**.
3. Open the **Client Configuration** tab.

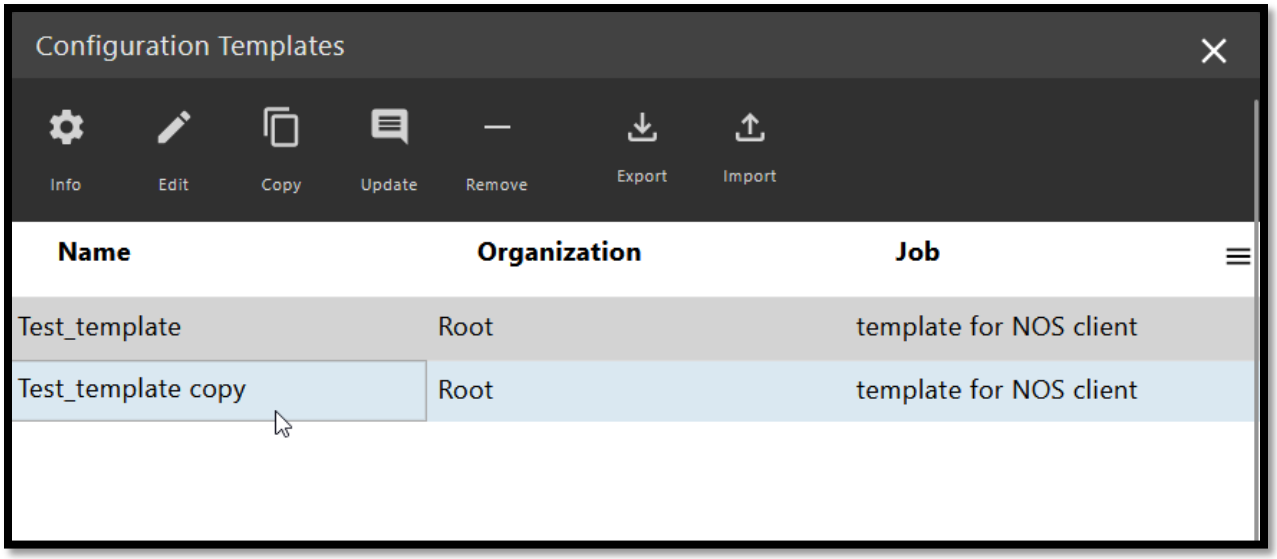
4. Check the **Automatic Client Configuration** box.



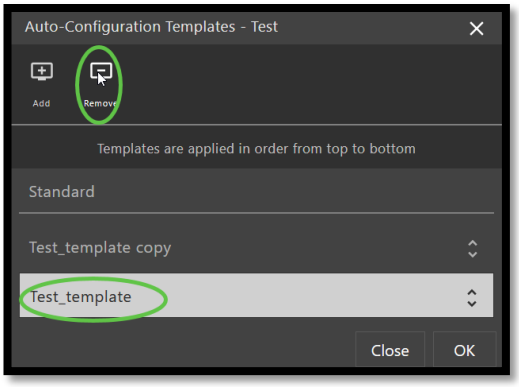
5. Click **Edit Configuration**.



6. Click **Add.**
7. When the **Stacking Configuration** message appears, click **OK**.
8. Select the new template.
9. Click **OK**.



10. Select the old template.



11. Click **Remove**.
12. Confirm that only the new template remains assigned to the group.
13. Click **OK**.
14. Click **OK** again.

How to check that the "Automatic Client Configuration" has been applied

You can confirm that the template was applied by checking the Job Log window and the Template or Template Applied columns in the Clients list.

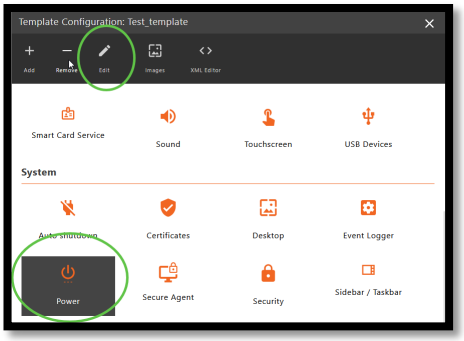
8.3.6 Removing Configuration items from your templates to prevent propagation to your 10ZiG Linux clients

You may want users to manage some settings locally while still applying other settings globally. To do this, remove specific configuration items from the template.

This example removes **Power** settings from a template. After removal, the template no longer overwrites local power settings on assigned clients.

As a best practice, copy the existing template first. Edit and test the copy before applying it to clients or groups.

1. Select **Templates** at the top.
2. Highlight the template you want to edit.
3. Select **Edit.**
4. In the **Configuration** window, select the **Power** applet.



5. Click **Remove**.
6. When prompted, click **OK** to confirm.
7. Confirm that the **Power** applet has been removed.
8. Click **OK** in the **Configuration Template** window to save the template.
9. Close the template dialog box.

The next time the template is applied, it will not apply Power settings.

To configure Power settings locally on the client:

1. On the 10ZiG Linux Client, open **Control Panel** by selecting the gears icon.
2. Open **Power**.
3. For **Power Button**, select **Do Nothing**.
4. Click **Save**.
5. Close **Control Panel**.

Future deployments of this template will not replace the local Power settings because Power settings were removed from the template.

8.3.7 Best Practices for your Templates

Follow these practices when creating and applying templates.

Template Naming and Descriptions

Use clear names and comments. Include version numbers, dates, and a summary of changes so administrators can understand what each template does and when it was created.

Copying and Editing Previous Templates

If a group already uses an Automatic Client Configuration template, copy the existing template and add new changes to the copy. Assign only the updated template to the group when possible. This avoids confusing template layering.

Deleting settings from templates

Copy the existing template before removing settings. Test the copied template before applying it to production clients or groups.

Testing your templates

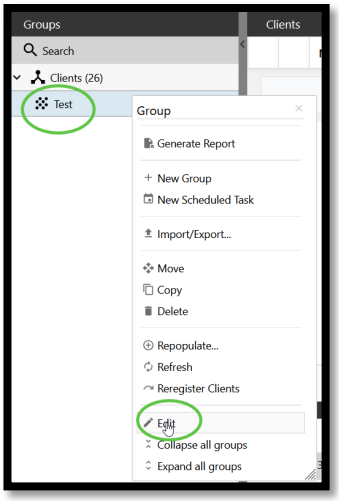
Test template changes thoroughly, especially changes that may restart clients, reset clients, or refresh the desktop.

If changes may interrupt users, apply them outside business hours or notify users before deployment.

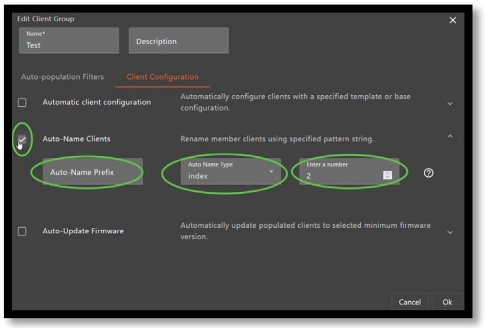
8.4 Adding Client Configuration Auto Naming to the Group

You can configure a group to automatically rename 10ZiG Linux Clients that register with it.

This example prefixes each device name with `TECHSVC-` followed by the last seven characters of the device MAC address.

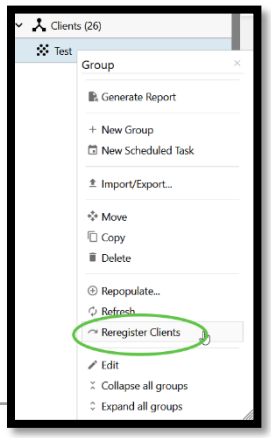


1. Right-click the **NOS-M-DEVICES** group.
2. Select **Edit**.
3. Open the **Client Configuration** tab.
4. Select **Auto-Name Clients**.



5. Enter the prefix **TECHSVC-**.
6. Select **MAC** from the dropdown list.
7. Use the up and down arrows to include the last seven characters of the MAC address.
8. Click **OK** to save the group settings.

To apply the new naming settings to existing registered clients, re-register the clients.



1. Right-click the **NOS-M-DEVICES** group.
2. Select **Reregister Clients**.
3. Check the **Job Log** window for the rename task.
4. Confirm that the client name has changed in the **Thin Clients** window.

If Secure-connected clients were discovered before the group was created, use **Repopulate** to add those clients to the group.

9. How to Retrieve, Edit, and Send your remote 10ZiG Linux Client Configs

This section explains how to remotely configure 10ZiG Linux Clients from the Web Console.

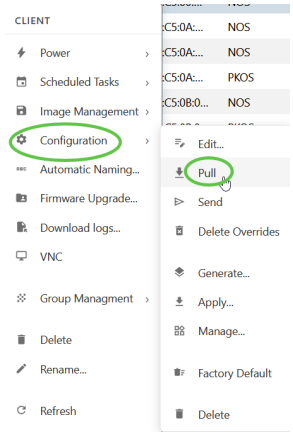
The basic workflow is:

1. Retrieve the current client configuration.
2. Edit the configuration.
3. Send the updated configuration back to the client.

9.1 Retrieving your 10ZiG Linux Client Config

Retrieve the client configuration before editing it.

1. Select the 10ZiG Linux Client from the list.



2. Click **Configuration > Pull.**

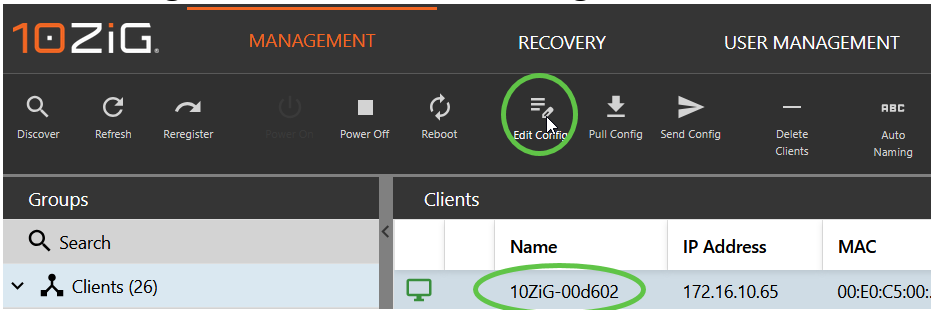
3. Check the **Job Log** window to confirm that the configuration was retrieved successfully.

9.2 Editing the Retrieved Config Settings of your 10ZiG Linux Client

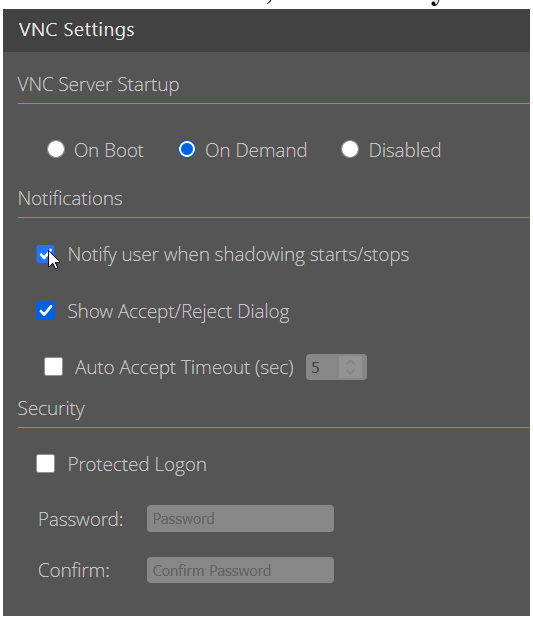
After the configuration is retrieved, you can edit client-specific settings and save them.

This example enables VNC shadowing notifications. When enabled, the client displays a notification when a VNC shadowing session starts or stops.

1. Select the 10ZiG Linux Client.
2. In the **Management** menu, click **Edit Config**.



3. When the configuration screen opens, select **VNC Settings**.
4. Under **Notifications**, select **Notify user when shadowing starts/stops**.

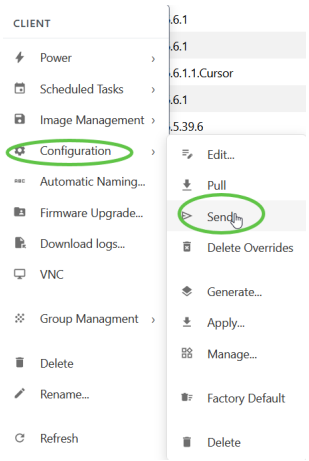


5. Click **Save**.

9.3 Sending the Config Settings back to your 10ZiG Linux Client

Configuration options available from the **Management** menu are also available by right-clicking a Linux client and selecting **Configuration**.

From the context menu, you can choose:



- **Edit**
- **Retrieve**
- **Send**

To send a saved configuration:

1. Right-click the Linux client.
2. Select **Configuration > Send**.
3. Check the **Job Log** window to confirm that the configuration was sent successfully.

9.4 Which configuration settings require reboots or soft resets/desktop restarts?

Some configuration changes require a desktop refresh, desktop restart, or full reboot.

The example in the previous section did not require a restart or reboot. Other settings may require one.

This is important when changes are applied during business hours. If a change may interrupt users, notify them first or schedule the change outside normal operating hours.

Configuration dialogs use symbols such as **+** or ***** to indicate settings that may require a reset or reboot.

Hardware

Display settings

When you open **Display** under **Hardware**, a **Configuration Modification Note** may appear. The note explains that changing this configuration may trigger a reboot or desktop restart when deployed to a client.

If you do not want to see the note each time, clear **Always show this message**.

Changing the Display Resolution and sending the config to the 10ZiG Linux Client

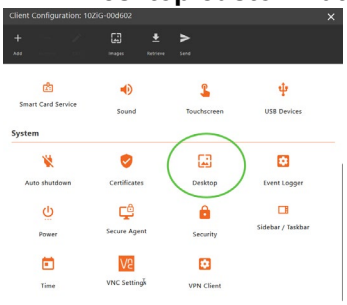
If you change the display resolution and send the configuration to the Linux client, the client may display a **Desktop Restart Required** message. The desktop restarts to apply the new settings.

System

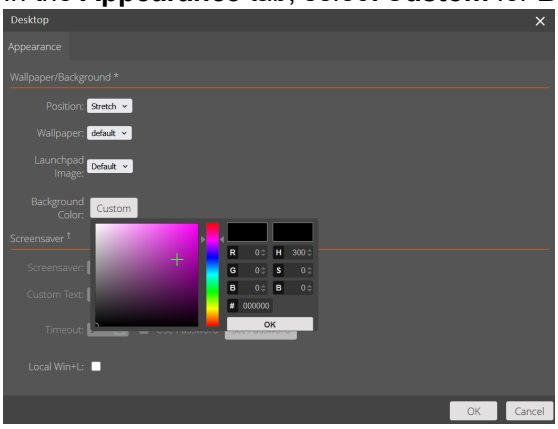
Changing the Desktop Colour and sending the config back to the 10ZiG Linux Client

This example changes the desktop background color and sends the configuration back to the client.

1. Select the 10ZiG Linux Client from the list.
2. Click **Configuration > Edit.**
3. In the **Desktop customization** window, review the available options.



   - **Wallpaper/Background** changes may require a desktop refresh.
   - **Screensaver** changes may require a desktop restart.
4. In the **Appearance** tab, select **Custom** for **Background Color**.



5. Choose a color.
6. Click **OK**.
7. Click **OK** in the **Desktop customization** window.
8. Click **OK** in the **Configuration** window.

9. When prompted to send the configuration, click **Yes**.

When the client receives the configuration, it may display a **Desktop Refresh Required** message. After a few seconds, the desktop refreshes and the new background color is applied.

---

10. Applying Firmware and Addon Upgrades to your 10ZiG Linux Clients and Client Groups

This section explains how to apply firmware and addon updates to 10ZiG Linux Clients.

Updates can be applied at the client level or group level.

At the group level, you can apply updates by:

- Adding firmware or addon updates to the group's **Client Configuration** using **Auto-Update Firmware**.
- Creating a scheduled task that runs the **Update Device Firmware** action.

At the client level, you can apply updates by:

- Selecting one or more clients and applying firmware or addons from the client context menu.
- Creating a scheduled task for one or more selected clients.

Scheduled firmware and addon task examples are covered in the Task Scheduler section.

10.1 Applying Firmware and Addon Updates to individual 10ZiG Linux Clients

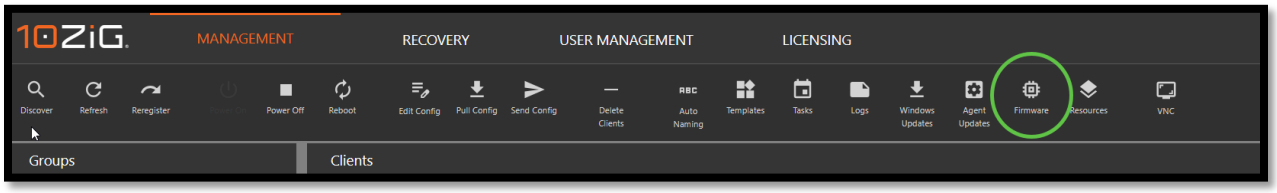
1. Select one or more 10ZiG Linux Clients in the **Clients** window.
2. Click **Firmware** on the **Management** menu.
    - Alternatively, right-click the client and select **Firmware Upgrade**.

Importing and Installing your Firmware Updates

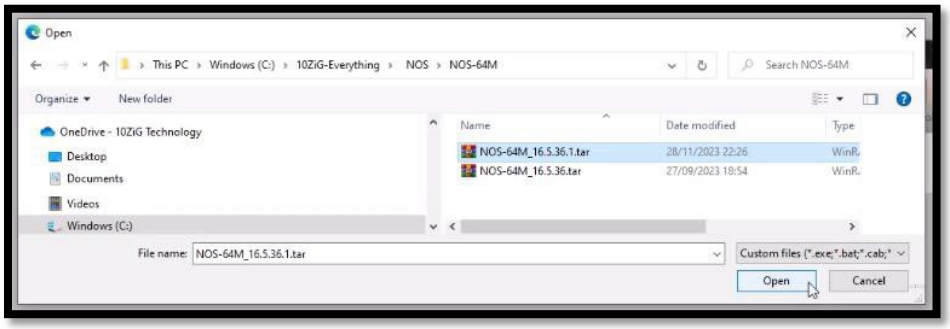
If firmware or addon packages are already installed, they appear in the list under the platform name or addon category.

To import firmware or addons:

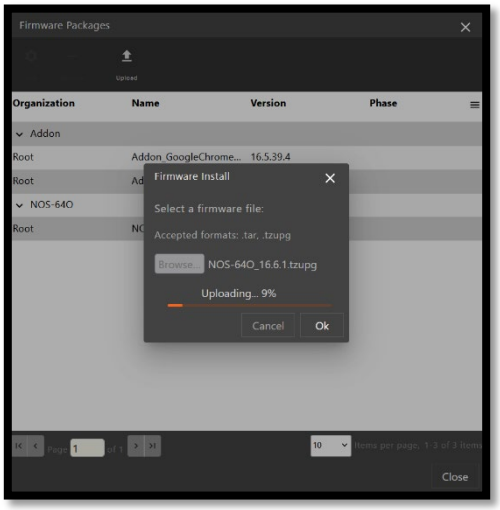
1. Click **Firmware**.



2. When the file selection window appears, click **Upload**.
3. In File Explorer, locate the firmware or addon package.
4. Select the package.
5. Click **Open**.
6. When prompted, click **Yes** to upload the file.
7. Wait for the upload to complete.
8. Select the uploaded package.
9. Click **Install** to install it on the 10ZiG Manager Server.



After installation, the package appears in the firmware list.



To apply the update:

1. Select the installed package.
2. Click **Apply**.
3. Confirm the action when prompted.
4. Monitor progress in the **Job Log** window.

When the upgrade completes, the client displays a reboot message.

Importing and Installing your Addon Updates

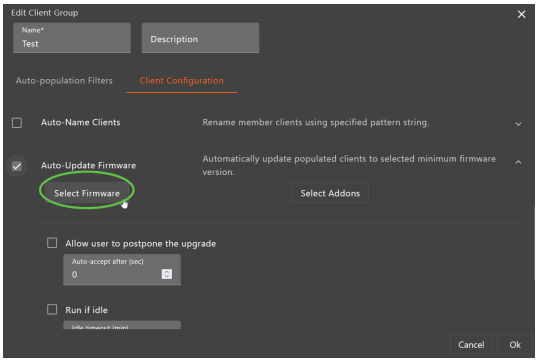
Addon updates use the same import and installation process as firmware updates. After they are imported and installed, they appear in the firmware packages window.

10.2 Setting your Group's Client Configuration to Automatically apply Firmware and Addon Updates

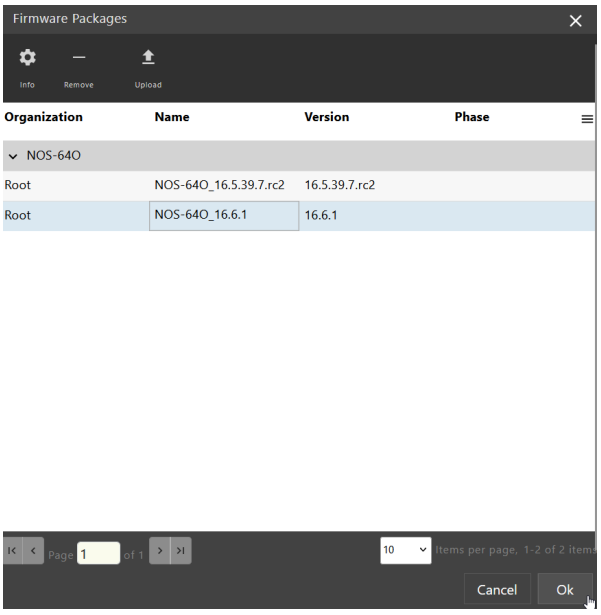
You can configure a group to automatically apply firmware or addon updates to Linux clients when they register with the group.

This example applies firmware version **16.5.36.1** to Linux clients in a group.

1. Right-click the group.
2. Select **Edit**.
3. Open the **Client Configuration** tab.
4. In **Auto-Update Firmware**, click **Select Firmware**.

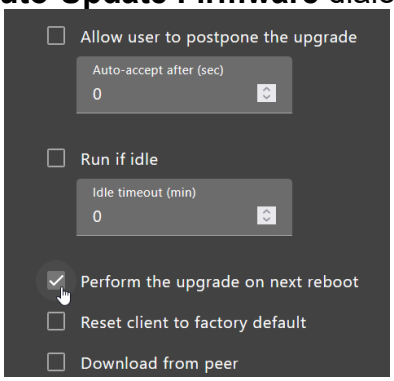


5. Select the platform heading, such as **NOS-64M**.
6. Select the firmware release, such as **NOS-64M_16.5.36.1**.



7. Click **OK**.

8. In the **Auto-Update Firmware** dialog, select **Perform the upgrade on next reboot**.



9. Click **OK**.

To start the update:

1. Select the client.
2. Click **Reboot**.
3. As the client restarts, the group's Auto-Update Firmware settings apply.

The firmware update progress appears on the client and in the **Job Log** window. After the update completes, the client performs a final reboot.

---

11. The 10ZiG Manager Task Scheduler

The Task Scheduler allows you to create scheduled tasks for individual 10ZiG Linux Clients or client groups.

This section explains available task actions, scheduling options, and example tasks.

11.1 Adding a scheduled task to your 10ZiG Linux Clients and groups

You can create scheduled tasks in several ways.

For individual clients or selected groups of clients:

1. Select one or more clients.
2. Click **Add Task** in the **Maintenance** menu.
    - Alternatively, right-click the selected clients and choose **Add Scheduled Task**.

For a group:

1. Right-click the group.
2. Select **New > Scheduled Task**.

The Task Scheduler screens are the same for both clients and groups.

11.2 Task Names

A task name can be any value, but it should clearly describe the task.

Use descriptive names when you have many groups, clients, or recurring tasks. Clear names make it easier to edit, remove, and troubleshoot scheduled tasks later.

For example, a vague name such as `SENDGROUP1-A-MESSAGE` may not be helpful if several message tasks exist. A better name should identify the message purpose, target group, and scheduled date or time.

11.3 Scheduled Task Actions

The following actions are available in the Task Scheduler.

Power-on client

Powers on supported clients through Wake-on-LAN (WOL).

Reboot Client

Restarts the selected 10ZiG Linux Client.

Shutdown client

Shuts down and powers off the selected 10ZiG Linux Client.

Update device firmware/addon

Applies selected firmware or addon packages to Linux clients.

Apply template configuration

Applies a selected template to 10ZiG Linux Clients or client groups.

Reset to factory default

Resets selected 10ZiG Linux Clients to factory default settings.

Display a message

Displays a message on selected 10ZiG Linux Clients. The message includes an acknowledgment button.

11.4 Scheduled Task – Start Date and Time

Start Date

The start date is based on the 10ZiG Manager Server time. For tasks with a frequency of **Once**, this is the date the task runs.

Start Time

The start time is the execution time based on the 10ZiG Manager Server.

Check the AM or PM setting carefully. For example, confirm that a task intended for 8:00 PM is not scheduled for 8:00 AM.

11.5 Scheduled Task – Frequency

Note: If the start date is today, the task runs only if the start time has not already passed. For example, if a one-time task is scheduled for 1:00 PM but saved at 1:01 PM, move the start time to a future time.

Once

Runs the task one time on the selected start date and start time. The task is not rescheduled.

On Interval

Runs the task at the selected start time, then repeats after the configured number of minutes.

The maximum interval is 1440 minutes, or 24 hours.

For example, to run a task every hour starting at 8:00 AM, set the start time to 8:00 AM and the interval to 60 minutes.

Daily

Runs the task every day at the selected start time. If today's start time has already passed, the first run occurs the next day.

Weekly

Runs the task on selected days of the week at the selected start time.

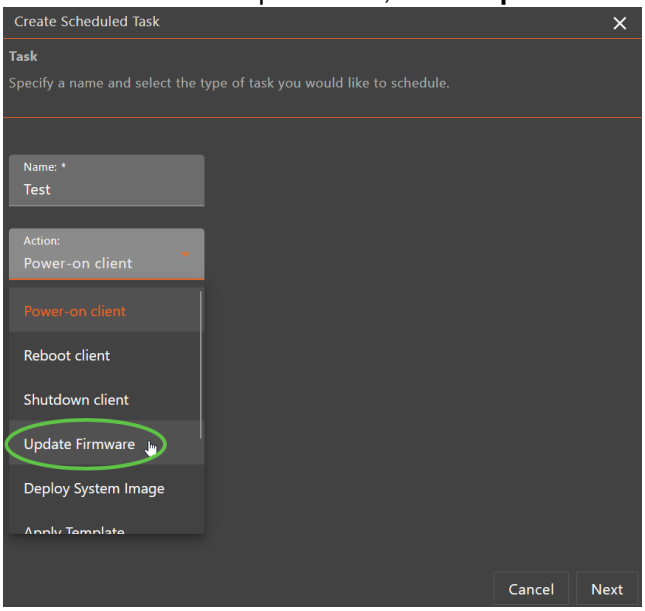
For example, you can schedule a task to run every Saturday and Sunday at 10:00 PM.

11.6 Scheduled Task Examples

Update device firmware/addon

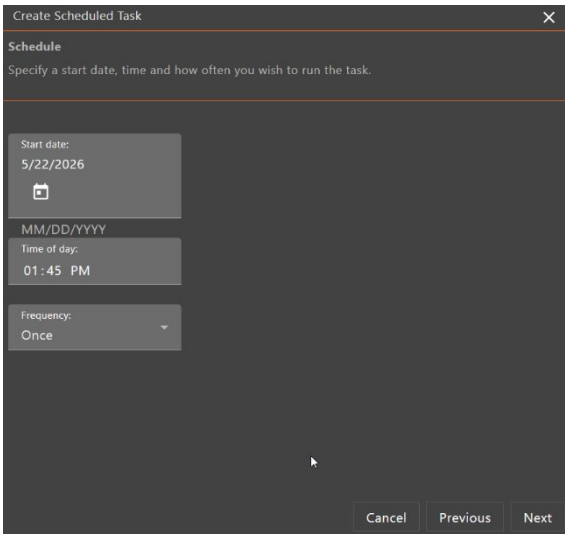
This example creates a scheduled task to apply a firmware update.

1. Right-click the group.
2. Select **New Scheduled Task.**
3. In the **Create Scheduled Task** window, enter a task name.
4. From the **Action** dropdown list, select **Update firmware**.



5. Click **Next**.
6. In the **Firmware Packages** window, select the package to apply.
    - This can be a firmware update or an addon.

7. If required, select the option to reset the client to factory defaults before the update.
8. Click **Next**.
9. Set the start date, start time, and frequency.
10. Click **Next** to review the summary.
11. Click **Finish** to save the task.

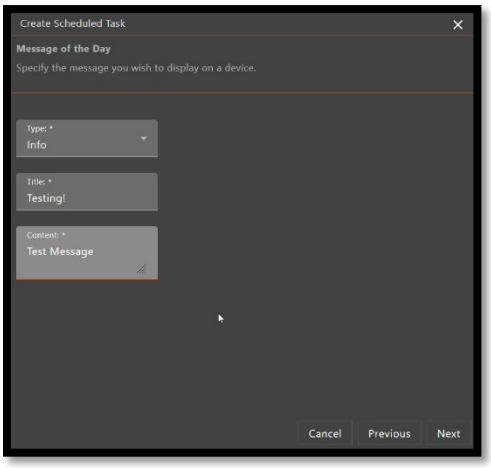


To change any settings before saving, click **Previous**, make the changes, and continue to **Finish**.

Display a Message

This example creates a scheduled task to display a message on client devices.

1. In the **Add Scheduled Task** window, enter a task name.
2. Select **Display a message** as the action.
3. Click **Next**.
4. Select the message type.
5. Enter the message title.
6. Enter the message text.
7. Click **Next**.
8. Set the start date, start time, and frequency.
9. Click **Next** to review the summary.
10. Click **Finish** to save the task.



11.7 Scheduled Task Results for Execution of "Display a Message" Task

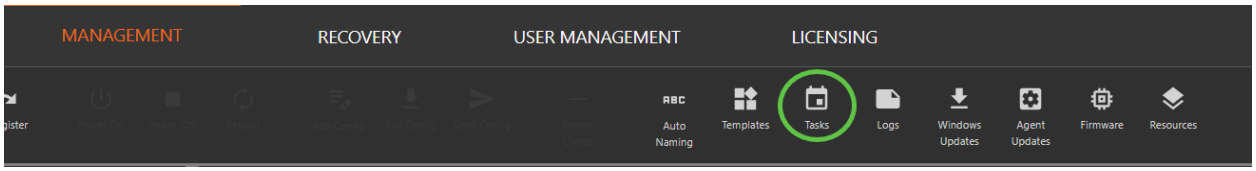
After a **Display a Message** task runs, the results appear in the **Job Log** window.

If you connect to the client through VNC, you can verify that the message appears on the client screen.

11.8 Editing or Deleting your tasks

To edit or delete scheduled tasks:

1. Open **Tasks.**



2. Select the task.
3. Choose whether to modify or remove it.

If you remove a task before its next scheduled run, the task will not run. Confirm that the task is no longer needed before deleting it.

12. Remote Controlling your Clients - VNC

This section explains how to control Linux clients remotely by using the built-in VNC viewer.

12.1 Connecting to the client via VNC

Earlier sections explained how to configure VNC settings, including user notifications when a remote session starts or stops.

To connect through VNC:

1. Select the client.
2. Click **VNC** in the **Management** menu.

After the connection succeeds, the client displays a notification if VNC notifications are enabled. The notification informs the user that the desktop is visible to someone shadowing the device.

During the VNC session, you can:

- Control the device remotely.
- Open the browser VNC window in full-screen mode.
- Disconnect from the session.

To exit full-screen mode, press **Esc**.

12.2 Disconnecting from the client via VNC

To disconnect from the remote VNC session, click **Disconnect**.

If VNC notifications are enabled, the client displays a message telling the user that the remote session has ended.

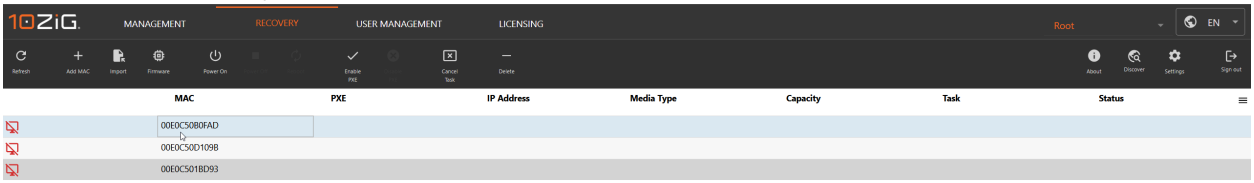
13. Recovery

The Recovery tab provides recovery tools for supported 10ZiG clients. Use it when a device cannot be restored through standard configuration, firmware, or scheduled-task workflows.

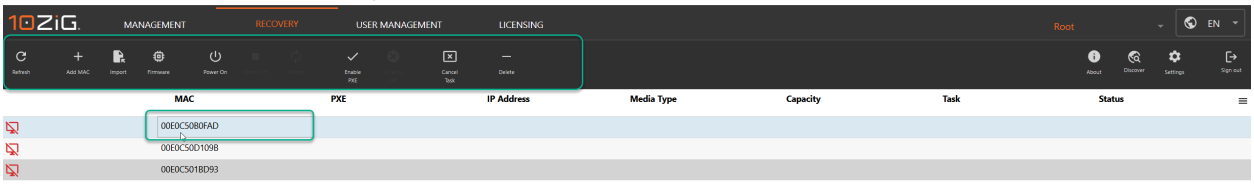
Recovery options can vary by client platform, firmware version, installed recovery components, and user permissions. If an expected option is not visible, confirm that the device supports the workflow and that the signed-in account has the required access.

13.1 General Recovery Workflow

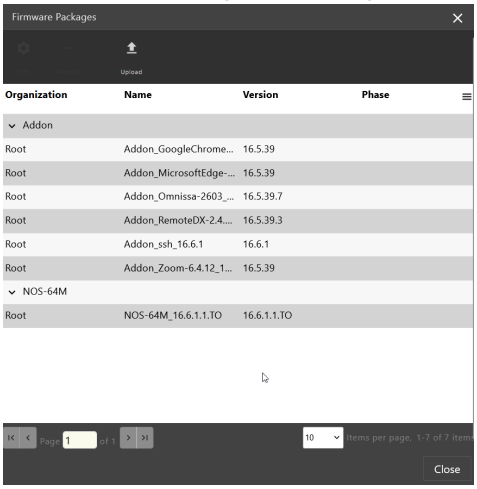
1. Open the Recovery tab.



2. Select the required recovery function.



3. Confirm the target device, group, image, or recovery resource.



4. Review any warning or confirmation message before starting the action.
5. Monitor the action in the Job Log window.
6. Verify the client state after recovery completes.

Recovery actions may interrupt device availability. Schedule recovery work outside normal operating hours where possible, or notify affected users before starting the action.

14. User Management

The User Management tab controls access to the 10ZiG Manager Web Console. Use it to manage local users, roles, Organizations, and supported external identity providers.

User Management determines who can sign in, which administrative functions they can use, and which Organization resources they can access.

14.1 Root-Level and Organization-Scoped Access

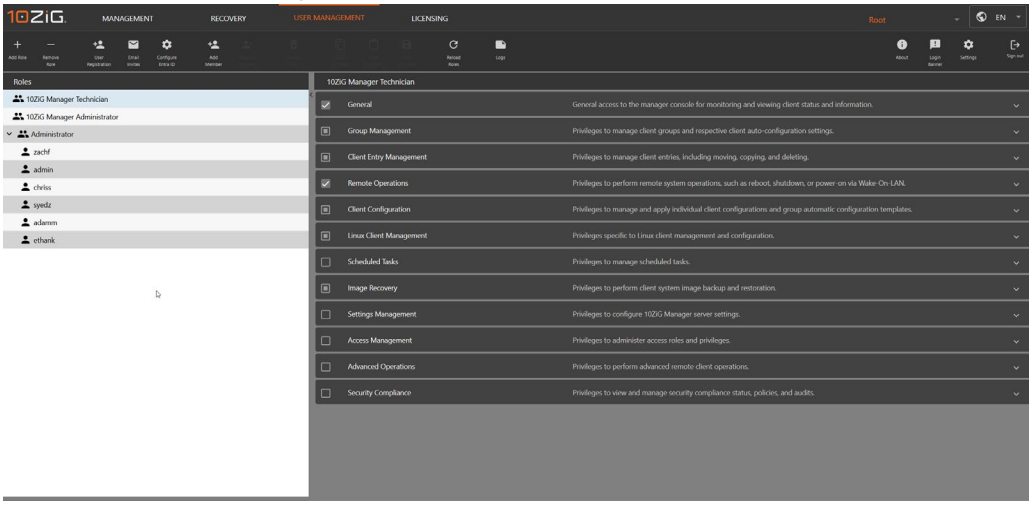
The root-level administrator has system-wide access to the 10ZiG Manager environment. Root-level access should be restricted to administrators who manage global settings, Organizations, licensing, and system-wide access.

Organization-scoped users should only see the clients, groups, templates, and actions assigned to their Organization and permitted by their role. Use the principle of least privilege when assigning access.

14.2 Creating and Managing Users

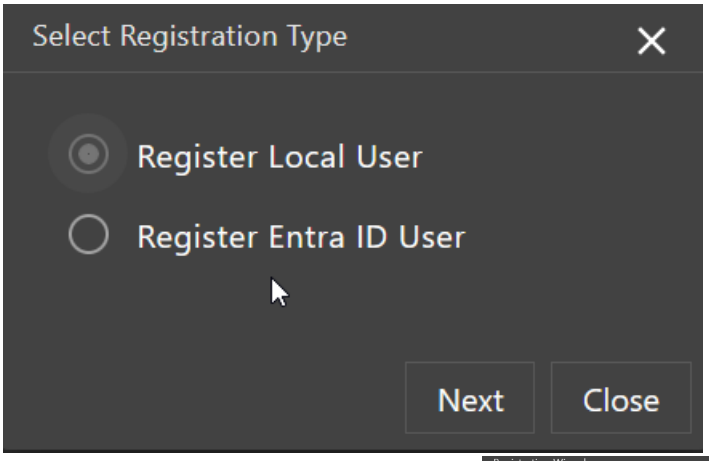
Use User Management to create accounts, assign roles, change Organization access, and remove accounts that are no longer required.

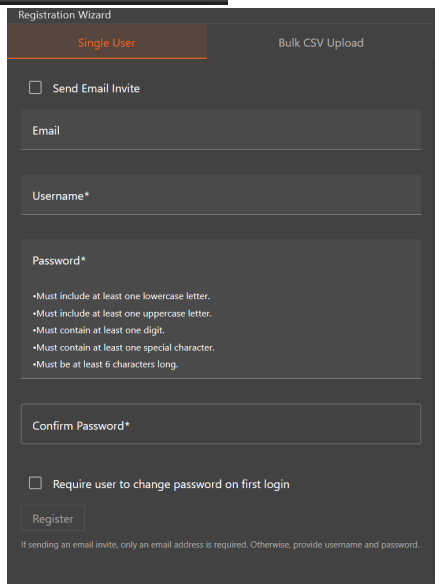
1. Open the User Management tab.



2. Select the user registration or user creation option.

3. Choose whether the account is a local user or uses a supported external identity provider.





4. Enter the required user information.
5. Assign the appropriate role and Organization access.
6. Save the account.
7. Test sign-in and access before the user manages production devices.

Disable or remove accounts promptly when access is no longer required. Review users, roles, and Organization assignments regularly.

14.3 Directory and Identity Provider Integration

Supported directory and identity provider integrations centralize authentication and simplify account administration. Configure integrations only after confirming the required identity-platform permissions, callback addresses, and role-mapping plan.

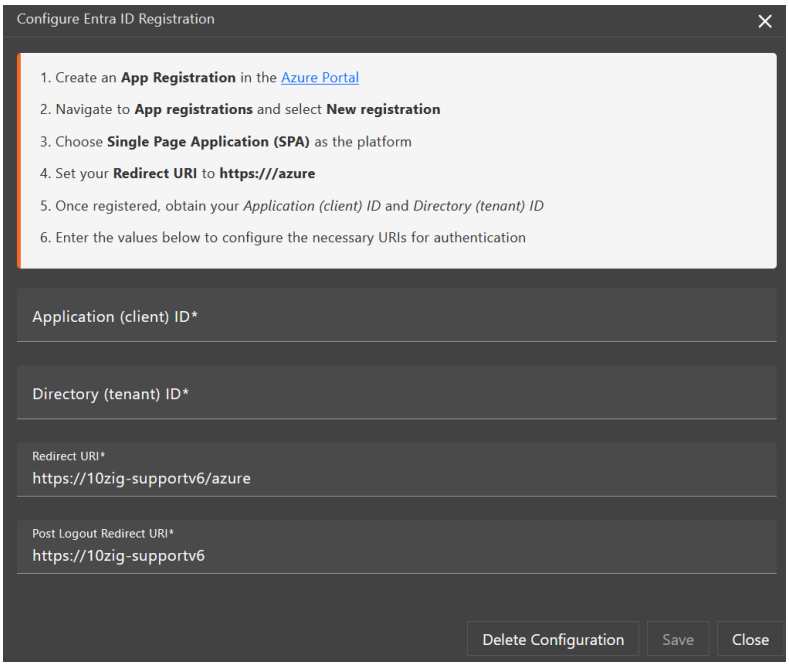
14.3.1 Microsoft Entra ID Integration

Microsoft Entra ID integration allows the Web Console to use Entra ID as an external identity provider, where supported and configured.

Before configuration, confirm that the required Entra tenant, application registration, redirect URI, credentials, and administrator permissions are available.

General Entra ID Configuration Workflow

1. Create or confirm the required application registration in Microsoft Entra ID.
2. Confirm the redirect URI required by the 10ZiG Manager Web Console.
3. Create the required client credential, such as a client secret or certificate.



4. Enter the tenant ID, client ID, and credential details in 10ZiG Manager User Management.
5. Map Entra users or groups to the correct 10ZiG Manager roles and Organizations.
6. Test sign-in with a limited test account before enabling production access.

If a user can authenticate but cannot see the expected devices or actions, verify the assigned role and Organization access in 10ZiG Manager.

14.3.2 Active Directory Integration

Active Directory support is expected in a future 10ZiG Manager release. Add the final configuration workflow and screenshots here after the feature, labels, and supported authentication method are confirmed.

Do not publish configuration steps for Active Directory until the installed Manager version explicitly supports the feature. Refer to the applicable release notes.

14.4 Authentication and Access Best Practices

- Limit root-level access to administrators who require system-wide control.
- Use Organization-scoped accounts for delegated administration.
- Assign the minimum permissions required for each role.
- Test new authentication integrations and role mappings with a limited account.
- Maintain at least one tested local administrative account before changing external authentication.
- Review users, roles, and Organization assignments regularly.

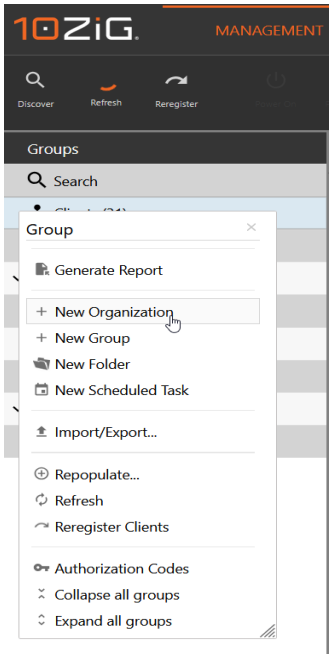
15. Organizations and Multi-Tenancy

Organizations provide multi-tenancy support in 10ZiG Manager. They separate devices, users, roles, and administrative boundaries within a single Manager environment.

Organizations are useful when one 10ZiG Manager instance manages multiple customers, departments, regions, or business units. For example, a managed service provider can separate customer environments, while an internal IT team can separate departments or administrative regions.

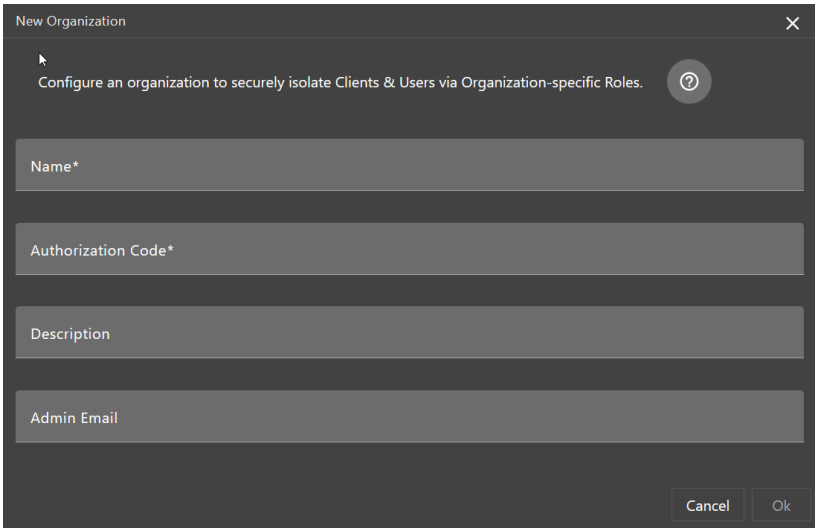
15.1 Creating an Organization

1. Open the Management tab.
2. Right click on the ‘Clients’ on the left side of the menu.



3. Select the option to create a new Organization.

4. Enter a clear Organization name and any required details.



5. Save the Organization.
6. Assign the appropriate users, roles, and clients to the Organization.

15.2 Organization Authorization Codes

An Organization authorization code can be used when a client must register directly into a specific Organization through Secure Agent. This is separate from connecting a client through Secure Connector without Organization assignment.

Use an Organization authorization code when devices must automatically appear under the correct tenant or administrative boundary during registration.

15.3 Organization Best Practices

- Use names that clearly identify the customer, department, region, or business unit.
- Restrict root-level access to trusted administrators.
- Assign users to the correct Organization and role before device management begins.
- Test registration with one client before onboarding a larger group.
- Document which authorization code belongs to each Organization and restrict access to those codes.

16. Licensing

The Licensing tab displays and manages 10ZiG Manager license information. Use it to confirm license status, licensed features, capacity, and any renewal or activation requirements.

Available information and actions can vary by license type and deployment model.

16.1 General Licensing Workflow

1. Open the Licensing tab.
2. Select Install.
3. Choose the license file to upload.
4. Import, activate, or update license information when required.
5. Save the change and confirm that the expected license status is displayed.

If the expected licensing information is not displayed, verify network connectivity, license validity, server time, and the permissions of the signed-in user.

17. Supporting Complimentary Video

10ZiG has a YouTube video called **Intro, Mgmt, & Best Practices of 10ZiG's Latest Linux v16.5 Firmware for 10ZiG NOS, PeakOS & RepurpOS**. This video complements the guide and covers the topics mentioned here.

Support

If you require support for any information in this document, contact your region's nearest Technical Support Center.

10ZiG Technology, Inc

Headquarters USA (North America)
2043 W. Lone Cactus Drive
Phoenix, AZ 85027
Phone: 866-865-5250
support@10zig.com
sales@10zig.com
www.10zig.com

10ZiG Technology Limited

Headquarters UK (EMEA)
7 Highcliffe Road
Leicester
LE5 1TY
UK
Phone: +44 (0)116 2148661
support@10zig.eu

sales@10zig.eu
www.10zig.eu