## Contents

Content .......................................................................................................................... 2
Quick Network Management Agent overview ..................................................................... 1
Package contents ........................................................................................................... 1
Preparing to install the Management Agent ................................................................. 2
Installing the Management Agent ................................................................................... 2
  First-time BakPak users ............................................................................................... 5
  Registering your Management Agent ........................................................................... 6
  RK-1 ............................................................................................................................ 8
  WR-1 ............................................................................................................................ 9
Accessing BakPak ............................................................................................................. 10
  Using the Wizard to set up accounts .......................................................................... 11
    Wizard for administrators ....................................................................................... 11
    Using the Technician Wizard ................................................................................... 16
Sub-agent features ............................................................................................................ 16
  Using two-way authentication .................................................................................. 18
    Logging in to BakPak using Authy Soft Token ....................................................... 20
    Logging in to BakPak using Onetouch ................................................................. 21
  Editing user information ............................................................................................ 22
Sites .................................................................................................................................. 24
  Removing a site .......................................................................................................... 26
  Scan for devices and device priority .......................................................................... 27
  Setting device priorities ............................................................................................. 29
  Setting device categories ......................................................................................... 31
  Adding devices manually ......................................................................................... 32
  Viewing all discovered and added devices .................................................................. 33
  Triplex .......................................................................................................................... 34
  Creating a network map ............................................................................................. 34
  Scanning across VLANs (Pakedge Zones) .................................................................. 38
Device information .......................................................................................................... 40
  Configuring VLANs on SX Series switches .............................................................. 42
  Control4 and BakPak .................................................................................................... 44
  Device Control ............................................................................................................ 46
    Example .................................................................................................................... 51
  Device Portal ............................................................................................................... 54
  Port monitoring .......................................................................................................... 55
  DDNS ............................................................................................................................ 57
  Management Agents .................................................................................................... 57
    Site recovery under a new Management Agent ..................................................... 58
Devices .............................................................................................................................. 59
  Group Management .................................................................................................... 59
    Firmware Management ............................................................................................. 60
    Configuration Management ...................................................................................... 61
    Power Control .......................................................................................................... 62
    Self-Healing .............................................................................................................. 66
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Priorities</td>
<td>67</td>
</tr>
<tr>
<td>Categories</td>
<td>67</td>
</tr>
<tr>
<td>Users</td>
<td>67</td>
</tr>
<tr>
<td>View/Create</td>
<td>67</td>
</tr>
<tr>
<td>Assigning permissions</td>
<td>69</td>
</tr>
<tr>
<td>Authy Management</td>
<td>71</td>
</tr>
<tr>
<td>Alerts</td>
<td>72</td>
</tr>
<tr>
<td>Manage</td>
<td>72</td>
</tr>
<tr>
<td>Actions</td>
<td>74</td>
</tr>
<tr>
<td>On-demand reports</td>
<td>74</td>
</tr>
<tr>
<td>Emailed Reports</td>
<td>75</td>
</tr>
<tr>
<td>Speed Test</td>
<td>76</td>
</tr>
<tr>
<td>Diagnostics</td>
<td>77</td>
</tr>
<tr>
<td>Collaboration</td>
<td>78</td>
</tr>
<tr>
<td>Contact Us</td>
<td>78</td>
</tr>
<tr>
<td>Limited Warranty</td>
<td>1</td>
</tr>
</tbody>
</table>
Quick Network Management Agent overview

With the Pakedge Network Management Agent (or just Management Agent), view diagnostics, check uptime and downtime, manage network devices, and perform reboots remotely. These features save both time and money that would otherwise be spent on service calls.

The front panel of the Management Agent displays a pair of blue LEDs. See Table 1 below for more information.

<table>
<thead>
<tr>
<th>Label</th>
<th>Function</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>HDD (not on NK-1)</td>
<td>hard drive activity</td>
<td>When lit, hard drive is in use</td>
</tr>
<tr>
<td>PWR</td>
<td>power indicator light</td>
<td>When lit, indicates that the unit has power</td>
</tr>
</tbody>
</table>

*Table 1: LED definitions*

The rear panel is where the physical cabling (power, Ethernet, console) is located. Table 2 describes each port and its function.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AC Connector</td>
<td>110~260V AC</td>
</tr>
<tr>
<td>Power Switch</td>
<td>powers the Management Agent on or off</td>
</tr>
<tr>
<td>USB 1 / 2</td>
<td>optional</td>
</tr>
<tr>
<td>LAN</td>
<td>MDI/MDIX RJ45 interface for connection to the LAN</td>
</tr>
<tr>
<td>HDMI (not on NK-1)</td>
<td>HDMI display for maintenance</td>
</tr>
<tr>
<td>Console</td>
<td>local management, speed 115200bps, RJ45 interface</td>
</tr>
</tbody>
</table>

*Table 2: NP36 rear panel port description*

**Package contents**

- Management Agent
- Power cable
- Mounting brackets
- Quick start guide
BakPak Cloud Management System

- Console cable

Preparing to install the Management Agent

If you have installed a managed switch before, the process of installing the Management Agent will be similar.

**Tools required:**
- Phillips screwdriver (if using rack-mount brackets).
- PC or laptop with Ethernet interface and a web browser (an integrated DB-9 port or USB-to-serial adapter may be necessary if you would like to use the console interface).
- Ethernet cable.

Installing the Management Agent

1. Open the box and remove the Management Agent.
2. If you are mounting the Management Agent in a standard 19” AV rack, attach the rack-mount brackets to the sides (rack-mount brackets are included). If you are not rack mounting, make sure that the Management Agent is physically mounted near power and network connections (for example, near a backbone switch or firewall/router).
3. Connect power to the device and press the power switch on the rear panel. The PWR LED will light up and the fans will start.
4. If you are using a Pakedge router that has an internal IP address of 192.168.1.99, you can connect the Management Agent to an available port on your router and proceed to the section titled “First-time BakPak users.” If your router is using an IP scheme of 192.168.1.X but has an IP address other than 192.168.1.99, then continue to Step 5. If your router is using an IP scheme that is different from 192.168.1.X, then skip to Step 10.
5. Connect an Ethernet cable from the Management Agent to your router.
6. Open a web browser (Mozilla Firefox is preferred). In the browser, enter the Management Agent’s default IP address of 192.168.1.237 (NP36) or 192.168.1.240 (NK-1) into the address bar and press Enter. A web page will appear, prompting you for a username and password.
7. Enter pakedge as the username and pakedgep (NP36) or pakedgen (NK-1) as the password, then click Login to log in to the web administration portal.
8. Click **LAN Settings**.

9. In the *Default Gateway* field, enter the IP address of your router, then click **Apply** to finalize the settings. You are now ready to create a Cloud Account and register your Management Agent. Proceed to the section “First-time BakPak users.”
10. Connect an Ethernet cable from your computer directly to the Management Agent.

11. Configure the PC with a static IP address of **192.168.1.10** and subnet mask of **255.255.255.0**, and then open any browser (Mozilla Firefox is preferred).

12. In the browser, enter the Management Agent’s default IP address of **192.168.1.237** (NP36) or **192.168.1.240** (NK-1) into the address bar and press **Enter**. A web page will appear prompting you for a username and password.

13. Enter **pakedge** for the username and **pakedgep (NP36) or pakedgen (NK-1)** for the password, then click **Login** to log in to the web administration portal.

14. Click **LAN Settings**.
15. Change the IP address of the Management Agent to match your network IP scheme, then click **Update** to finalize your settings.

Now you can connect the Management Agent to your router.

**First-time BakPak users**

If you are new to BakPak, you need to create your Admin account to register your Management Agent and create accounts for your technicians. To do this, follow the steps below. If you have already created an Admin account, skip to “Registering your Management Agent.”

1. Contact our Sales department at:
   
   Email: sales@pakedge.com

   Have the email address that you wish to use ready. Our Sales department will email you a dealer registration code.

2. After you have received this code, go to mybakpak.com.
3. Click **Dealer Admin** account.

4. Fill out the required information to register for your BakPak account. Make sure to enter the dealer code you received from our Sales department, then click **Register**.

5. You have now created your Admin BakPak account. You can begin to register Management Agents under your account.

**Registering your Management Agent**

**To register your Management Agent (NP36 or NK-1):**

1. Open a web browser, enter the Management Agent’s IP address into the address bar, and press **Enter**. The default IP address is **192.168.1.237** (NP36) or **192.168.1.240** (NK-1). A web page will appear, prompting you for a username and password.
2. Enter **pakedge** for the username and **pakedgep** (NP36) or **pakedgen** (NK-1) for the password, then click **Login** to log in to the web administration portal.

After you have logged into the Management Agent, you will see the main page.

3. Click **Registration**.

You will be redirected to an agreement page.

4. Click **I Accept** to continue.

5. Enter the email address and password to the admin account for your company, enter a name for the Management Agent, select your time zone, then click **Register**.

6. Note that the customer name and customer email address are required for Management Agent registration. The customer where the management agent is going to be installed will receive an email from us and has the option to opt-out by replying to the email with the subject line “opt-out.” We will receive the email from the customer and will delete the Management Agent from our database, then we will notify the dealer.
7. You will be redirected to mybakpak.com under your account. Your Management Agent has now been registered.

**RK-1**

**To register your Management Agent on an RK-1:**

This functionality is only available on the RK-1 as of firmware 1.05.

1. After updating your RK-1 to firmware version 1.05, log in to the RK-1 GUI. A new section called BakPak will appear. Under BakPak, you will either see one or two options. If the router has been previously registered, two options will appear: **Registration** and **Manual upgrade**. If this is the first time registering the router, you will only see **Registration**. The **Registration** section allows you to connect this RK-1 to the BakPak cloud acting as a Management Agent.

2. To connect, you must first create a BakPak account with mybakpak.com. Click the **Register to BakPak** button to begin the registration process.

To register the RK-1, you must be connected to the router either through its local network or a VPN tunnel to the router.
After getting registered, BakPak will perform any required updates automatically. In the situation where BakPak is unable to update itself automatically, the **Manual Upgrade** option is available for users to load a BakPak firmware file to the RK-1.

This section also shows the current version of BakPak running on the RK-1 and the most recent available version of BakPak.

**WR-1**

*Note: Please note that the WR-1 is a sub-agent.*

Sub-agents do not behave like management agents. A sub-agent cannot scan the network to find other devices and monitor them; it can only monitor itself and perform specific actions on itself.

**To register your Management Agent on an WR-1:**

1. Using a laptop or a desktop computer, go to mybakpak.com and login.
2. After logging in, complete the **Register Management Agent** form. The form automatically populates WR-1 information; simply enter an Agent Name and click **Register Agent**.
3. You have successfully added the WR-1 to your BakPak account.

Accessing BakPak

1. To access your BakPak account, enter mybakpak.com into your web browser and log in with your credentials. After you have logged in, you will be redirected to the Dashboard.

2. To log out of BakPak, click **Logout** at the upper-right corner of the screen.
Using the Wizard to set up accounts

The BakPak Cloud Management System offers two versions of the set up wizard: one for administrators and one for technicians.

With the wizard,
- Administrators can set up sites, create users, and grant permissions.
- Technicians can create sites, assign technicians, set alerts, and categorize devices.

Wizard for administrators

With the set up wizard, an administrator can set up sites, create users, and grant permissions.

Note: If you have registered a Management Agent to your account but have not created a site/site for that Management Agent, you will be prompted to run the Wizard to set it up.

Step 1: Creating Sites
In the first part of the wizard, create a site using either a Management Agent or a Sub·agent.

Note: When adding a site to a full management agent (such as the NK-1/RK-1) or a sub·agent (direct to cloud, such as WR-1), set up options differ. See instructions below.
Create a site with a Management Agent
To create a site using a Management Agent:

1. Click **Add Site** and complete the following form:

   ![Add Management Agent Site Form]

   a. Scroll to select the **Management Agent**.
   b. Give the site a **Name** and then add all the necessary VLAN information
      
      Tip: For more information about VLANs and how to add them, see Sites.
      
      Tip: If adding a sub-agent, the information required will be different. (See below).

2. Click **OK**.

   A scan will run to detect all devices on the network. After the scan is complete, you will be directed to the second part of the wizard (where you can create technicians/users).
Create a site with a sub-agent

To create a site using a sub-agent:

1. Click **Add Site**.
2. On the upper right, click the plus sign and complete the following form:

   ![Add Management Agent Site](image)

3. From the **Management Agent** list, pick your Sub-Agent.
   (In this example, WR-1-Office is selected).
   Reminder: The information required to add a sub-agent differs from information required to add a regular management agent (NK-1 or RK-1).
4. Enter the required site information and click **OK**.
   a. **Site Name**. Think of the site as a group where you can add all your sub-agents. Use the customer’s name or another name.
   b. **Device Name**. List the name of the device.
   c. **Device Location**. List the location where device is stored (server room, living room, etc.).
   d. **Address**. List the physical location of the WR-1.
      Tip: Note that the **Address** field is not the address of the site. (Sub-Agent sites do not have addresses).

The sub-agent device is added to the site.
5. If you want to add more sub-agents to this site, click the plus sign.

**Step 2: Create Users**
In the second part of the wizard, add users to the site.

To create new users:

1. In the second section of the wizard, enter the name and contact information for each technician/user, and then click **Create**.

These accounts will be granted permissions to manage specific customers’ sites based on the **Permissions** set in the third part of the Wizard.

**Step 3: Setup Permissions**
In the third part of the wizard, add permissions to each user.

**Note:** A technician must be added to a group to apply permissions.

To set up permissions:

1. Since a technician must be added to a group to apply permissions, be sure to create a permission group.
   a. Click **Add New** to create a new group.
   b. Select the user(s) you want to add to the group.
c. Give the group a name, then click **Create**.
After you have created your users and groups, you will be able to assign advanced permissions, which define what users can and cannot do. For information on more advanced permissions, see **Users**.

2. Click **Finish**. You are directed to the ** Sites** page.
Using the Technician Wizard

With the set-up wizard, technicians can create sites, assign technicians, set alerts, and categorize devices.

**Welcome, Tech**

With BakPak you can monitor networks, A/V and automation equipment, and unlimited 3rd party products while mitigating onsite visits with real-time visibility and remote assistance. This Setup Wizard will fast track you through creating sites, assigning technicians, setting alerts, and categorizing devices.

Click “Add Site” to add a new customer or job site. Once you have created the new profile BakPak can run a scan and detect all the devices on that site.

If a profile already exists for the site, you can click “Next” to skip this step.

Simply log in as a technician and complete the wizard.

**Step 1: Add Sites**
In the first part of the wizard, create a site using a “Management Agent” or a “Sub-agent.”

**Step 2: Device Groups**
In the second part of the wizard, create **Device Groups**. Devices can be grouped together so that you can apply settings to them all at once. Refer to “Group management” for more information about Device Groups and how to use them.

**Step 3: Alerts**
For more information on alerts and management, see “Alerts.”

**Step 4: Device Priorities**
For more information on setting up device priorities, see “Setting device priorities.”

**Step 5: Device Categories**
For more information on setting up device categories, see “Device categories.”

**Sub-agent features**

After adding a device into the sub-agent site, you will have access to the set of features supported by the device. (Currently, the only device that supports the sub-agent is the WR-1).
WR-1 features include:

1. Reading up time
2. Online/offline Alerts
3. Reading CPU and Memory usage
4. Speed Tests
   
   *Speed tests are run on demand. (Historical data is not available).*
5. Device Reboot
   
   *Use Device Reboot to reboot the WR-1.*
6. SSID Configuration
   
   *Use SSID Configuration to change your SSID name and security profile.*
   
   Please note that you cannot create security profiles from BakPak. The security profiles must be created on the WR-1 first before they will display in BakPak.

   Once security profiles are created on the WR-1, you will be able to change the password on these security profiles. You can also pick which security profile to apply to each SSID.
7. Zone Configuration (LAN IP Address, DHCP...)
   
   Use Zone Configuration to read the WAN settings.

   You can also update your LAN settings, enable/disable DHCP, edit DHCP start and end IP addresses, and modify the lease time.
8. FW Update
   
   Use FW Update to update the WR-1 FW from the cloud.
9. Notes
   
   Use **Notes** to add notes as needed.
10. Events

    **Events** records every action done by each user of the WR-1.
Using two-way authentication

The Authy app adds an extra layer of security, and allows users to require two-step authentication when signing into their BakPak account.

With two-step authentication, dealers or technicians will know when someone is trying to use their BakPak log in, and they can then deny or approve the request.

Tip: To use this feature, at least one Premier Management Agent will need to be set up on BakPak.

To begin, install the Authy app on your smartphone.

To install the Authy app:

1. Go to Google Play or iTunes Store and download the Authy app.

2. After it is installed, launch the app.
   You will be prompted to enter your email and phone number, as shown.

3. Select SMS to receive a text message when someone is signing into your account.
4. Click the blue **Add** button to add an account.

5. Enter a password and then confirm the password.

6. Navigate to **Dashboard > Users > Authy Management** and complete the following form:

![Authy Management Form](image)

7. Type the email address and the phone number used in the previous steps.

8. From the *AUTHENTICATION TYPE* drop-down menu, select **Send Token via Authy App** or **Onetouch**.
   - *Authy App*. The Authy App Token will generate a code that will be used on login.
   - *Onetouch*. When someone is trying to log in to your account, Onetouch will send a push notification to your phone and ask you to approve or deny the request.

9. When you are ready, click **Register**.
   Tip: If you see the following screen on your smartphone, tap your phone’s **Back** button.
Logging in to BakPak using Authy Soft Token

1. Once the Authy app is activated, go to mybakpak.com and log in.

2. On your smartphone, open the Authy app, and then select the BakPak Site account. The screen displays a code with a timer. The code (your login token) expires in 20 seconds.
3. Type the code from your smartphone's Authy app in the *Authy Code* field on your computer, then click **Submit**.

Logging in to BakPak using Onetouch

1. Once Onetouch is activated, go to *mybakpak.com* and log in.

2. Your smartphone will receive a notification (visible in the notification area) that Authy is asking for access.
   a. To resend the Onetouch request, click **Resend Onetouch** on your computer.
   b. You can also decide to use the Authy SoftToken instead by clicking **Use SoftToken** on your computer.
3. Tap **Accept** to approve the login (or **Deny** to cancel it). If you tapped **Accept**, you’ll be logged in. You will also be asked if you would like to save the device that you are logging into.

4. If you don’t want to have to log in from the device again, click **Save**.

---

**Editing user information**

To edit your user information:

1. Log in to mybakpak.com.
2. Click the cog icon located at the top left of the Dashboard.

3. A panel with your user information displays on the left.
4. Choose a display name. 
   *Your display name displays at the upper left of the BakPak screen.*

5. Change or update your password if necessary.

6. Optional: Select the plug type, based on the country you live in.
   *This will change the style of the PDU outlets shown in “Device view” (discussed in a later section).*

For example, if you live in the U.S., select **America**. The plugs on your PDU devices will display as shown below.

If you live in the U.K. and select **UK**, the plugs will display as shown below.
7. Optional: Choose between **Celsius** (C) and **Fahrenheit** (F).

8. Click **Update** after making the necessary changes.

**Sites**

To add a registered Management Agent:

1. Log in to mybakpak.com and go to **Sites > View/Create**.

2. On the upper right, click the plus sign.

3. In the new screen, select your Management Agent from the drop-down menu.

   *Please note: Management Agents must be registered before they appear in the drop-down menu. (See "Registering your Management Agent" for help).*
4. **Site Name** and **Address**:
   Enter a **Site Name** and street **Address**. *The street address is required to display your site’s weather information.*

5. **Pakedge Zone Information**:
   If you are using a Pakedge Fortinet router or a Pakedge RE-2 and RK-1 router, click **Fetch VLAN Info** to detect VLAN information automatically.
   a. If you are using a Fortinet Router and you have changed the default username/password on the router, deselect the option **Use Defaults** to enter the new credentials.
   b. You can enter the VLAN information manually if you choose to by clicking the **Manual** tab.

6. **VLAN Information**:
   To add VLAN information manually:
   a. Enter the first IP address of your network.
Since the example above uses the **192.168.51.0** network, its first IP address would be **192.168.51.1**.

b. **VLAN ID:**
   If you are using multiple VLANs, click the [+] icon to add another VLAN.

   ![VLAN Information](Image)

   **Tip:** Adding multiple VLANs will allow the Management Agent to scan devices on VLANs other than the default.

   **Tip:** It is recommended that the Management Agent remain on VLAN 1.

   **Note:** For BakPak to successfully scan across VLANs, it must be connected to a hybrid switch port or the router directly (recommended).

c. When you are finished, click **OK**.

   ![Home](Image)

   The new site should display on the **Sites** page.

### Removing a site

**To remove a site from your BakPak account:**

1. Log in to mybakpak.com and go to **Sites > View/Create**.
   a. To delete a single site: From the list of sites, hover to the left of the site you wish to remove, and click the delete icon.

   ![Home](Image)

   b. To delete multiple sites: Hover to over the site you wish to remove and select the check box. After selecting all the sites you wish to remove, click the **Delete** icon (upper right).
2. Click **OK** to remove the site.

![Confirmation dialog]

**Note:** This will not delete the Management Agent from your site, but it will remove all devices from your Management Agent.

## Scan for devices and device priority

The Management Agent can scan your network to find devices. After the devices are discovered, you can prioritize them by level of importance.

**To scan your network and build a network map:**

1. Log into mybakpak.com and go to **Sites > View/Create**.
2. Click on a site to edit it.
3. Click the **icon**, located near the top of the page, to begin device discovery.

![Device discovery]

The Management Agent scans the network for your devices.  
*This may take a few moments.*
After scanning is complete, a list of discovered devices displays.

4. Click Select All at the upper-right corner to select all devices. (You can also select devices manually by clicking on them.) Click the icon to add them to your site.

BakPak will ask if you would like to set up priorities for your devices. Priorities allow you to designate importance for devices on your network.

5. Click Setup Now. For help setting priorities, refer to “Setting device priorities.”

Note: If you would like to set up priorities later, click Skip.

6. To see if the Pakedge devices on the network are ready for management, click Check. BakPak will run a series of tests to ensure all the pakedge devices are accessible and ready for management.
Setting device priorities

To set device monitoring priorities:

1. Click **Setup now** (at the end of the procedure above).
   - OR –

   From the **Dashboard**, go to **Devices > Priorities**.

   A list of device priorities displays.
• By default, any Pakedge devices will be classified as *High Priority* and all other devices are classified as *Unmonitored Devices*.

• Devices classified as *Internet of Things & Wireless Devices* will be monitored but will be reported offline only after an extended amount of time. This will keep wireless devices from spamming alerts.

• Devices classified as *Unmonitored Devices* will not have alerts sent out when they go offline. Any non-Pakedge devices will be classified as *Unmonitored Devices* by default. **Note:** Devices will still show as offline or online in the site.

2. Hover over a priority icon until it changes to a gear icon, then click the gear icon 🔄 to display a list of the network devices with that priority.

3. Click a device to select it and move it over to the *Devices Selected* group. Your settings are automatically saved.
Setting device categories

To set device categories:

1. Log into mybakpak.com and go to Dashboard > Devices > Categories. Using the tabs, choose from two types of categories: Control4 Devices and Other Devices.

   ![Control4 Device Management](image)

   Tip: The Other Devices category is used for devices that are not Control4 devices.

2. Under the Control4 Devices category, you’ll see a group called Control4 Device Bin. Hover over it, then click the gear icon to display a list of devices available. (You can use this option to categorize devices that did not get auto-categorized after the scan).

   ![Control4 Device Bin](image)

3. Select the device, pick its category, and click Tag. A new category appears.

4. To view the device’s association with Control4, navigate back to Dashboard > Sites > View, select your site, scroll to the Automation Controllers category, and click the ZigBee icon. The device you selected earlier now appears in this list.
Adding devices manually

If Auto Device Discovery does not add all networked devices to the network, you can add the missing devices manually.

To manually add network devices:

1. In the Device View page, click the Add Device button. In the new screen, enter details about the new device.

2. Select whether the device is Pakedge, Control4, or Other, then select the model (if applicable).

3. For Control4 devices, select the device’s Model Type and Model.
4. Configure any other applicable settings (such as **Device AP Address** and **Web Port**) and click **OK** to add it to the network.

**Viewing all discovered and added devices**

**To view a categorized list of all discovered and added devices:**

1. Log into mybakpak.com and go to **Dashboard > Sites > View/Create**. Select a site in the **Sites** page to display a list of known network devices.

2. Scroll to view the entire list, and click the category title bar or the ⌛ symbol to collapse the category.
Triplex

Triplex is used to view connection issues and IP conflicts.

To use Triplex:

1. If there are any problems with a site, a widget called Triplex appears as shown below.

2. Click Triplex > Connection Problems. If there were any issues or IP conflicts, they will be listed here.

Creating a network map

After discovering all devices, you can create a network map to illustrate the physical topology of your network. Use the following steps to create your network map.

To create a network map:

1. Log into mybakpak.com and go to Dashboard > Sites > View/Create.
2. Navigate to your site, switch to the Network Map View, and then click the icon to have BakPak attempt to automap your network.

After the auto-map is complete, your network map will display:
3. If BakPak was unable to fully complete your network map, complete it manually.

In the following example, an SX-24P is connected to an RE-1. To illustrate that on the network map, drag the SX-24P over into the RE-1.

When the two icons are close to each other, a red line will appear connecting them to each other.
4. When prompted, enter the port number used on the SX-24P to connect to the RE-1 (and vice versa), then click **Save Port Information** to continue.

The switch is now connected to the RE-1. Do the same task on the S24P8 switch in this example, which is also connected to the RE-1.

5. Drag the switch over to the RE-1.
6. Enter the required port information, then click **Save Port Information**.

The network map is complete.
Note: A green ring around a device indicates that the device is online. A red ring indicates the device is offline, and a yellow ring indicates that one or more devices connected to it are offline.

7. You can download the network map in a PDF or Excel format and save it for your records. To do so, click the PDF or CSV icons under the *Network Map* section.

Scanning across VLANs (Pakedge Zones)

The Management Agent can scan across VLANs to discover devices on the network.

**To allow scanning across VLANs:**

1. Log in to [mybakpak.com](http://mybakpak.com) and go to Dashboard > Sites > View/Create.
2. Hover over your site and click the gear icon.
3. Enter the VLAN information for your network (or have the Management Agent auto detect the VLAN information).

In this example, VLAN information was entered manually. Since **192.168.51.1** is the first IP address of VLAN 1, we enter 1 as the VLAN ID.

**Note:** If your network has a different IP scheme than the Pakedge default, you will need to enter the appropriate network information. For example, if your VLAN 1 IP scheme is 10.0.0.X, you would enter **10.0.0.1** as the IP address.

4. Click the **+** icon to add another VLAN.

(VLAN2 and VLAN3 have been added in this example).

5. Repeat Step 4 to continue adding VLANs onto the Management Agent.
6. Click OK to finalize the settings.
   Now the Management Agent can find devices across VLANs.

7. To scan for devices, follow the steps outlined in “Creating a network map.”

Device information
The Sites page displays key information on devices you have added.

To display device information:
1. Log in to mybakpak.com and go to Dashboard > Sites > View/Create.
2. Open a site and then click to expand a device.
   As an example, the RE-1 is shown below. Uptime displays near the top.
3. If desired, add a note on the lower right.

Tip: Notes display in the device view.

4. If supported, update a device's firmware via BakPak. For example, with the Pakedge RE-1 router, click **Firmware** to see available updates. Then click **Update** to update the firmware.

For a managed switch, BakPak displays information about the VLAN port configuration (shown below).
Configuring VLANs on SX Series switches

VLANS can be configured using our SX Series switches.

In this section, learn to add new VLANs to switches and configure switch ports to be Hybrid ports or Access ports. This can be done from BakPak (without going to the UI of the switch).

To configure a VLAN on an SX Series switch:

1. Click the switch and wait for the ports’ statuses to appear.
2. Then click Add VLAN.

A pop-up displays the VLANs that are already on the switch and provides a place to enter a VLAN ID.

Enter the ID and click Add.
3. To edit VLAN information on a switch port, hover over the port and click **Edit VLAN**.

A pop-up gives the option to make the port a Hybrid port or an Access port. For a Hybrid port, select **Hybrid** and enter the Untagged and Tagged VLAN information. For an Access port, select **Access** and enter the **VLAN ID** this port will belong to.
Control4 and BakPak

When running a device discovery scan, BakPak will identify your Control4 automation controllers and all ZigBee, Z-Wave, and IP devices controlled by it.

**Note:** After the scan is complete, BakPak will try to auto-categorize most of your Control4 devices. The process will take about 3-5 minutes after the scan, and then the information will update. To view the updated information, click to expand the ZigBee widget.

Below, a list of categorized displays. (You can do the same with the IP widget).

If you have made any project updates in Composer (such as name changes), you can always click **Update Project Info** to add this information to BakPak.
If you have added a driver for a PDU (such as Panamax or a Pakedge PowerPak) in Composer, the PDU will show under the IP widget as shown in the image below (P8 Drive).

To enable control for ports of the Control4 controller under the IP widget, hover over the device and click the cog wheel to edit it.

Update the device information by completing the **Device is** field, selecting the **Model**, and entering the **Username/Password** for the device. When you are done, click **OK**.

The page will refresh, and you will be able to control the ports for the PowerPak from the Control4 IP widget.
Device Control

Use **Device Control** to access a device monitored by BakPak (without VPN or port forwarding). Services include HTTP, HTTPS, Telnet, SSH, RDP, and much more.

In the following example, we will open a tunnel session to an S24P8 switch.

1. Log in to [mybakpak.com](http://mybakpak.com) and click **Sites > View/Create**.
2. Open a site and then click to expand a device.
3. Select **Device Control**.

Tip: Once a scan is complete, BakPak automatically checks services and ports that are open on a device and creates connections for them.
4. If you would like to add a new service on a specific port, click **Add New Connection**.

   ![Image of the BakPak Cloud Management System](image)

   For example,
   
   a. Select **HTTP** as the service, **TCP** as the protocol, and 80 as the port.

      Tip: The number in the **Choose Timer** field indicates how long the tunnel will be open (in minutes).

      i. If you click **Save**, the connection created will be saved for later use.

      ii. If you click **Save and Connect**, the connection will be saved and generate a tunnel for immediate use.
5. Once the tunnel is open, a log in link displays.

Click the link and log in to the switch.

Example: RDP

If you need to access a Windows computer remotely through remote desktop protocol (RDP), you can use **Device Control** to remotely access that computer without needing to perform any additional configurations on the router.

To access a Windows computer through a remote desktop connection:

1. Log in to mybakpak.com.
2. Click **Dashboard > Sites > View/Create**, and open a site.
3. Scroll to the Windows computer, and click to expand it.
4. Select **Device Control > Add New Connection**.
4. In the dialog, select RDP as the **Service**. (The **Protocol** and **Port** fields will auto-populate, because BakPak is familiar with RDP). Click **Save** or **Save and Connect**.

5. Once the tunnel is open, a link displays. Copy this link into the Remote Desktop application.

6. After pasting this link into the Remote Desktop application, click **Connect**.
7. The Windows login screen displays.

8. In some applications, the port information and IP address must be entered in separate fields. This includes applications that allow connection to devices via Telnet or SSH (such as PuTTY, shown below).
For help using BakPak’s **Device Control** feature with Telnet/SSH, see below.

**Example: Telnet**

To use PuTTY to telnet into a Pakedge S24P8 switch on the network:

1. Log in to mybakpak.com and go to **Dashboard > Sites > View/Create**.
2. Open a site and then click to expand a device.
3. Select **Device Control**.
4. Select **Telnet** as the service, then click **Submit**.
5. After the tunnel is open, a link displays as shown in the image below. Tip: The number after the colon is the port number that was opened for the tunnel. (In this example, the port number is 32421).

6. Copy the link

7. Open Putty, and in the *Host Name (or IP address)* field, paste the link.
8. Step 6 contains the port number opened for this tunnel. In this example, it is port 23488, so we enter that number in PuTTY and click **Open**.
You now have Telnet access to the S24P8 switch.

Device Portal

With Device Portal, log in to the UI of your devices without port forwarding or VPN access.

To log in to a device’s GUI:

1. Log in to mybakpak.com and go to Dashboard > Sites > View/Create.
2. Click on a device that has a web GUI, then click to expand the switch.

The log in page for the device will open in a separate window.
Port monitoring

From the Monitoring tab, add services to monitor devices.

For example, some devices do not have IP addresses or cannot be monitored using IP, but they do respond on specific ports. In this case, you can create a service to monitor a specific port (or ports) on a device.

To monitor specific ports on a device:

1. Log in to mybakpak.com and go to Dashboard > Sites > View/Create.
2. Open a site. Find the device you want to monitor and click to expand it.
4. Pick a service from the list and click Add. The new service will be added as shown below.

5. In this example, an alert is set for port 22. If the service does not respond on port 22, an email alert will be sent to the user on the account.

6. Optionally, mark a port as Critical. If Critical is checked, it indicates that the port being monitored (in the above case 22), will affect the online/offline status of the device. If Critical is checked and the port does not respond on that device, the device will be marked as offline.
DDNS

If you have created any DDNS entries using Pakedge routers, you will see them listed on the DDNS page.

To access the DDNS page, log in to mybakpak.com and go to Dashboard > Sites > DDNS.

Here, you can also release a DDNS entry to use it on another router by clicking the trash can when you hover over an entry.

Management Agents

From Management Agent, view all Management Agents registered under your account.

To update a Management Agent:

1. Log in to mybakpak.com and go to Dashboard > Sites > Management Agents.

2. From the list, click Firmware to see if a firmware update is available for your Management Agent.

If the firmware is up to date, a green ring appears under firmware (as shown).

3. If there is a firmware update, you will be asked if you would like to update the firmware. (The update should take about 5-10 minutes).

4. To manually upgrade the firmware on your Management Agent, download the latest firmware from the Dealer Portal on the Pakedge website.
   **Note:** If the Management Agent does not upgrade automatically, a manual upgrade may be necessary.

5. After downloading the firmware to your computer, log in to the Management Agent by typing its IP address into your web browser.
6. After logging in, click **Firmware Update** and go to the firmware file.

Site recovery under a new Management Agent

If you have a site or a site under an old management agent and you would like to use it on a new management agent, register the new Management Agent. (To register the Management Agent, see Registering your Management Agent).

To assign a new Management Agent:

1. Log into mybakpak.com and go to **Sites > Management Agents > Recover Site**.

2. Select the old management agent from the **Old Management Agent** list, then select the Management Agent you are replacing it with in the **New Management Agent** list.
3. Click **Recover**. Your site settings will be transferred to the new Management Agent. (There is no need to set up the site again).

# Devices

## Group Management

Group Management allows you to group devices together and apply settings to them in other sections of BakPak.

**To create a group:**

1. Log into mybakpak.com and go to **Dashboard > Devices > Groups > View/Create**.
2. Click the **+** icon to create a new group.
3. Click to select the devices you would like to add to the group.
4. Scroll down and enter a **Group Name**.
5. Click to select which sections that you would like to add this group to.
6. Click **Create**.

The new group displays.
Firmware Management

The *Firmware Management* page allows you to apply firmware to any of the devices in a management group.

To apply a firmware update to a device group:

1. Navigate to **Devices > Groups > Firmware Management** (make sure that you have created a group that participates in Firmware Management following the steps above).
2. Click the management group that includes the device you would like to update.

The devices in the group display, along with any available firmware updates. (In this example, a firmware update is available for a RE-1 router).

3. To apply the firmware update, click on the **RE-1** and then click **Apply to All**.

4. Click **OK**. The firmware on the RE-1 is up to date.
Configuration Management

Under *Configuration Management*, back up configuration files from supported devices so that they can be restored as needed.

In the following example, we will back up files from an RE-1 router and a WK-1 access point.

**To back up configuration files from a supported device:**

1. Log in to mybakpak.com and go to Dashboard > Devices > Groups > Configuration Management.
2. Click the management group previously created.
3. Select both the RE-1 and WK-1 and click Save All.
4. Click OK in the pop-up menu.

BakPak will create backup configuration files for the selected devices.

5. To apply a configuration to a device, click Selected.
   (In this example, RE-1 is selected).
6. Click OK in the pop-up window.

The configuration file will be pushed to the router.

Power Control

With *Power Control*, power cycle individual ports on a Pakedge managed PoE switch or PowerPak (PDU), or group ports together to power cycle multiple ports at once.

**To power cycle ports:**

1. Log in to mybakpak.com and go to Dashboard > Devices > Groups > Power Control.
2. Click the management group with the device you wish to manage. (In this example, the previously created group is edited).
3. Select the SX-24P switch.
   A virtual switch appears, and a blue lightning bolt indicates an active PoE port.

4. **Hover** over a PoE active port to **Turn Off**, **Power Cycle**, or **Rename** the port.
5. Click on the port for two different options: Create New Port Group or Add to Port Group. Click Create New Port Group.

6. Give the port group a name and click OK. The port group will be used to identify a certain group of ports on the switch.

7. Click Port Groups. You will see your port group listed.
8. Hover over the group and click the plus icon.

Here, configure a schedule for ports to be either power cycled or powered on and off at certain times.

9. Click **Turn Off / On**.

10. Choose between a **Daily** or **Consecutive** schedule.
    A daily schedule will occur every day.
    The example shows a schedule that is set to turn off at 6:05 a.m. and then back on at 6:10 a.m. every weekday.
11. To create a schedule for power cycling a group, click **Power Cycle**. Complete the form and click **Create**.

   *This example shows a schedule that is set to power cycle devices at 6:00 am on every weekday.*
12. After the schedule is created, you will be redirected to the Schedule management page. Click on your group to view its schedules.

Self-Healing

Under Self-Healing, set ports to power cycle when connectivity issues occur. Self-Healing also allows you to auto-ping a device. If pings fail, the port on the switch automatically reboots.

To set up Self-Healing:

1. Log into mybakpak.com and go to Dashboard > Devices > Groups > Self Healing.
2. Click to expand an item and then select a device.
3. Then hover over the port you would like to configure.
   In this example, we’ll set up an auto-ping for an IP camera connected to port number 7.
4. Enter the IP address of the camera under *Ping IP Address.*
   The *Wait Time* field shows how long BakPak will wait (in minutes) before power cycling that device after it has stopped responding.

   **Reboot Limit** and **Time Period** go together. Set the maximum number of reboots allowed in a given time period (in hours).

**Priorities**

From *Device Priorities* ([Dashboard > Devices > Priorities]), modify the priority levels for your devices. For additional information, see the section *Scan for devices and device priority.*

**Categories**

See *Setting device categories.* ([Dashboard > Devices > Categories]).

**Users**

Under **Users,**

- Create accounts for your technicians and assign permissions to them.
- Set up login security using two-way authentication.

**View/Create**

Under **View/Create,** create technician accounts.

**To create technician accounts:**

1. Log in to mybakpak.com and go to **Dashboard > Users > View/Create Users.**
2. Click the icon.
3. Fill out the form (required fields are marked in red). Then click **Create**.

4. After the technician is created, navigate to **Users > Groups & Permissions**. In order to apply permissions to a technician, they must first be added to a group.

5. Under **Groups and Permissions**, click **+** to create a new group.

6. Select the user you want to add to the group. Give the group a name and click **Create**.
Assigning permissions

After creating users and groups, you will be able to assign them permissions. Permissions define what users can and cannot do.

Below, learn about the five available permissions.

To assign permissions:

1. Open the group.
   a. Log into mybakpak.com and go to Dashboard > User > Groups and Permissions.
   b. Next to the group you would like to edit, click Advanced Permissions.

2. Select your desired settings and click Apply when you are finished.

There are four types of permissions.

3. Global permissions are the general permissions applied to all sites.

4. Management Agent permissions apply to Management Agents and take precedence over global permissions.
   a. Click to select the Management Agent(s).
   b. Expand and select to choose settings.
      i. Checking Global Permission will set the permissions to the default global setting.
   c. Click Apply to save your work.
5. **Device** permissions apply only to the devices from the Management Agents you choose.
   a. Select the **Management Agent** and device that you want to apply permissions to.
   b. Expand and select to choose settings.
      i. If you want the devices to use the default Management Agent settings, select **Use Management Agent Permission**.
   c. Click **Apply** to save your work.

   **Note:** You need to apply the permission settings one at a time for each device.
6. Port permissions override all other permissions and allow you to choose which ports users have access to.
   a. Select the **Management Agent** and the device that you want to apply the port permissions to.
   b. Expand and then select the port and permission settings.
      i. If you want the devices to use the default device settings, select **Use Device Permission**.
   c. Click **Apply** to save your work.

---

**Authy Management**

For help with Authy management, see [Using two-way authentication](#).
To set up alerts:

1. Log in to mybakpak.com and navigate to **Dashboard > Alerts > Manage**.
2. Hover over the **Default** alert and click the cog wheel.

3. Select which devices should be included in the default alert. (By default, all Pakedge devices are included).
4. Scroll down and click **Save** to finalize your settings.

5. **Optional:** If you would like to receive notifications via SMS, scroll down and enter your phone number. Add a descriptive **Label** for the alert.
For notifications by email, enter an email address.
(The BakPak toggle indicates that you will receive a push notification from BakPak on your mobile device).
6. To create different alert settings for different devices, create a custom alert. To create a new alert, go to **Dashboard > Alerts > Alert Management**, and click the **+** icon.

7. Fill out the necessary information and click **Create**. Be sure to select the devices you want to include in this alert.

**Note**: When entering a phone number for international texts, use the following format: `011 + country code + area code + number`.

**Note**: An admin can create an alert and assign only one technician to that alert. Two technicians cannot be part of the same alert.

**Note**: A default Management Agent alert is sent when the Management Agent loses communication with the cloud. For example, if a site loses power, you will receive only a single notification from BakPak saying your Management Agent is offline.
On-demand reports

To generate on-demand reports:

1. Log in to mybakpak.com and go to Dashboard > Actions > Reports > On-Demand Reports.
2. Click the management group created previously.

(In this example, the Pakedge S24P8 switch is selected).

3. The Quick View tab displays CPU and memory usage.

4. The Device Events tab displays important events that have occurred.

The image below shows the timestamps of a Pakedge WK-1 access point that went offline and came back on.

5. The Visualizations tab will graph various aspects of devices such as CPU, Memory, and Online/Offline history (shown below).

Tip: The graph can be downloaded as a PDF.
BakPak Cloud Management System

6. **User Reports** record every user’s action on any device. Click **User Reports**, and then choose a user from the list. Select a start date/end date and click **Refresh** to display the user’s activities.

**Emailed Reports**

Under **Emailed Reports**, you can create reports to be sent to any email address (including email addresses for technicians and end users). You can create daily, weekly, or monthly reports.

There are two types of reports: **Site** and **Overview**. The **Site** report includes information about a specific site, and the **Overview** report includes information about all the sites under your account.
BakPak Cloud Management System

To generate emailed reports:
1. Log in to mybakpak.com and go to Dashboard > Actions > Reports > Emailed Reports.
2. Complete the form and select which users should receive the report.
3. Click Save to schedule the report email.

Speed Test

Under Speed Test, view speed test results for all Management Agents (including historical data for up to one month).

Note: Speed tests can also be run on-demand. Click the Play icon to run a speed test.

To change speed test frequency:
1. Log into mybakpak.com and go to Dashboard > Actions > Speed Tests.
2. Click the cog wheel next to the site name, make any edits, and Save your changes.
3. On this page, you may want to set thresholds for Download, Upload, Latency, and Jitter.
4. Next to the site name, click an option, enter a value, then click Set Threshold.
   (As needed, use Remove Threshold).
   Note: You will receive an alert if the value you entered is above or below the threshold.
Diagnostics

Under **Diagnostics**, check the status of BakPak services and test the alert system.

Go to **Dashboard > Actions > Diagnostics.**
Collaboration

Under **Collaboration**, generate a token for tech support personnel to temporarily access your BakPak account (without having to share your BakPak username/password).

1. Log in to mybakpak.com and go to **Dashboard > Actions > Collaboration**.
2. Click **Generate Access Token** to get a token that can be given to support.

Contact Us

The *Contact Us* page contains contact information for the various departments at Pakedge.

---

**Sales:**
Cell (650) 365-8702 or email sales@pakedge.com

**Support:**
Call (650) 365-8705 or email support@pakedge.com

**Marketing:**
Cell (714) 830-4593 or email marketing@pakedge.com

**Customer Service:**
Call (650) 365-8701 or email customerservice@pakedge.com
Limited Warranty

Congratulations on your purchase of a Pakedge Device & Software product! Pakedge designs and manufactures the finest home-networking products. With proper installation, setup, and care, you should enjoy many years of unparalleled performance. Please read this consumer protection plan carefully and safeguard it with your other important documents.

This is a LIMITED WARRANTY, as defined by the U.S. Consumer Product Warranty and Federal Trade Commission Improvement Act.

What Is Covered Under the Terms of This Warranty?

SERVICE LABOR: Pakedge will pay for service labor by an approved Pakedge service center when needed, as a result of a manufacturing defect. This is covered for a period of 3 years, starting on the effective date of delivery to the end user.

PARTS: Pakedge will provide new or rebuilt replacement parts for parts that fail due to defects in materials or workmanship. This is covered for a period of 3 years, starting on the effective date of delivery to the end user. Such replacement parts are then subsequently warranted for the remaining portion (if any) of the original warranty period.

What Is Not Covered Under the Terms of This Warranty?

This warranty only covers failure due to defects in materials and workmanship that occur during normal use and does not cover normal maintenance. This warranty does not cover any appearance item; any damage to living structures; failure resulting from accident (example: flood, electrical shorts, insulation); misuse, abuse, neglect, mishandling, misapplication, faulty or improper installation or setup adjustments; improper maintenance, alteration, improper use of any input signal and/or power, damage due to lightning or power line surges, spikes and brownouts; damage that occurs during shipping or transit; or damage that is attributed to Acts of God.

The foregoing limited warranty is the sole warranty of Pakedge and is applicable only to products sold as new by Authorized Dealers. The remedies provided herein are in lieu of a) any and all other remedies and warranties, whether expressed, implied or statutory, including but not limited to: any implied warranty of merchantability, fitness for a particular purpose or non-infringement, and b) any and all obligations and liabilities of Pakedge for damages including but not limited to incidental, consequential or special damages, or any financial loss, lost profits or expense, or loss of network connection arising out of or in connection with the purchase, use or performance of the Product, even if Pakedge has been advised of the possibility of such damages.

CAUTION: DAMAGE RESULTING DIRECTLY OR INDIRECTLY FROM IMPROPER INSTALLATION OR SETUP IS SPECIFICALLY EXCLUDED FROM COVERAGE UNDER THIS WARRANTY. IT IS IMPERATIVE THAT INSTALLATION AND SETUP WORK BE PERFORMED ONLY BY AN AUTHORIZED PAKEDGE DEALER TO PROTECT YOUR RIGHTS UNDER THIS WARRANTY. THIS WILL ALSO ENSURE THAT YOU ENJOY THE FINE PERFORMANCE YOUR PAKEDGE PRODUCT IS CAPABLE OF PROVIDING.
Rights, Limits, and Exclusions

Pakedge limits its obligation under any implied warranties under state laws to a period not to exceed the warranty period. There are no express warranties. Pakedge also excludes any obligation on its part for incidental or consequential damages related to the failure of this product to function properly. Some states do not allow limitations on how long an implied warranty lasts, and some states do not allow the exclusion or limitation of incidental or consequential damages. In this case, the above limitations or exclusions may not apply to you. This warranty gives you specific legal rights, and you may also have other rights that vary from state to state.

Effective Warranty Date

This warranty begins on the effective date of delivery to the end user. For your convenience, keep the original bill of sale as evidence of the purchase date from your authorized dealer.

Important: Warranty Registration

Please register your product at www.pakedge.com. It is imperative that Pakedge knows how to reach you promptly if we should discover a safety problem or product update for which you must be notified. In addition, you may be eligible for discounts on future upgrades as new networking standards come about.

To Obtain Service, Contact Your Pakedge Dealer

Repairs made under the terms of the Limited Warranty covering your Pakedge product will be performed by an Authorized Pakedge Service Center. These arrangements must be made through the selling Pakedge Dealer. If this is not possible, contact Pakedge directly for further instructions. Prior to returning a defective Product directly to Pakedge, you must obtain a Return Material Authorization number and shipping instructions. Return shipping costs will be the responsibility of the owner.