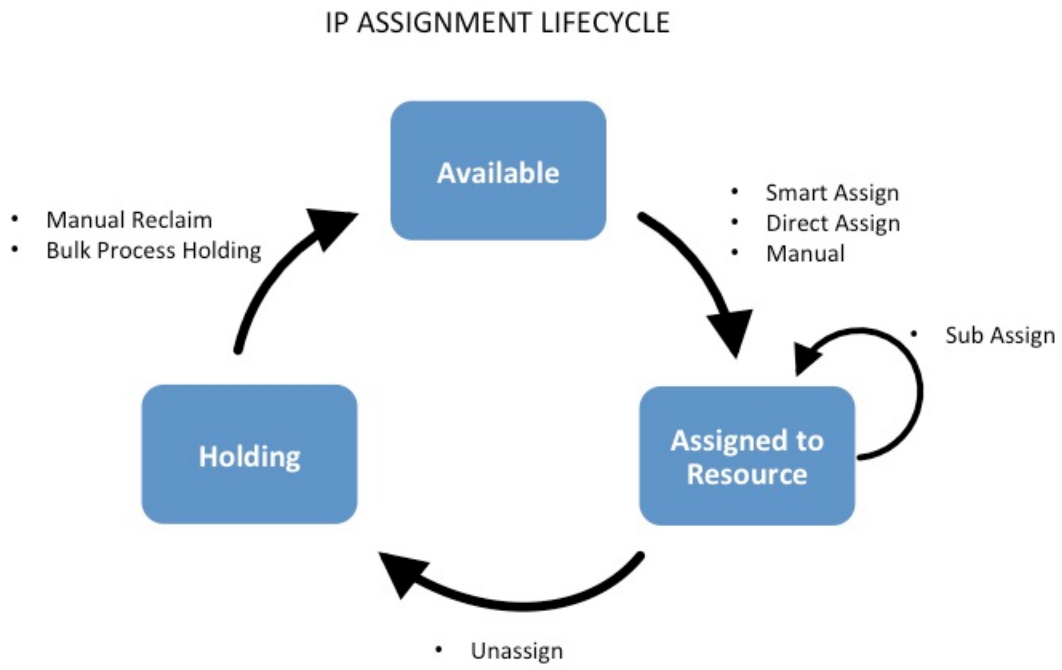
Workflow Concepts

Workflow Concepts

IP Assignment Lifecycle

In ProVision, the IP assignment lifecycle starts with an available block which is free to be assigned to any IPAM-enabled resource holder. There are multiple methods that may be used to assign a block to a resource holder: Smart Assign, Direct Assign, or Manual Assign (Smart Browse).

Once an IP block is assigned, blocks can be further subassigned via the same methods if desired. When an assigned block is un-assigned it proceeds into the Holding Tank: a special resource where blocks are held until either a set time has elapsed or until they are manually reclaimed to 'available' status.



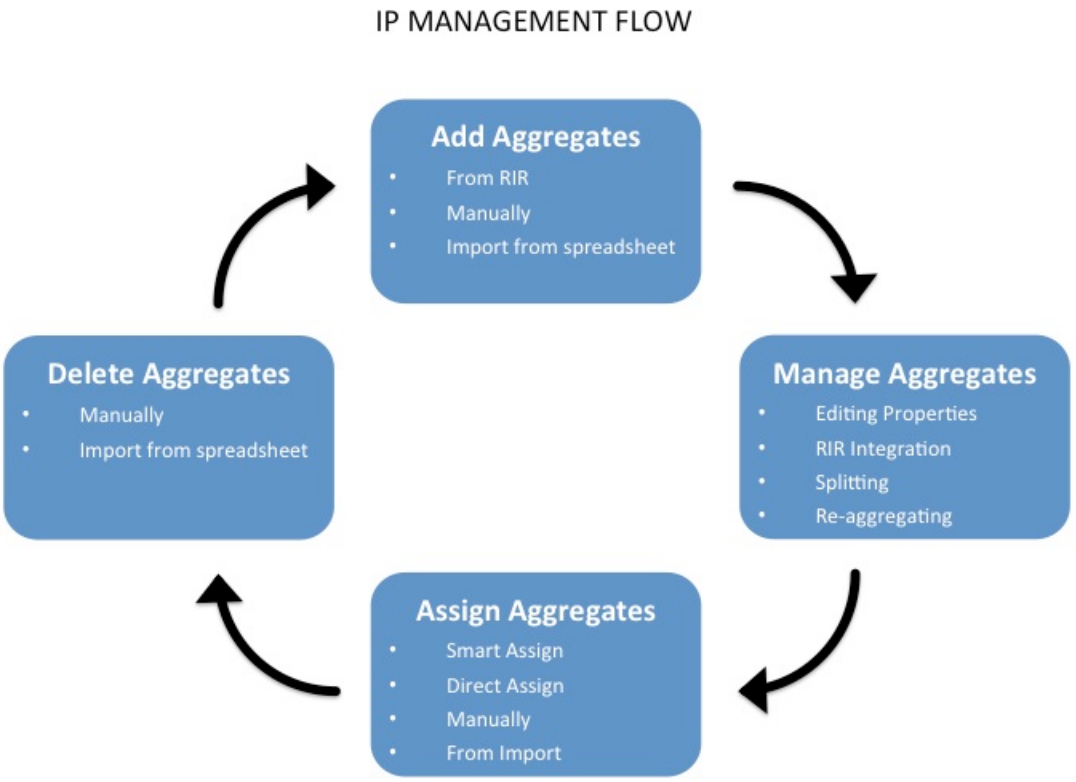
For more information on performing tasks in this IP Assignment Lifecycle, see the following documentation sections:

- Working with IP Blocks
- IPAM Administration

IP Management

IP Management is comprised of four basic functions: adding aggregates into ProVision, managing those aggregate blocks, assigning them to a resource, and deleting the aggregates.

ProVision provides multiple ways for you to achieve each step, depending on your needs. For example, if your organization currently uses spreadsheet data to track aggregates, ProVision provides tools that can import your existing spreadsheets for bulk updates, saving you time. Need to just quickly assign a single IP? Direct Assign will allow you to do so with just a few clicks.



For more information on performing tasks in this IP Management Flow, see the following documentation sections:

- Working with IP Blocks
- IPAM Administration
- Importing Your Data
- Import Aggregate Blocks

Peering

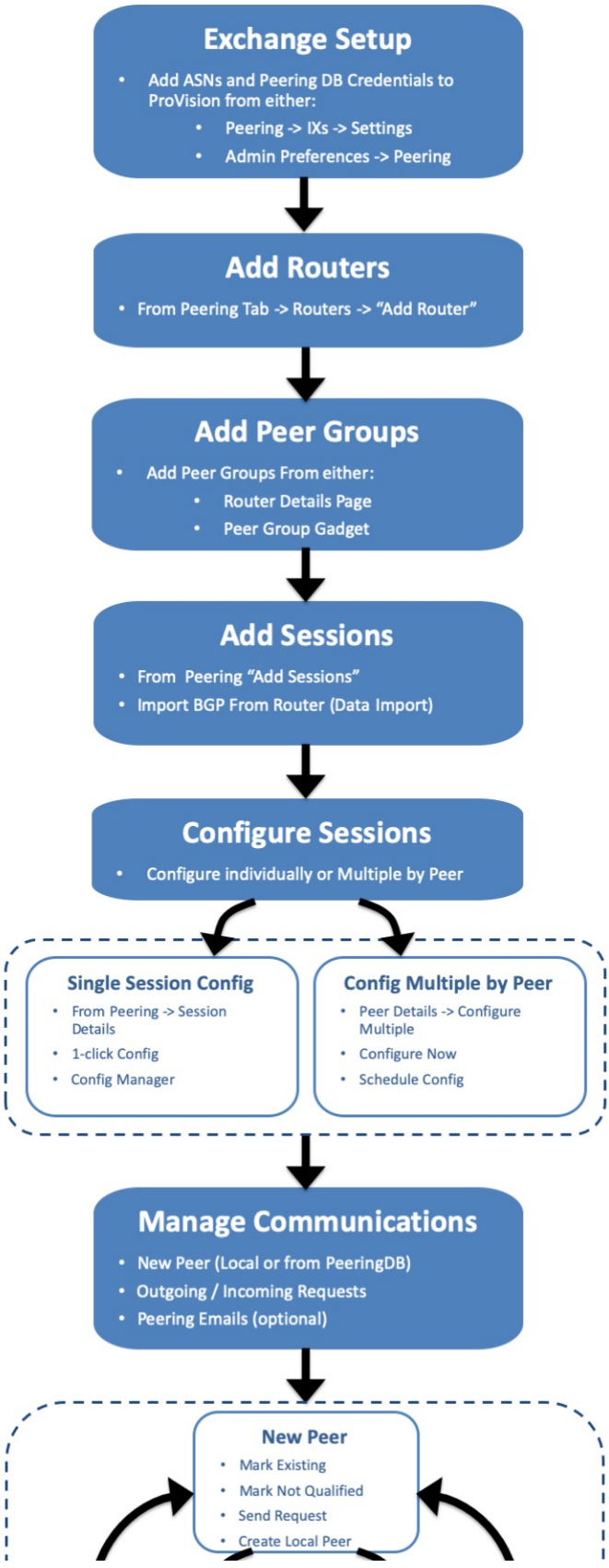
Initially, ASNs and Peering DB information will need to be entered into ProVision to enable Peering functionality. After that, Peering starts with designating Routers. Routers may be added from the "Add Router" button under the Peering Tab Routers sub-tab. Once a router has been created, Peer Groups may be added from the Router Details page or the Peer Group Gadget.

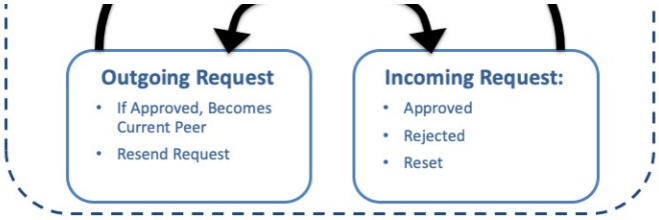
After the router(s) and Peer Groups have been created, Sessions need to be added. Sessions may be added manually through the "Add Session" dialog in the Peering tab, or Imported from a router (requires Admin permissions).

Once a session has been created, it can be configured and managed through the Sessions list and Session details page (using 1-click Config or Config Management), or multiple sessions may be configured for a specific Peer via the "Configure Multiple Sessions" option, which will provide options to either "Config Now" or "Schedule Config" for a later time.

Managing Peer Communications is done primarily from the Exchange Communications menu, sending requests and marking peers as existing / not qualified / approved, etc. If desired, a corporate Peering email account may be associated with ProVision under the Peering Emails subtab, allowing for peering requests to be viewed from ProVision and associated with Peers.

PEERING WORKFLOW





For more information on performing tasks under Peering, see the following documentation sections:

Peering:

- Peering
- Peering Exchanges
- Peering Routers
- Peering Sessions
- Import Peering Sessions

VLAN Manager

The VLAN Manager allows users to add domains and VLANs to their ProVision instance, and associate them with IP blocks. Customizable VLAN columns - including up to ten user-defined metadata columns - allow you to rename column headers, set the display order, select which columns are visible, and display your own information fields.

Permissions and VLAN

The Permissions structure in VLAN includes the following items of note:

The following VLAN tasks requires Admin-level permissions:

- Adding new Numbering Authority ranges for VLAN use
- Editing IPAM / VLAN Columns
- Adding, editing, and removing Domains
- Adding, editing, and removing VLANs

Non-Admin users may:

- View the VLAN Home Page and utilization data, however, only resources that the user has view permissions for will display under the "Resources" and "Recent Assignments

VLAN Workflow:

Create Domain(s)

The workflow starts with creating a domain in the IPAM Tab VLAN section of ProVision, by clicking the "Add Domain" button and entering domain information.

VLAN domains may be created as pre-set Numbering Authority ranges, or defined manually. Two default Numbering Authority VLAN ranges are provided, one for a Cisco Standard domain, and another for a Cisco Extended Domain. Admins may create new Numbering Authority ranges at any time to support other router types, range extents, or exclusions. Those ranges will then be available as options when adding a new domain from the VLAN area. If you select to create a new domain by defining a manual range, you may enter the range extents, any exclusions, and associate a specific router if desired.

Add / Edit VLANs

VLANs may be added to the domain at the time the domain is created (via the "Add VLANs" input area) or added to an existing domain later via the "Add VLANs" button. You can add one VLAN, multiple VLANs, a large range of VLANs, or a mixed selection at the same time.

Once a VLAN has been added to a domain, the VLAN may be edited to add a VLAN name or metadata information, and have IP blocks associated with it.

Add IP Blocks to VLANs

Once a VLAN has been added to a domain, IP blocks may be associated with ('assigned to') that VLAN. There are multiple methods to set the VLAN for a block:

- **Individual block edit** - Edit one or more blocks and set the Domain and VLAN fields to the desired values. Direct edit may be performed from IPAM Manage, VLAN Manage, and the IPAM Gadget, by selecting "Edit Block".
- **Direct Assign a block** - Open the "Assign Blocks" panel, expand "Direct Assign", and type in the CIDR to assign to the VLAN. Advanced options are available to distinguish between duplicate blocks. The "Assign Block" panel is available from the VLAN's Utilization Box, and/or the VLAN Manage header bar.
- **Smart Browse for blocks** - Open the "Assign Blocks" panel, expand "Browse Assign", and enter filter criteria to create a list of blocks meeting that criteria. Then, select one or blocks from the list to assign to the VLAN. The "Assign Block" panel is available from the VLAN's Utilization Box, and/or the VLAN Manage header bar.

After assigning a block to the VLAN by any method, that block will immediately display in VLAN Manage for that VLAN, in the VLAN's Quickview Panel, and the VLAN Utilization display panel will be updated to include the new block.

Manage Domains and VLANs

Managing VLANs and blocks under the VLANs may include standard IPAM tasks, such as editing blocks, splitting / merging blocks, or allocating/ assigning / unassigning the blocks to a resource. All of these functions, and more, may be performed from either VLAN Manage or IPAM Manage.

Other tasks, such as editing VLAN names, metadata, or adding/removing VLANs from a domain are performed from the VLAN Action Panels on the VLAN Home page, or from VLAN Manage.

Editing Domains - including renaming, adding metadata, and deleting - may be performed from VLAN Advanced.

DHCP

The DHCP Workflow begins with adding DHCP Servers into ProVision and creating an additional DHCP Groups as needed.

New DHCP servers may be added from the DHCP Tab - DHCP Servers subtab by clicking "Add Server". Type in the server information, select the service, and choose the resource to which the DHCP server belongs if applicable. This creates a hierarchical relationship, with the server as a child resource under the selected parent, and affects how permissions are handled for the server and pools. Then, enter any service-specific or advanced settings for the server. You may also choose which DHCP group to associate with the server if the group already exists, but you may also add that setting later.

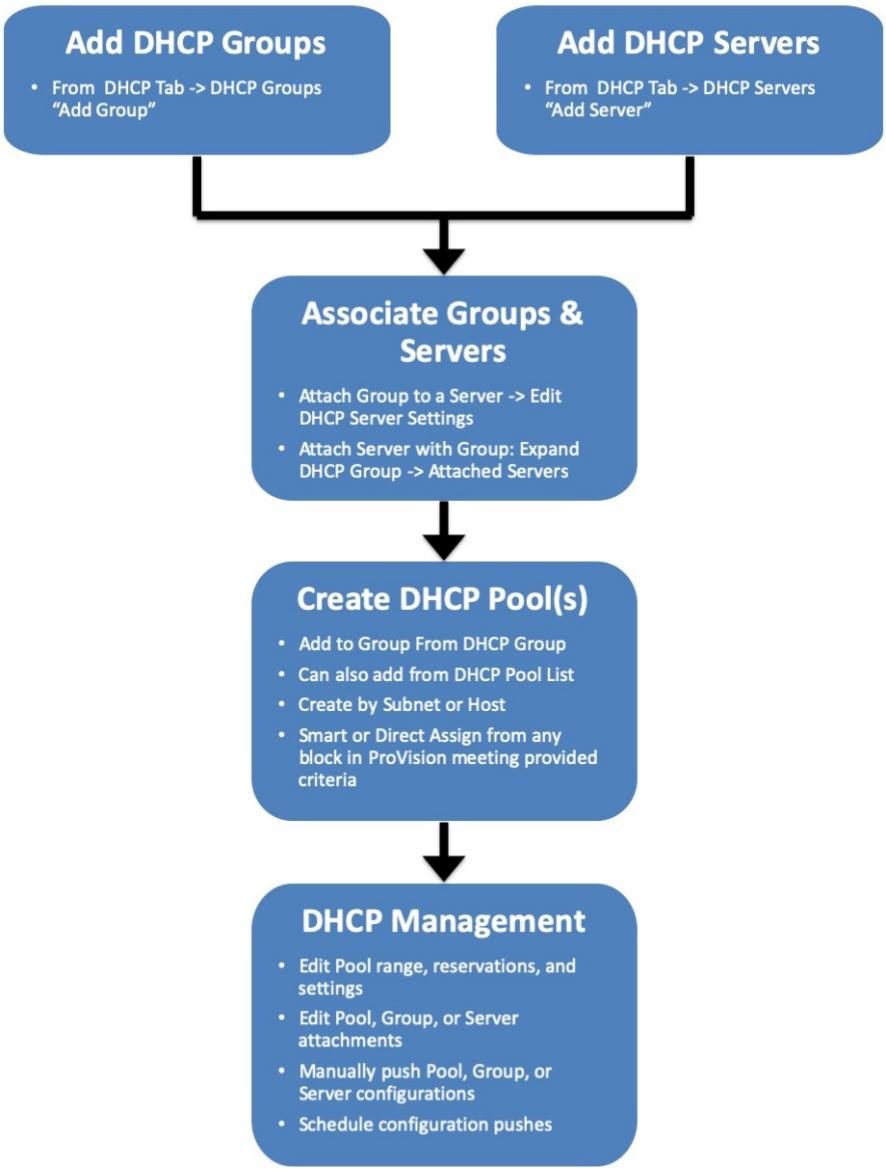
If desired, you may create additional DHCP Groups to organize certain pools and associated DHCP servers together to push concurrently, with the option of a common failover value. A common scenario is using separate DHCP Groups per server, or separate Groups for IPv4 vs. IPv6 pools. A new DHCP Group may be created from the DHCP Groups subtab "Add Group" button. Enter the Group Name and parent resource. Once created, you may attach a DHCP server to the Group, associate a failover, and add pools to it.

Next, you may add/assign DHCP pools. Before assigning pools, ensure that you have suitable IP aggregates created in ProVision meeting your desired parameters to assign to the pool (such as desired RIR, region, VLAN, or allocated to a specific Resource). If assigning a pool out from a specific resource, ensure ahead of time that the resource contains suitable blocks that have subassignments enabled.

To add a pool to a DHCP Group, click the "Add Pool" button for that group. You may also add a pool from the DHCP Pools subtab without associating the pool with a DHCP Group. From the "Create New Pool" dialog, select the pool type ("Subnet" or "Host), enter in the relevant information, and select to either Direct Assign a specific block, or have ProVision Smart Assign a block based on provided filter criteria - such as assigned resource, region, rule, or VLAN. Click "Save" to complete the Pool assignment.

Once servers, groups, and pools have been created, you may complete management tasks such as pushing configs on either a server, group, or individual pool level, schedule pushes, update reservations or assignment ranges, and change group/server associations as needed.

DHCP WORKFLOW



For more information on DHCP tasks, see the following sections:

- DHCP Tab
- Working with DHCP Groups
- Working with DHCP Pools
- Working with DHCP Gadgets
- DHCP Administration
- Working with DHCP Servers

DNS Workflow

DNS in ProVision revolves around Groups. Zones are gathered under Groups, servers attached to Groups, and pushes may be done on a per Group level. Thus, the first workflow step in DNS is to set up one or more DNS Groups. A "Default Group" is automatically provided, but other Groups may be desired to organize zones and default values.

To create a new DNS Group, click the "Add Group" button from the **DNS Groups** tab. Enter the desired default values for the Group, and save. If only using the Default Group, ensure the default parameter values are set as needed. For more information, see Working with DNS Groups.

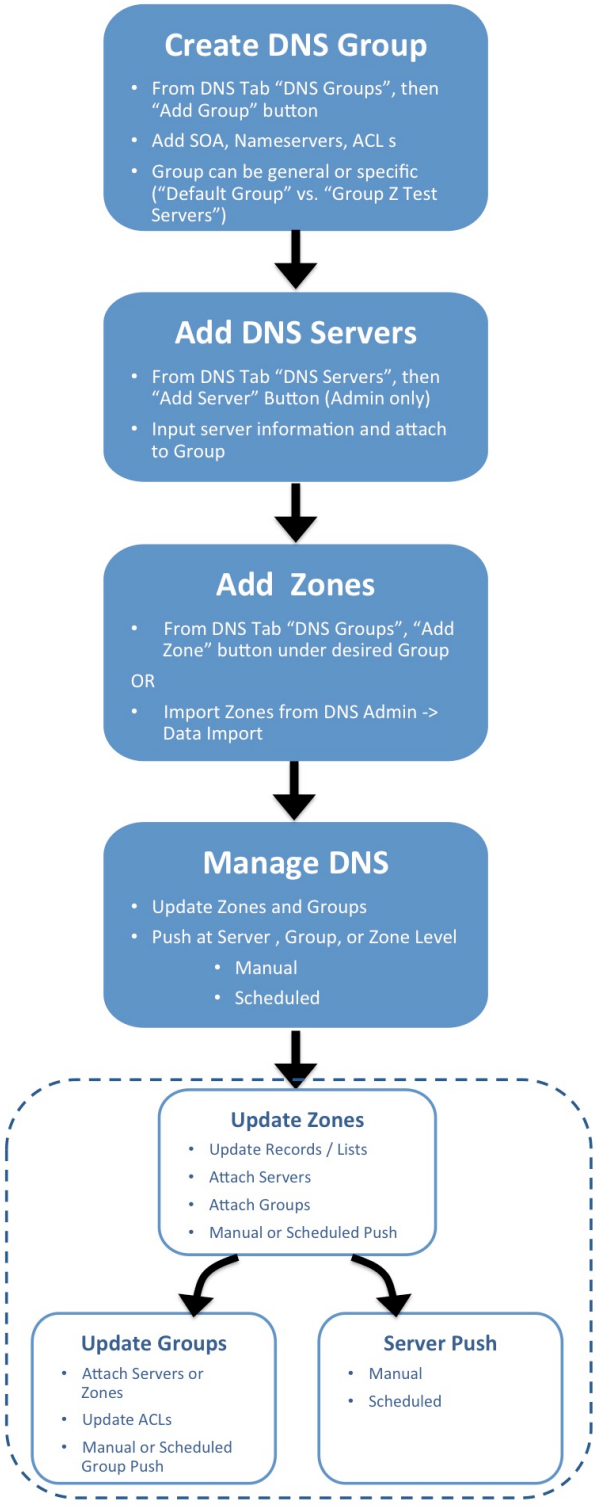
After Groups have been set up, DNS servers should be added or settings verified. Admin users may add DNS servers from the **DNS Servers** tab "Add Server" button. Input the server information and save. Existing servers may be reviewed and edited by clicking on the server name in the DNS Server List. Once a server is created, it may be attached to any DNS Group under the Group's "Attached Servers" module. Attaching a server to a Group will allow for zones in that group to be pushed to the attached server(s). See Working with DNS Servers.

Next, add zones to your groups. Zones may be manually added under each group by clicking the "Add Zone" button, or it may be imported via DNS Importers into a selected Group. Add the zone and record information, and save. See Working with DNS Zones for additional information.

Zones may be only exist once per Group, but may be duplicated under multiple Groups. Zones may also be moved from Group to Group as needed.

At this point, all major components of the DNS system have been added - from here management tasks take over. Zones may be updated and moved to or from Groups; Groups may be edited with different default values or servers, and pushes maybe be performed for an individual zone, a full Group, or for an entire server. Pushes may be manual or scheduled for a future time through the Scheduler.

DNS WORKFLOW



For more information on DNS tasks, see the following sections:

- DNS Tab
- Working with DNS Groups
- Working with DNS Zones
- DNS Administration
- Working with DNS Servers
- Import DNS Zones

Approvals Workflows

Initial Setup

The high level process to use when first setting up approvals is as follows:

1. Review User Groups and Approval Process Needs

Step 1 - Review Existing User Groups and Process Needs

When setting up Approvals for the first time, review the information in the previous section under "Approvals Fundamentals" to ensure a basic understanding of how Policies, Actions, and User Groups relate together in Approvals.

Then, take a few minutes to think about the following questions to get a better sense of how to use Approvals with your specific organization:

Who are the users that perform DNS / DHCP tasks, and at what level?

Affects which users should be included in what User Groups

What User Group(s) are they in?

Approvals settings are applied to the User Group, not individuals - ensure users with similar oversight needs are grouped together

What actions made by a certain user group should be automatically denied, if any?

Assign the "Deny Action" policy to that Action/User Group combination

What actions made by a certain user group should require oversight (admin approval / rejection)?

Assign "Approve Action" to that Action/User Group combination

Who is the admin / User Group that will make the final approval on a change?

Ensure the approver(s) is in a User Group with the "Approve Action" policy assigned for the actions requiring approval

Should any changes require multiple admins / User Groups to approve it in order to execute?

A single user from every group assigned with "Approve Action" must approve the action for it to succeed

If two admins are required to both separately agree on a change, they should be under two separate User Groups assigned "Approve Action"

What User Groups would need to receive email Approval Status notifications, and on what type of actions?

Affects whether to enable notifications and set up the scheduler task to send the notifications, and to what User Groups. When enabled, all users of the relevant group(s) will receive the email(s)

Once your User Groups are optimized for use with Approvals, you may want to write down a quick note on which Action Types and policies are planned for each group.

2. Edit User Groups / Create Approvals-Specific User Groups, if needed

Step 2 - Add or Edit User Groups

From here, depending on the answers to the questions in step 1, you may need to do one or more of the following from the **Users** tab:

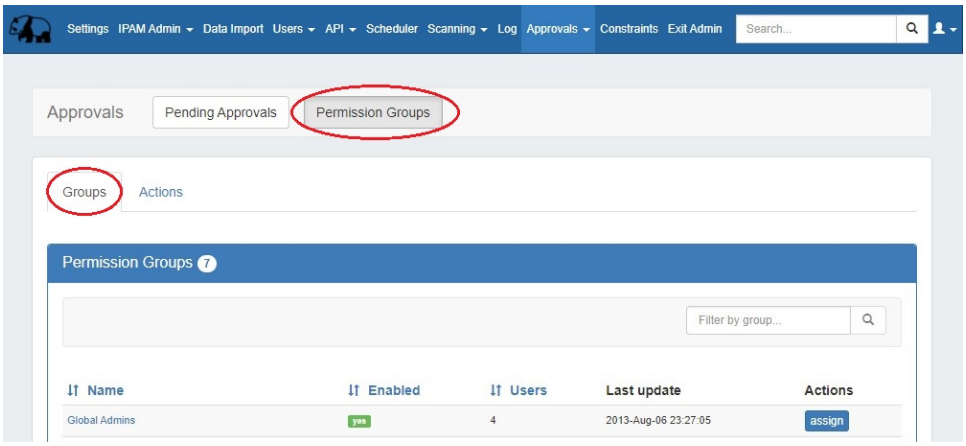
a. Edit existing User Groups to add or remove users, in order to combine users who will need similar action types approved.
b. Verify the User Groups have appropriate CRUD permissions set to perform the action(s) to be approved (e.g, you may have previously removed "Create" permissions for a group, but if the intent is now for those users to have "Add" actions approved by an Admin, the submitter will need User Group resource "Create" permissions back!)
c. Create new User Groups specifically for use with Approvals (recommended)
d. Associate users with different, or additional User Groups (remember - users can be associated with multiple groups!)

For more information on adding and editing User Groups, see Users & Permissions, Global Permissions, and Working With Users.

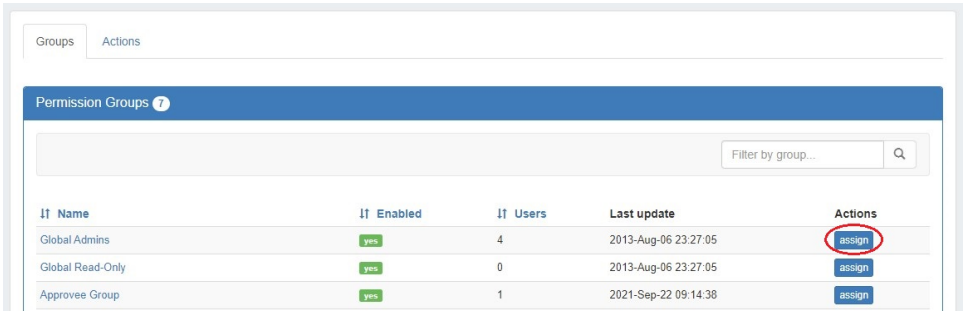
3. Assign Action and Policy Settings to User Groups

Step 3 - Assign Approval Action Settings to Groups

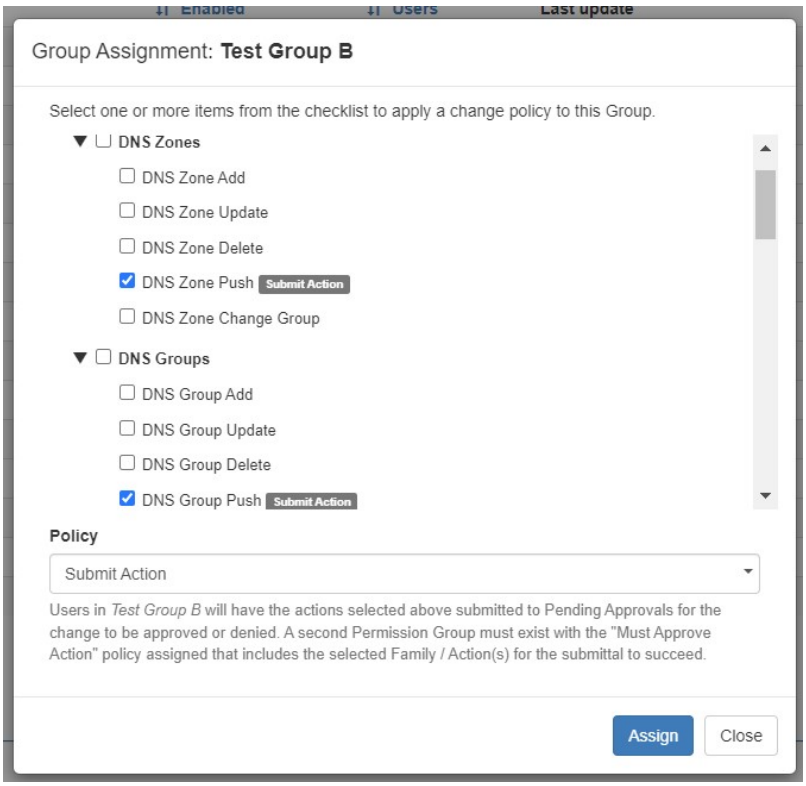
From the Approvals Tab, navigate to the **Permission Groups** sub-tab.



Then, under the **Groups** page tab, find the User Group you wish to want to assign a policy to and click "Assign".



Clicking the "Assign" button for a group brings up a checklist to select what policy to apply to the group for what Family and Actions (i.e. DNS Zone 'Add' or DNS Group 'Update'). Select either "Deny Action", "Submit Action", or "Approve Action" under Policy. Once a policy is selected, you can "quick-select" all actions for a DNS Family (Severs, Groups, Zones, Records) or DHCP Family (Servers, Groups, Pools, Reservations) by clicking the checkbox next to the family name, or only select individual action types for each Family.

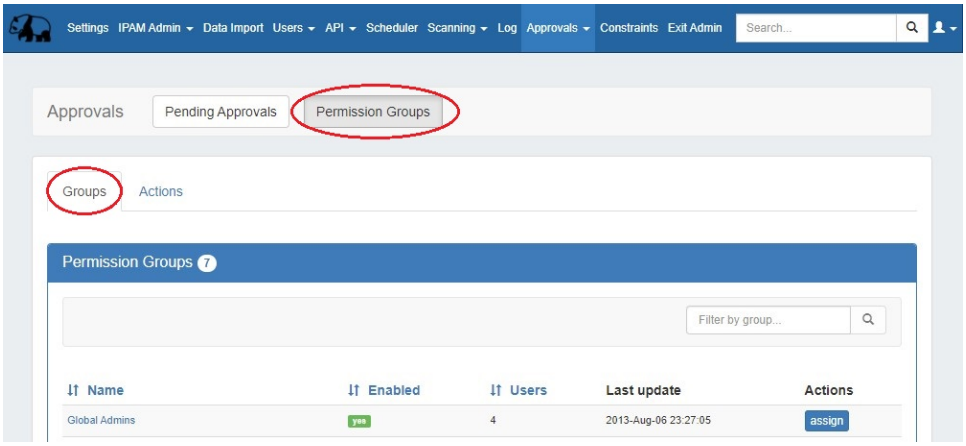


When done, Click "Assign", and repeat as needed for other Policy types or User Groups.

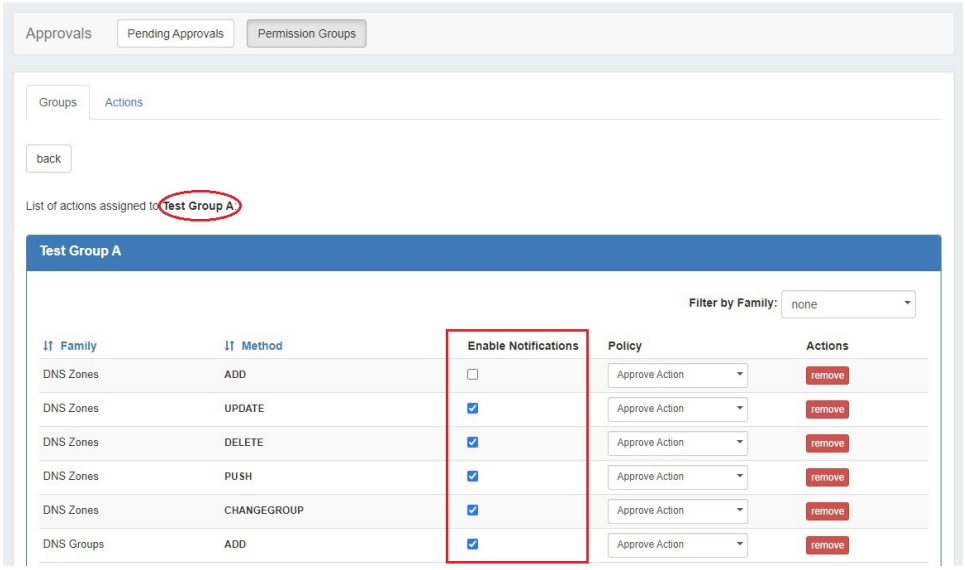
4. If using Approvals notifications, enable notifications for the appropriate Permissions Group(s)

Step 4 - Enable Notifications (Optional)

From the Approvals Tab, navigate to the **Permission Groups** sub-tab **Groups** page tab.



Click on the group name for which you want to set notifications - the Group Permissions Detail page will provide additional information on the group's settings.



For any Family/Action that you want to enable notifications, click the checkbox under "Enable Notifications". All users of that group will get email notifications when a change of the selected type(s) are made.

5. If using Approvals notifications, set up a Scheduler task for "Approvals - Process Subscription"

Step 5 - Add Scheduler Task: "Approvals - Process Subscription"

The "Approvals - Process Subscription" task processes approval request events and handles the sending of notification emails to subscribed Approvals Groups - this task must be created and running on a regular interval in order for Approval Notification emails to be sent.

In order to receive the most up to date information in the Approval Notifications, is recommended to create this task with a run time of "every 5 minutes" and no end date.

For information on setting up Scheduler Tasks, see Scheduler Tab.

6. Set up a Scheduler Task for "Approvals - Delete events older than 1 month", to occasionally clear out old and obsolete Approval request events

Step 6 - Add Scheduler Task: "Approvals - Delete events older than 1 month"

The "Approvals - Delete events older than 1 month" task deletes any Approvals history events older than 30 days.

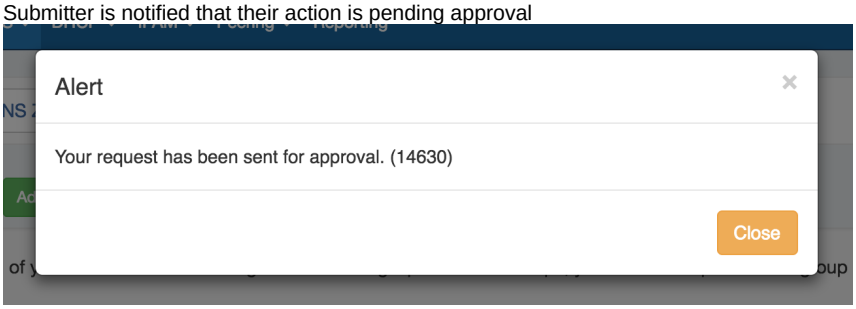
It is recommended to set this task to run monthly with no end date, to clear out obsolete approvals items, reduce data storage space needs, and reduce approvals page load time.

For information on setting up Scheduler Tasks, see Scheduler Tab.

Daily Use

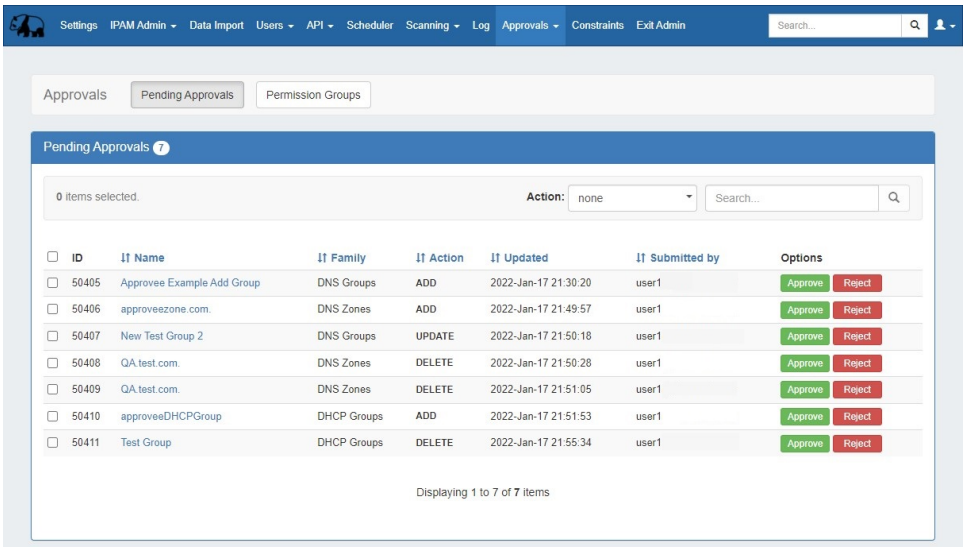
On a day-to-day basis after initial setup, an Approvals Workflow will be similar to the following (with "Submitter" as the user whose actions require approval, and "Approver" as the admin with the ability to approve/reject the change):

1. Submitter makes an action (either by action type or DNS Family) that requires approval
2. Submitter is notified that their action is pending approval

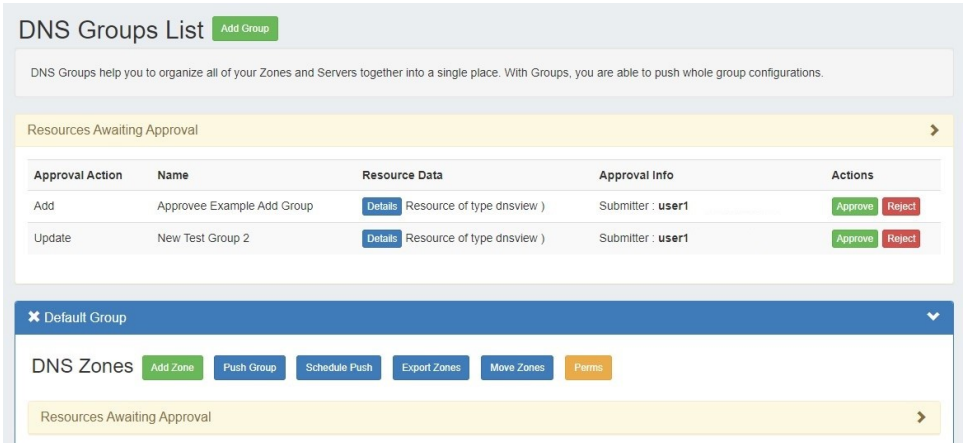


3. The requested change is sent to the **Approvals** Tab **Pending Approvals** list, and also to the **DNS** **Resources Awaiting Approval** module (the submitter may see their own submitted action under "Resources awaiting approval", but only Approvers can take approve /reject actions)

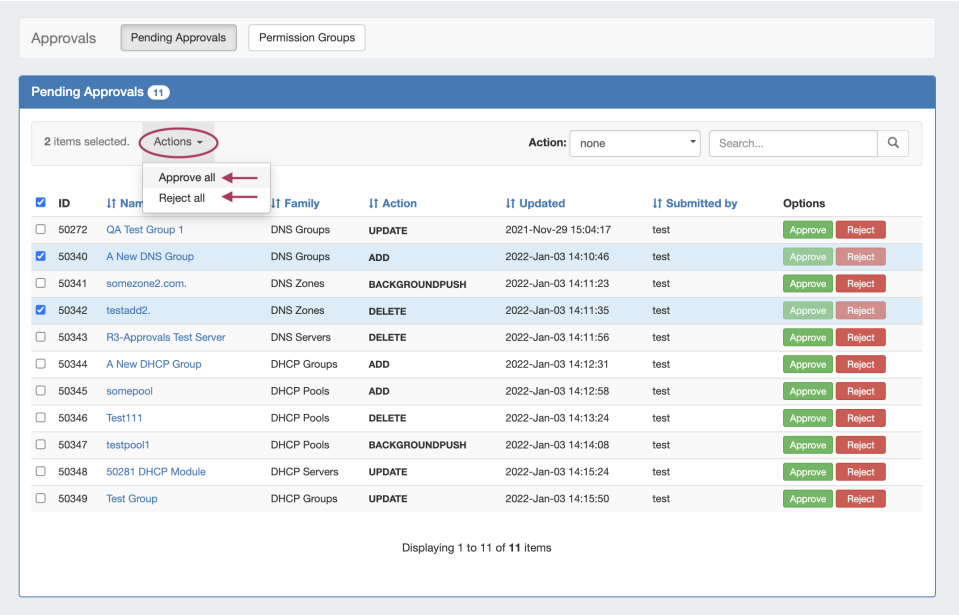
   The **Pending Approvals** list is under the **Approvals** Tab. It shows Approvals events (change requests) for which the user has the ability to Approve or Deny - it does not show approval requests for all of ProVision or those for other users.



   A "Resources Awaiting Approval" module will display in selected DNS / DHCP pages to Users with Admin / Approval permissions, if a change has been submitted on that page that is pending approval by the User's Approval Group.

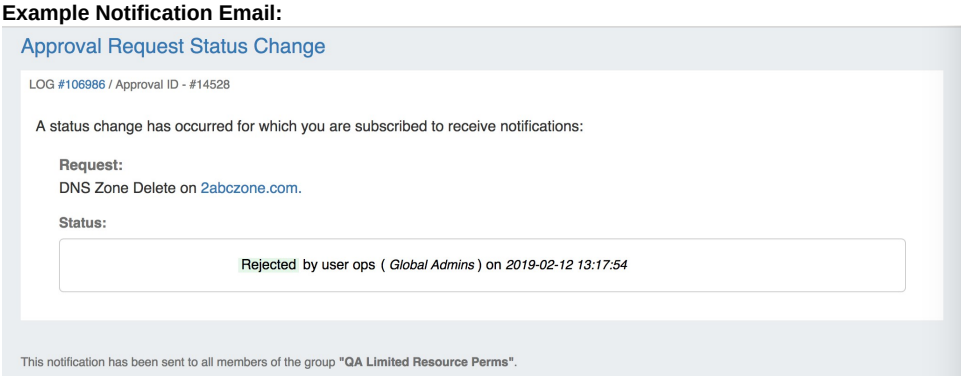


4. The Approver reviews the change in either their **Approvals** Tab **Pending Approvals** list, or the **Resources Awaiting Approval** module, and chooses to Approve or Reject the change:



a. If Approved, and no other groups need to approve it, then the change executes and is saved. A status change notification email is sent, if enabled.
b. If Approved, and is waiting approval from an additional User Group, the change continues to be held as Pending, until the other group responds (Both groups must "Approve" for the change to execute). A status change notification email is sent, if enabled, stating that the change is awaiting another Group.
c. If Rejected, the change is not executed. A status change notification email is sent, if enabled.

Example Notification Email:



See the following areas for more information on Approvals:

- DNS Tab
- DHCP Tab
- Approvals
- Pending Approvals
- Permission Groups
- Scheduler Tab