

Admin Management Tools

Accessed from the System Configuration menu, this is where you create/edit roles and permission as well as Admin User Accounts.

- [Manage Roles and Permissions](#)
- [Permissions in OPS-COM](#)
- [Manage Administrator Groups](#)
- [Manage Admin User Accounts](#)
- [IP Filtering for Admin Users](#)

Manage Roles and Permissions

Roles and Permissions in OPS-COM provide granular control over what administrative users can access and do within the system. This feature allows administrators to define specific responsibilities, enhance security, and ensure that each user has appropriate access levels, streamlining operations and maintaining data integrity.

Using this Feature

1. Click **System Configuration**, then **Admin Management**, and click **Manage Roles**.

Creating and Managing Roles

Roles are central to the permissions system, acting as templates for sets of permissions.

1. The **Manage Administrator Roles** page will display. The **System Administrator** (Primary) role is pre-defined and allows you to create new roles and assign them to other admin users.
2. To create a new role, click the **Add New Role** button at the bottom of the page.
3. Enter a descriptive **Role Name** and a **Description** for that role.
 - The description will appear as a rollover tooltip when you mouse over the **Edit Role** button for that role.

- Click **Save Role** to save your new role.

Administrator Roles

Primary Admin	Permissions	
Tomahawk	Permissions	
Administrator Highest Front Line	Permissions	
Appeals Officer	Permissions	
Counter Admin	Permissions	
Dispatcher	Permissions	
Financial Admin	Permissions	
Incident Manager Admin	Permissions	
Incident Officer	Permissions	
Locker Admin	Permissions	
Parking Manager Admin	Permissions	
Parking Validation Manager	Permissions	

Manage Administrator Roles

Editing Permissions: Administrator Highest Front Line

10 4 13 12 24 11 8 5 17

- ☒ View Users Ability to view Users information
- ☒ Edit Users Ability to add / edit Users
- ☒ Delete User Aliases Ability to delete Aliases from a User's Profile
- ☒ Edit Vehicle Information Ability to edit Vehicle Information
- ☒ Edit Forms Ability to edit and create forms in the Form Builder (User Management / Forms)
- ☒ View Forms Ability to view completed form data but not edit the forms
- ☒ Manage Active Alarms Can manage active alarms on user profiles.
- ☒ Send Bulk Emails Ability to send Bulk Emails to Users
- ☒ View User Uploads View the files that have been uploaded by a user.

Editing Existing Roles

You can modify the name and description of any role (except the **System Administrator** role).

- On the **Manage Administrator Roles** screen, click the **Edit Role** button next to the role you wish to update.
- Make your desired changes to the **Role Name** and/or **Description**.
- Click **Save Role** to save your edits.

Assigning Permissions to a Role

Once a role is created, you'll define what actions users assigned to that role can perform by setting its permissions. [Refer to this article for more detailed Permissions information.](#)

- On the **Manage Administrator Roles** screen, click the **Permissions** button next to the role you want to configure. The **Editing Permissions** screen will display.
- The top bar displays various icons, mirroring the OPS-COM menu structure. The number next to each icon indicates how many permissions within that category have been selected for the current role.
- Click an icon (e.g., a "Permit" icon, a "Violations" icon) to display the specific permissions available within that category.
- To grant a permission, enable the checkbox next to that permission's name.
- Once you have navigated through each icon and selected all the necessary permissions for the role, click **Save Permissions**. The role, with its defined permissions, is now created and ready for assignment.

Assigning Roles to Admin Users

After roles are defined, you can assign them to your administrative users.

1. Click **System Configuration**, then **Admin Management**, and click **Edit Admin Users**. The **Manage Active Administrators** page will display.
 2. Select an existing user you wish to modify, or choose to create a new user.
 3. On the left side of the screen, add or confirm the **User Information** (e.g., name, email).
 4. On the right side, select the role(s) you wish to apply to that user from the available options.
 5. You can also add a **Comment** for any relevant notes about the user's role or status.
 6. Click **Update User** when you have finished making your changes.
-

Best Practices & Considerations

- **Principle of Least Privilege:** Always adhere to the principle of least privilege. Grant users only the permissions absolutely necessary for them to perform their job functions. This minimizes security risks and potential for accidental errors.
- **Role-Based Access Control:** Utilize roles to manage permissions efficiently. Instead of assigning individual permissions to each user, create roles (e.g., "Enforcement Officer," "Permit Manager," "Finance Admin") and assign users to those roles. This simplifies onboarding, offboarding, and auditing.
- **Clear Role Descriptions:** Use the role description field to clearly state the purpose of the role and the types of permissions it encompasses. This helps administrators understand what each role is intended for.
- **Regular Review:** Periodically review your defined roles and user assignments to ensure they remain appropriate as job responsibilities change or staff join/leave your organization.
- **Test New Roles:** Before deploying a new role to active users, test it with a test administrator account to confirm that the assigned permissions function as expected and do not inadvertently grant too much or too little access.

Permissions in OPS-COM

User Management Permissions

Permission Names	Description
View Users	Allows the admin user to view, but not change, the users in the system. User Search functionality is enabled.
Edit Users	<p>Allows the admin user to edit users in the system including new User Registration.</p> <p>This should be used with the 'View Users' permission.</p> <ul style="list-style-type: none">• If 'View Users' is enabled, Admins can see the user history including Permits and Violations issued (but not the details) and any payments outstanding for this user.• If 'View Users' is not enabled, Admins can only use the User Registration portion and cannot search for existing users.
Delete User Aliases	This permission allows users to Update User Aliases. It cannot be used without 'View Users' and 'Edit Users' turned on.
Edit Vehicle Information	Allows Admin to update vehicles and view the vehicle's history. Admins can also do a Plate Search from the User Management menu. In addition, Admins can see the DNTT reports.
Edit Forms	Allows Admins to create, update and view forms.
View Forms	Allows Admins to view all forms and see the user-submitted entries of forms. Users cannot create or edit forms without the 'Edit Forms' permission.
Manage Active Alarms	Allows Admins the ability to update and clear alarms on the user's profile. This must be used with 'View Users' and 'Edit Users' permissions enabled.
Send Bulk Email	Allows Admins to send email messages to various groups of Users.
View User Uploads	View the files that have been uploaded by a user.
Delete User Uploads	Delete the files uploaded by users.

Locker Permissions

Permission Names	Description
View Lockers	Allows the Admin to view lockers and look at locker history. As well the Admin can see lockers awaiting payment.
Edit Locker Information	Allows users to edit the locker information.
Allocate Lockers	Ability to allocate locker numbers to a building area.
Edit Locker Allocations	Allows creation and editing of locker sales windows, allows Admin users to view active locker sales window

Parking Permissions

Permission Names	Description
Pricing & Lot Administration	Allows Admins to create and edit lots. This permission will not work by itself. The Admin must also have the following permissions: <ul style="list-style-type: none">• View Permits• Edit Permits• Allocate Permits• Edit Permit Allocations
View Permits	This allows the Admin to view Permit records, do Permit Switches and to view waiting lists.
Edit Permits	This allows the Admin to edit Permit details. This permission allows access to most functions that relate to permits.
Allocate Permits	Grants the ability to allocate permits to different lots. This permission will also grant all privileges of the 'View Permits' permission.
Edit Permit Allocations	Allows access to edit the Permit Allocation Sales Window and the Active Permit Sales Window.
View Access Cards	Allows the Admin to view Access cards. This will not work without the 'View Permits' permission enabled as well.
Edit Access Cards	Allows the Admin to edit Access cards. This will not work without the 'View Permits' permission enabled as well.

Add Access Cards	Allows the Admin to add Access cards. This will not work without the 'View Permits' permission enabled as well.
Create Temp Permit Entries	Allows Admins to use the Parking Validation utility. Please note,
Manage Validator Group Records	View and delete records created with the validation tool from admins within the same group as the admin.
Manage All Validator Records	View and delete records created with the Validate Parking tool from other admins.
Edit Unpaid Standard Permit Costs	Ability to change the price on an unpaid standard permit.
Prorate Permit Purchases	Allows the Admin to prorate permit purchases for the end user. This cannot be used without 'User Management' permissions and 'Edit Permits' enabled.
Access Subscription Report	Ability to access the Subscription Verification Report and export results.

Violations Permissions

Permission Names	Description
View Violations	Allows the Admin to see information about violations including, basic user details and details of any payments.
Edit Violations	Allows the Admin to search for violations. This permission requires 'View Violations' to see the details.
Edit Violation ticket number	Grants the ability to edit a violation number if you also have the 'View Violations' permission.
Display as Ticket Writer	Grants the ability to be a ticket writer on the Handheld or the Web if the Admin also has the 'Add New Violations'.
Add New Violations	Allows the Admin to issue a violation. The Admin must have the 'Edit Vehicle Information' permission found in the User Management section.
Grant Violation Appeals	Gives the ability to manage Appeals and grant them. The Admin must have the 'View Appeal Reports' permission as well.
View Appeal Reports	Allows the Admin to view Appeal reports for different officers. Admins must also have the 'View Violations' and 'Edit Violations' permissions.
Issue / View Violation Notices	Allows the Admin the ability to issue and View Violation Notices.
Manage Collections	Grants the ability to manage the collections process for violations.

View Violation Reports	Allows the Admin to view financial and statistical reports regarding violations. Admins must have the 'View Violations' permission as well.
Pay Violations in Collections	Allow for the admin to process payments on violations that are in collections.
Purchase while Outstanding	Purchase items for the user while the user has a violation that has been sent to collections. Only necessary while Prevent Purchases is turned on in the settings.

Incident Permissions

Permission Names	Description
Add/Edit Contact History User Notes	Grants the Admin the ability to add / edit notes in contact history. You must have User Management permissions to use this since it is accessed through the user profile.
Delete User Contact History Notes	Grants the Admin the ability to delete User notes in contact history. You must have User Management permissions to use this since it is accessed through the user profile. You must also have the 'Add/Edit Contact History User Notes' permission.
View All Incidents	This is a master permission that grants the ability to view all Incidents. This permission is normally used for high-level Admins as it grants access to all information.
Add Incidents	Allows the Admin to add incidents and have an incident reported on their behalf.
Open Incidents	Allows the Admin to open incidents that are closed. This requires the 'View all Incidents' permission. This permission is normally used for high-level Admins.
Delete Incident	USE WITH CAUTION - This permission should only be added to a Primary Admin. If this is enabled the Admin can remove the incident and all related records and files where they are not used in other reports. There is a button on the incident to "Delete Incident".
Edit Incidents	Grants the ability to edit Incidents. This requires the 'View all Incidents' permission. This permission is normally used for high-level Admins.
View Incidents - Self	Allows the Admin to view Incidents if they are listed as the reporter.
Edit Task Notes on Incidents	Grants the ability to edit comments on Incident tasks. Requires the 'View all Incidents' permission.

Edit Incident summaries	Allows the Admin to edit Incident Summaries. Requires the 'View all Incidents' permission.
Incident Administrator	Grants the ability to view and edit incidents. This permission is normally used for high-level Admins.
View/Edit Confidential Information	Allows the Admin to View/Edit Confidential Information on reported incidents. Requires the 'View all Incidents' permission.
Be assigned Tasks Directly	Allows the Admin to be assigned as an investigator for an Incident.
Edit Incident Tasks	Grants the ability to edit Incident Tasks. Requires the 'View all Incidents' permission.
Close Incidents / Checklists	Grants the ability to close Incidents and Checklists. Requires the following permissions: <ul style="list-style-type: none"> • View all Incidents • Incident Administrator
Assign Incident to Case Manager	Allows the Admin to Ability to assign a Case Manager to an Incident. Requires the 'View all Incidents' permission.
Assign Incident To An Investigator	Allows the Admin to assign an Investigator to an Incident. Requires the 'View all Incidents' permission. This permission is normally used for high-level Admins.
Assign Incident To A Different Investigator	Allows the Admin to assign a different Investigator to an Incident. Requires the 'View all Incidents' permission. This permission is normally used for high-level Admins.
Is Incident Case Manager	Allows the Admin to be listed as a Case Manager that can be assigned to an Incident.
Is Incident Shift Manager	Allows the Admin to be listed as an Incident Shift Manager. This will require some other high-level permissions as required for the job.
View Incidents Distribution Reports	Grants the ability to view the Incident Distribution Reports.
View Incident Reports	Grants the ability to view all Incident Reports in OPS-COM.
View Incident In-House Report	Grants the ability to view the Unpaid In-House Incident report.
Export Incident Reports	Grants the ability to export the Recent Incidents Report and the Sub-location Report to Excel.

Dispatch Permissions

Permission Names	Description
View License Plate Alarms	Allows Admins to view License Plate alarms.

Receive License Plate Alarms via email	Allows Admins to receive Plate Alarms via email if they also have subscribed to the Alarms list.
View People Alarms	Allows Admins to view People alarms.
Receive People Alarms via email	Allows Admins to receive People Alarms via email if they also have subscribed to the Alarms list.
Add New Dispatch Logs	Grants the ability to add dispatch logs.
Edit Dispatch Logs	Grants the ability to edit the Admin's own dispatch logs.
Edit All Dispatch Logs	Grants the ability to edit the dispatch logs of other Admins.
Open Dispatch Logs	Allows Admins to Open dispatch logs.
View Dispatch Logs	Allows Admins to View dispatch logs and close log records.
Add/Drop Dispatch Logs	Grants the ability to remove the association of a Dispatch Log with an incident.
View Cameras	Allows the Admins to view Cameras, if this is configured with OPS-COM.

Payment Permissions

Permission Names	Description
Manage User Credit Cards	Grants the ability to add, remove and update credit cards from Users.
View Payments	Grants the ability to view payments. Limited access to user information is also granted.
Edit Payments	Allows the Admin to process payments. Admin must have the 'View Payments' permission.
Change Payment Type	Allows the Admin to change the Payment Type of a payment.
Drop Payments	Allows the Admin to drop payments.
Mark Bulk Payments	Grants the ability to mark Bulk payments for bulk processing.
Refund Payments	Grants the ability to refund payments, but not process.
Process Refunds/Adjustments	Allows the Admin to process refunds and adjustments.
Edit Payment Types	Ability to configure available payment types.

System Content Permissions

Permission Names	Description
View and Select Files	Grants the ability to view and select files for use in editors. Admins must have the 'Manage System Messages' permission as well.
Manage Files	Allows the Admin to add and remove files for use with content editors. Admins must have the 'Manage System Messages' permission as well.
Manage System Messages	Grants the ability to edit the email templates, home page messages, system messages, Temp Permit Text and Notice Literature.
View History Search	Allows the Admin to view history searches if they also have the corresponding User Management permissions.
Purge Old Data	Allows the Admin to purge Data older than 7 years.
Manage Templates	Create and edit page templates.

System Configuration Permissions

Permission Names	Description
Manage Roles	Grants the ability to manage roles and permissions. This is typically the job of a Primary Admin only.
Edit Administrators	Allows the Admin to edit other Admin user accounts and assign roles based on their job description. This requires 'Manage Roles' to function. This is typically the job of a Primary Admin only.
Manage System Configuration	Grants the ability to edit the System Settings. This is typically the job of a Primary Admin only.
Manage User Types and Departments	Allows the Admin to manage User Types and Departments.
Manage Vehicle Configuration	Allows the Admin to setup the different Vehicles descriptions that are used in OPS-COM.
Manage Permit Types and States	Allows Admins to manage the Zones, Groups, Common Lots and Permit States. This must be used the 'Edit Permits' permission.
Manage Access Cards	Grants the ability to setup Access card options.
Manage Locations	Grants the ability to setup Locations options for use in OPS-COM.
Manage Handhelds	Allows the Admin to manage settings stored in the Handheld Commons area
Manage Violation Offence Types	Allows the Admin to manage ticket types and ticket offence items.
Manage Alert Lists	Allows the Admin to setup alert and alarm email lists.

Manage Distribution Configuration	Allows the Admin access the Distribution setup options.
Manage Dispatch Configuration	Grants the ability to the Dispatch setup options.
Manage Incident Configuration	Allows the Admin to configure the IncidentAdmin options.
Reset Database	Allows the Admin to the reset their preview database for testing.
Change Dashboards	Can change their default dashboard
Edit Dashboard Items	The ability to edit custom dashboard items.
Edit Dashboard Layouts	The ability to edit dashboard layouts
Manage Tables	The ability to manage data tables.
Reset Tables	The ability to reset data tables.
Manage Duplicates	Grants the ability to resolve duplicates in the system.
Access Beta Site	Can access the Beta Site
View Banners	Can view various banners such as trial and usage limits

Manage Administrator Groups

Administrator Groups in OPS-COM allow you to organize administrative users into logical teams or departments. This feature simplifies management by enabling you to apply specific settings, distribute communications, or assign tasks to a collective of administrators rather than managing each user individually, enhancing organizational efficiency and control.

Using this Feature

1. Click **System Configuration**, then **Admin Management**, and click **Manage Groups**.

You'll be directed to the **Manage Administrator Groups** page, which lists all existing groups. Initially, this page may be empty if no groups have been created yet.

Creating a New Administrator Group

1. Click **Add New**.
2. The **Adding New Group** form will appear where you can define your group.
3. Fill out the required information for the group, such as the **Group Name**.
4. Click **Save Group** to finalize the creation.

Once saved, your newly created group will appear in the list on the left-hand side of the page.

Working with Groups

After creating groups, you can perform various management actions. While the provided content focuses on creation, typical group management also involves:

- **Editing Group Details:** You can usually click on a group's name or an **Edit** button next to it to modify its name or other associated settings.
- **Assigning Administrators to Groups:** Administrators are assigned to groups through their individual user profiles.
 1. Navigate to **System Configuration**, then **Admin Management**.

2. Click **Edit Admin Users**.
3. Select the desired administrator.
4. Within their profile settings, you'll find an option to assign them to one or more **Admin Groups**.

- **Deleting Groups:** Most systems allow you to delete groups that are no longer needed, often with a confirmation prompt. Be aware that deleting a group might impact any administrators or settings associated with it.
-

Best Practices & Considerations

- **Logical Organization:** Create groups that reflect your organizational structure (e.g., "Enforcement Team," "Permit Office Staff," "IT Support"). This makes it easier to manage permissions, communicate, and assign responsibilities.
- **Streamlined Management:** Using groups simplifies tasks like sending system-wide messages or applying default settings, as you can target a group rather than selecting individual administrators.
- **Clarity in Naming:** Use clear and concise names for your groups to avoid confusion among administrators.
- **Regular Review:** Periodically review your Administrator Groups to ensure they remain relevant and accurately reflect your team's structure and needs. Remove any outdated or unused groups to maintain a clean system.

Manage Admin User Accounts

Creating and managing administrator accounts in OPS-COM is essential for granting system access to staff, defining their responsibilities through roles, and maintaining secure and accurate user records. This article guides OPS-COM administrators through the process of creating new admin accounts, editing existing ones, resetting passwords, and disabling accounts as needed.

Using this Feature

1. Hover over **System Config**, click **Admin Management**, then **Edit Admin Users**. The **Manage Active Administrators** screen displays, providing options for both new user creation and existing user modification.

Creating a New Admin Account

1. On the **Manage Active Administrators** screen, select **+ Create New Admin**.
2. The screen will display the **Create New Administrator** form divided into two sections:
 - On the left, you will **enter the user information** for the new administrator (e.g., username, first name, last name, email, and initial password).
 - On the right, in the **Active Roles** form, you will **select the admin role(s)** this person will be granted. For more information about Roles and Permissions [refer to this wiki article](#).
3. Once all information is entered and roles are selected, click **Insert New User** to add the admin account to the system.

Editing an Existing Admin Account

1. On the **Manage Active Administrators** page, select the user you wish to modify.
2. You can now change any of the available options for that selected user, including their personal information, roles, and account status.
3. Click **Update User** when you are finished making your changes.

Viewing Login Activity

- For any selected user, you can click the **Login Activity** button to view a log of when the administrator last logged into the OPS-COM system or a handheld device.

Resetting an Admin's Password

1. Locate the specific administrator's account.
2. In the **Password** field, enter a temporary password. The password is hidden (displayed as asterisks "*****"), but you can simply type over the existing symbols.
3. **Inform the admin of this temporary password.**
4. When the admin logs in using the temporary password, they will be prompted to update their password to a more secure, personal one.

Disabling an Admin Account

Admin users cannot be permanently deleted from the system because their accounts are often linked to historical data (e.g., ticket issuance, system changes). If an admin user changes roles or leaves the organization, the best practice is to disable their account.

Important Reporting Note - It is very important to leave the admin user's permissions in place even when disabling their account, as these permissions will still affect historical reporting (e.g., showing which permissions were active at the time certain actions were performed). Once the account is disabled, any existing permissions obviously cannot be actioned by that user, but they remain associated for reporting purposes.

1. Hover over the **System Config** menu, click **Admin Management**, then **Edit Admin Users**.
2. Select the user's account you wish to disable (e.g., "jim_daniels").
3. The user's profile will display. Locate the checkbox titled **Activate this account and allow system login**.
4. **Uncheck** this box to disable the account.
5. Click **Update User** to apply the change.

After disabling, the account will now appear on the **Manage Disabled Administrators** page, accessed by clicking on **View Disabled** on the **Manage Active Administrators** page.

This action can be reversed at any time by editing the user account and re-checking the **Activate this account and allow system login** checkbox.

Best Practices & Considerations

- **Secure Initial Passwords:** When creating new accounts or resetting passwords, use strong, temporary passwords and instruct users to change them immediately upon first

login.

- **Role-Based Access:** Always assign appropriate roles to admin users. Avoid giving **Primary Administrator** access unless absolutely necessary. Granular roles ensure users only have access to the functions they need.
 - **Prompt Disabling:** Disable accounts promptly when an employee's role changes or they leave the organization. This is a critical security measure.
 - **Audit Login Activity:** Regularly review the **Login Activity** for admin accounts to monitor for unusual patterns or unauthorized access attempts.
 - **Clear Documentation:** Maintain internal records of your admin accounts, their assigned roles, and any specific notes, especially for disabled accounts.
-

Related Video

<https://www.youtube.com/embed/pKpDFhMcTXA?wmode=opaque>

<https://www.youtube.com/embed/VDg5pjzDc28?wmode=opaque>

IP Filtering for Admin Users

IP Filtering in OPS-COM provides administrators with a robust security layer by restricting user access based on their device's IP (Internet Protocol) address. This feature enhances system security by ensuring that only authorized users from specified networks or devices can log into OPS-COM, allowing for tailored access control according to individual roles and organizational security policies.

Setup & Configuration

IP filtering configurations are managed within each administrator's user profile in OPS-COM.

What is an IP Address?

An IP address is a unique numerical label assigned to each device connected to an IP network. It typically consists of four groups of numbers (octets), separated by dots (e.g., `192.168.1.1`).

- The **first two octets** generally identify the network your device is on.
- The **last two octets** further narrow the address down to a specific machine within that network.
- To find your current public IP address, you can visit a website like `whatismyip.net` or simply search "What is My IP" in Google.

To Configure IP Filtering in OPS-COM:

1. Hover over the **System Config**, then **Admin Management**, and click **Edit Admin Users**.
2. On the **Manage Active Administrators** page, select the specific user you wish to edit.
3. Locate the **Allowed IPs** field within the user's profile configuration. This is where you will enter the IP filtering rules.

Create New Administrator

[Back](#)

Login Activity

Login As Admin

☐ Activate this account and allow system login

Username

apowers

Password

Setting the password will require the admin to update their password again upon their next login.

Passwords are case sensitive.

Email

apowers@ops-com.com

Display Name

Admin Groups

Active Dashboard

** Default Layout

Cadre No.

Task Group

Redirect To

Allowed IPs

one per line

A single period matches all IP's
123.45 An IP prefix matches a WAN network
123.45.67.89 A full IP matches a WAN address
123.* Wildcards do not work
mydomain.com Domain names do not work

Lookback hours for dispatch

Blank allows this user to search all logs

Active Roles

☐ System AdministratorHigh level access including managing roles

☐ TomahawkTomahawk users offer system support

☐ System ManagerSecond level administrator

☐ Alarm MonitorsAdmins who should be notified by alarms

☒ Appeals OfficerGrant, uphold or cancel violations

☒ Counter StaffAccept payments and assign permits

☐ DispatcherManage dispatches and assign to incidents

☐ Financial ManagerManage payments, refunds and all reporting

☐ Incident Admin

☐ Incident ManagerAccess to manages all incidents

☐ Incident OfficerOfficer working with incidents

☐ Incident Officer Jr.

☐ Locker ManagerManages all aspects of lockers

☐ Parking ManagerSet up parking lots, allocations, and pricing

☐ Patrol OfficerIssues violations and citations

☐ Test RoleTest permissions.

☐ Validation AttendantRecords parking validations

☐ Validation ManagerValidate plates and includes reporting

Using this Feature

The **Allowed IPs** field in an admin user's profile controls their access to the OPS-COM system. The level of access can be precisely tailored:

Configuration Options for Allowed IP Addresses

Allow Access from Any Network (Least Restrictive)

This is typically used for high-level managers or directors who require access from diverse locations (e.g., while traveling, from a home office, or an internet cafe).

Note: In some cases, networks might be locked down or behind a firewall. Additional configuration on the part of your IT department may be required to allow external access.

- **Configuration:** Enter a single **dot** (.) in the **Allowed IP Addresses** field.
- **Result:** The user will be able to log in from literally any network location, whether internal or external to your organization's specific network.

Restrict Access to a Specific Network

This is ideal for regular office workers who primarily require access only from their designated office network.

- **Configuration:** Enter the **first two octets** of the network's IP address (e.g., 10.32).
- **Result:** The user can log in from any computer connected to that specific network, but will be restricted from accessing OPS-COM from any other network.

Restrict Access to a Specific Computer (Most Restrictive)

This is suitable for part-time employees or student workers who are designated to use only one particular machine for OPS-COM access.

- **Configuration:** Enter the **full IP address** of the specific computer (e.g., 10.32.1.144).
- **Result:** The user can only log in to OPS-COM from that single, specified computer.

Allow Access from Multiple Specific Computers

This is useful in office settings where an employee may use a few designated workstations.

- **Configuration:** Enter the **full IP address** of each allowed computer, placing each address on a **separate line** within the **Allowed IPs** field (e.g., 10.32.1.144 followed by 10.32.1.154 on the next line).
- **Result:** The user can log in from any of the explicitly listed computers.

Allow Access from Multiple Specific Networks

This is applicable for employees working out of multiple campus locations or different buildings within a municipal organization, each on a distinct local area network.

- **Configuration:** Enter the **first two octets** of each allowed network, placing each network segment on a **separate line** within the **Allowed IPs** field (e.g., 10.32 on one line and 10.40 on another).
- **Result:** The user can log in from any computer on the specified networks.

Basic IP Filtering Rules Recap

- **Good Configurations:**

- . - A single period to match all IP addresses (least restrictive).
- 10.32 - A partial IP address to match all computers on a specific network.
- 10.32.1.144 - A full IP address to match a specific computer (most restrictive).

- **Invalid Configurations:**

- 10.* - Wildcards (*) like this will **not** work.
 - ops-com.com - Domain names will **not** work; only numerical IP addresses are supported for filtering.
-

Best Practices & Considerations

- **Security vs. Flexibility:** Balance the need for security with the practical access requirements of your administrators. More restrictive settings (full IP) offer higher security but less flexibility.
- **Dynamic IPs:** Be aware that many internet service providers assign dynamic IP addresses that can change over time. If your administrators access OPS-COM from external locations with dynamic IPs, using a full IP filter will frequently require updates, making the "single dot" setting often more practical for such scenarios.
- **Internal Network Changes:** If your organization's internal network IP scheme changes, remember to update the **Allowed IPs** field for all affected administrators.
- **IPv6 Consideration:** When using IP filtering, it is generally recommended to enter your IPv6 IP address if your network primarily uses IPv6, as IPv4 addresses are becoming less common for external facing services.
- **IT Department Collaboration:** For complex network setups, especially involving firewalls or VPNs, collaborate with your IT department to ensure proper network configuration aligns with your OPS-COM IP filtering rules.