DELEGATE IPAM ADMINISTRATION

IPAM setup creates appropriate security groups to isolate and restrict the permissions available to different sets of IPAM administrators and users. The installation process creates local security groups on the IPAM server, which provide permissions required for administering and using the multiple services employed by IPAM. For example, IP lease audit collection could be restricted to a specific set of administrators only. It is possible to display MSM configuration data to all DHCP Users, while MSM configuration rollout itself may be restricted to only a relevant subset of administrative accounts.

IPAM installation automatically creates the following local user groups:

- **IPAM Users**: Members of this group can view all information in server discovery, IP address space, and server management. They can view IPAM and DHCP server operational events, but cannot view IP address tracking information.
- **IPAM MSM Administrators**: IPAM multi-server management (MSM) administrators have IPAM Users privileges and can perform IPAM common management tasks and server management tasks.
- **IPAM ASM Administrators**: IPAM address space management (ASM) administrators have IPAM Users privileges and can perform IPAM common management tasks and IP address space tasks.
- **IPAM IP Audit Administrators**: Members of this group have IPAM Users privileges and can perform IPAM common management tasks and can view IP address tracking information.
- **IPAM Administrators**: IPAM Administrators have the privileges to view all IPAM data and perform all IPAM tasks.

http://go.microsoft.com/fwlink/?LinkId=83477).

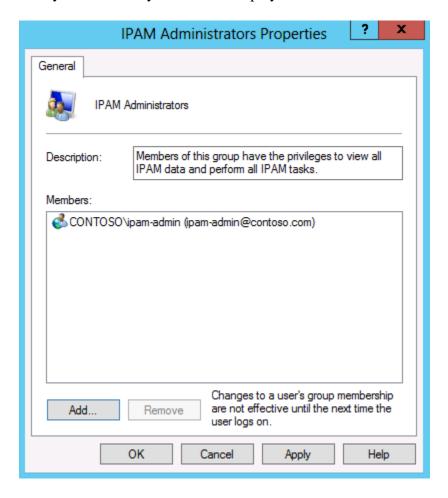
Assigning IPAM administrator roles

Use the following procedures to assign IPAM administrator roles using built-in local security groups on the IPAM server:

To assign IPAM administrator roles

- 1. On the IPAM server, click **Tools** on the Server Manager menu and then click **Computer Management**.
- 2. In the Computer Management console tree, open **Local Users and Groups** and then click **Groups**. The following local IPAM security groups are displayed:
 - o **IPAM Administrators**: IPAM administrators can view all IPAM data and manage all IPAM features.
 - o **IPAM ASM Administrators**: IPAM address space management (ASM) administrators can manage IP address blocks, ranges, and addresses.
 - IPAM IP Audit Administrators: IPAM IP audit administrators can view IP address tracking data.

- o **IPAM MSM Administrators**: IPAM multi-server management (MSM) administrators can manage DNS and DHCP servers.
- o **IPAM Users**: IPAM users can view information in IPAM, but cannot manage IPAM features or view IP address tracking data.
- 3. To add a user or group to the group, double-click the group, click **Add**, type the username under **Enter the object names to select**, and then click **OK**.
- 4. Verify that the user you added is displayed under **Members**.



- 5. To remove a user or group from the group, click the user under **Members** and then click **Remove**.
- 6. To add or remove another user or group, repeat this procedure.
- 7. Click **OK** when you are finished, and then close the Computer Management console.

The following table summarizes IPAM actions and functions that are permitted or denied with membership in the specified security group. Access rights are additive if a user or group is a member of multiple security groups.

	Convon	IP	Monitor	Event	IP Address	Common
Security Group	Server Inventory	Address	and	Catalog	Tracking	Management
	inventor y	Space	Manage	Catalog	Tracking	Tasks

IPAM Administrators	Manage	Manage	Manage	View	View	Manage
IPAM ASM Administrators	Manage*	Manage	View	View	Denied	Manage
IPAM IP Audit Administrators	Manage*	View	View	View	View	Manage
IPAM MSM Administrators	Manage*	View	Manage	View	Denied	Manage
IPAM Users	View	View	View	View	Denied	View

^{*}If the Group Policy-based automatic provisioning method is used, GPO access permission must be delegated to add or remove servers from GPO security filtering.

Common management tasks include:

- Connect to an IPAM server
- IPAM settings:
 - o Configure server discovery
 - Configure custom fields
 - o Configure utilization threshold
- Starts server discovery
- Retrieve all server data

Members of the local **Administrators** group on the IPAM server also have permission to modify the server inventory and perform common management tasks.

If a user does not have sufficient privileges to perform an action, they will receive an alert that is unique to the action they are attempting to perform.

