Comprehensive Guide to Microsoft 365 Administration and Network Security

This guide provides in-depth instructions for managing Microsoft Entra ID roles, tracking user email activity, and configuring network security settings on Wi-Fi routers and UniFi OS.

Part 1: Managing Microsoft Entra ID Roles

Classifying Microsoft Entra ID Roles

Microsoft Entra ID (formerly Azure Active Directory) uses a Role-Based Access Control (RBAC) model to delegate administrative tasks. Classifying and assigning the correct roles is crucial for security and operational efficiency. The core principle is "least privilege," meaning users should only be granted the permissions necessary to perform their job functions.

Common Role Classifications:

- **Global Administrators:** Have unrestricted access to all management features. This role should be used sparingly and assigned to a very limited number of trusted individuals.
- **User Management:** For tasks related to creating, editing, and deleting user accounts. Roles include **User Administrator** and **Helpdesk Administrator**.
- **Security and Compliance:** For managing security settings, monitoring threats, and ensuring compliance. Key roles include **Security Administrator**, **Compliance Administrator**, and **Conditional Access Administrator**.
- **Service-Specific Administrators:** For managing individual Microsoft 365 services like Exchange, SharePoint, and Teams. Examples are **Exchange Administrator**, **SharePoint Administrator**, and **Teams Administrator**.
- **Billing and Licensing:** For managing subscriptions, licenses, and billing. The primary role is **Billing Administrator**.
- **Device Management:** For enrolling, managing, and securing devices through services like Intune. The **Intune Administrator** role is central to this.

Detailed Explanation of Key Microsoft Entra ID Built-in Roles

Microsoft Entra ID provides a wide range of built-in roles, each with a specific set of permissions. Here are some of the most common ones:

Role	Description	Common Use Cases
Global Administrator	Unrestricted access to all features in Microsoft Entra ID and other Microsoft services that rely on it.	Initial setup of the tenant, managing other administrators, and performing high-impact configuration changes.

User Administrator	Can create and manage all aspects of users and groups, including resetting passwords for most users.	IT support staff responsible for day-to-day user account management.
Helpdesk Administrator	Can reset passwords for non-administrators and Helpdesk Administrators.	Front-line support teams that handle password reset requests.
Security Administrator	Can manage security-related features in services like Microsoft Defender for Cloud Apps and Microsoft Entra ID Protection.	Security teams responsible for monitoring and responding to security threats.
Exchange Administrator	Full management of the Exchange Online environment, including mailboxes, transport rules, and anti-spam settings.	Email administrators who manage the organization's messaging infrastructure.
SharePoint Administrator	Full management of the SharePoint Online environment, including site collections, user profiles, and sharing settings.	Collaboration specialists who manage SharePoint sites and content.
Teams Administrator	Full management of the Microsoft Teams service, including creating and managing teams, policies, and settings.	Administrators responsible for the organization's Teams deployment and governance.
Billing Administrator	Can make purchases, manage subscriptions, manage support tickets, and monitor service health.	Finance or IT staff responsible for managing Microsoft 365 subscriptions and costs.
Intune Administrator	Manages devices using Microsoft Intune, including configuring policies, managing apps, and performing remote actions on devices.	Mobile device management (MDM) and mobile application management (MAM) administrators.

Part 2: Tracing and Auditing Sent Emails in Microsoft 365

How to Trace a User's Sent Emails in Outlook using Message Trace (Exchange Admin Center)

Message Trace is a powerful tool within the Exchange Admin Center for tracking email flow.

1. **Access the Exchange Admin Center:** Navigate to admin.exchange.microsoft.com.
2. **Go to Message Trace:** In the left-hand menu, go to **Mail flow > Message trace**.
3. **Start a Trace:**

   a. Click on **"Start a trace"**.
   b. **Senders and Recipients:** In the "Senders" field, enter the email address of the user whose sent items you want to trace. You can leave the "Recipients" field blank to see all sent emails from that user.
   c. **Time range:** Specify the time frame for your search. You can choose from predefined ranges or set a custom range.
   d. **Report type:** For detailed results, you can choose a "Summary report" for a quick overview or an "Enhanced summary" or "Extended report" for more in-depth information.
4. **Run the Trace:** Click **"Search"**. The results will show all emails sent by the specified user within the selected time frame, along with delivery status and other details.

How to Check Sent Mail Activity using Audit Logs in Microsoft Purview

The Microsoft Purview compliance portal provides audit logs that can track various user activities, including sending emails.

1. **Access Microsoft Purview:** Go to compliance.microsoft.com.
2. **Navigate to Audit:** In the left navigation pane, click on **Audit**.
3. **Configure the Search:**
   a. **Activities:** In the "Activities" field, type and select **"Sent message"** or **"Sent message using Send on Behalf"** and **"Sent message using Send As"**.
   b. **Users:** Specify the user(s) you want to investigate.
   c. **Date and time range:** Select the period you want to audit.
4. **Run the Search:** Click the **"Search"** button. The results will display a log of when the specified users sent emails, including the IP address from which the email was sent.

How to Search Sent Mail Audit Logs using PowerShell in Exchange Online

For more advanced or automated searches, you can use PowerShell.

1. **Connect to Exchange Online PowerShell:** You will first need to connect to your Exchange Online instance using PowerShell. This typically involves running `Connect-ExchangeOnline`.
2. **Run the Search-UnifiedAuditLog Cmdlet:** Use the `Search-UnifiedAuditLog` cmdlet to query the audit logs.

Example: To find all emails sent by `user@example.com` in the last 7 days:

codePowershell

```
Search-UnifiedAuditLog -StartDate (Get-Date).AddDays(-7) -EndDate (Get-Date) -UserIds "user@example.com" -
Operations "Send"
```

This command will return a detailed log of all "Send" operations performed by the specified user in the given timeframe.

Part 3: Network and UniFi Configuration

How to Block Websites and Ports Using a Wi-Fi Router

The process for blocking websites and ports can vary depending on the router's manufacturer and firmware. However, the general steps are similar.

To Block Websites:

1. **Log in to your router's admin panel:** This is usually done by entering the router's IP address (e.g., 192.168.1.1 or 192.168.0.1) into a web browser.
2. **Find the "Parental Controls," "Content Filtering," or "Website Blocking" section:** The name of this feature can differ.
3. **Add the website to block:** Enter the domain name of the website you want to block (e.g., `example.com`). Some routers also allow blocking based on keywords.
4. **Apply the settings:** Save your changes. The router will now prevent devices on your network from accessing the specified websites.

To Block Ports:

1. **Log in to your router's admin panel.**
2. **Locate the "Firewall," "Port Filtering," or "Access Control" settings.**
3. **Create a new rule:** You will typically need to specify the following:
    a. **Source IP Address:** You can often leave this as "Any" to block the port for all devices.
    b. **Destination IP Address:** Leave as "Any" to block the port for all destinations.
    c. **Protocol:** Choose TCP, UDP, or Both.
    d. **Port Range:** Enter the port number you want to block.
    e. **Action:** Select "Block" or "Deny."
4. **Save and apply the rule.**

How to Find the UniFi OS Admin Password

If you have forgotten your UniFi OS admin password, the method for recovery depends on your setup.

- **Check your Ubiquiti Account:** If your UniFi OS console is linked to your Ubiquiti account, you can often reset the password through the Ubiquiti SSO portal (account.ui.com).
- **Physical Reset:** If you cannot access your account, you will likely need to perform a physical factory reset of the UniFi Console (e.g., UniFi Dream Machine, Cloud Key). This will erase all configurations and require you to set up the device again from scratch. The reset button is

usually a small, recessed button that you'll need a paperclip to press and hold for about 10 seconds until the device indicates it is resetting.

How to Allow UDP 5060 in a Router and UniFi OS

UDP port 5060 is commonly used for the Session Initiation Protocol (SIP), which is essential for many VoIP (Voice over IP) phone systems.

On a Standard Wi-Fi Router:

1. **Log in to your router's admin panel.**
2. **Find the "Port Forwarding" or "Virtual Server" section.**
3. **Create a new port forwarding rule:**
    a. **Service Name/Description:** Enter a name for the rule (e.g., "SIP" or "VoIP").
    b. **Port Range:** Enter `5060` for both the start and end port.
    c. **Protocol:** Select **UDP**.
    d. **Local IP/Server IP Address:** Enter the internal IP address of the device that needs to receive the traffic (e.g., your VoIP phone or PBX server).
4. **Save and apply the rule.**

On UniFi OS:

1. **Open the UniFi Network application.**
2. **Navigate to Settings:** Click on the gear icon in the left menu.
3. **Go to Firewall & Security** (or **Routing & Firewall** in older versions).
4. **Create a New Port Forwarding Rule:**
    a. Under the "Port Forwarding" section, click **"Create New Rule"**.
    b. **Name:** Give the rule a descriptive name (e.g., "Allow SIP UDP").
    c. **Enable:** Make sure the rule is enabled.
    d. **From:** Select **"Any"** to allow traffic from any external IP address.
    e. **Port:** Enter `5060`.
    f. **Forward IP:** Enter the IP address of the device on your local network that should receive the SIP traffic.
    g. **Forward Port:** Enter `5060`.
    h. **Protocol:** Select **UDP**.
5. **Apply Changes:** Click **"Apply Changes"** to save and activate the rule.