

# Exchange Server Auditing

How to enable logging of important Exchange Server changes

## Exchange Server Audit Settings

- Open the **Exchange Management Shell**, and run the following cmdlets:
  - `Set-AdminAuditLogConfig -AdminAuditLogEnabled $true`
  - `Set-AdminAuditLogConfig -AdminAuditLogCmdlets *`
  - `Set-AdminAuditLogConfig -AdminAuditLogParameters *`
  - `Set-AdminAuditLogConfig -LogLevel Verbose (for Exchange 2013)`

## Audit Log View in Exchange 2010

- Open the **Exchange Control Panel** in your browser > navigate to "Roles & Auditing" > Auditing (Tab):
  - *Run an administrator role group report*
  - *Export the Administrator Audit Log*
- Specify the date range. Search for cmdlets listed in "Common Cmdlets" box

## Audit Log View in Exchange 2013

- Open the **Exchange Admin Center** in your browser > Compliance Management > Auditing > click "View the administrator audit log"
- Specify the date range. Search for cmdlets listed in "Common Cmdlets" box

## MSExchange Management Log

- Run **eventvwr.msc** > Applications and Services Logs > MSExchange Management > search for cmdlets listed in "Common Cmdlets" box

## Audit Log Search via Exchange Management Shell

- Open the **Exchange Management Shell**
- Run the following cmdlets in order to search Admin audit log:
  - `Search-AdminAuditLog`
  - `New-AdminAuditLogSearch`
- You can specify search date by adding "`-Parameters -StartDate MM/DD/YYYY -EndDate MM/DD/YYYY`"
- You can also specify cmdlets and parameters. Run "`get-help Search-AdminAuditLog`" for more information

## For Detailed Exchange Server Auditing, Try Netwrix Auditor - [netwrix.com/go/trial-es](http://netwrix.com/go/trial-es)

- **Change auditing:** detection, reporting and alerting on all configuration changes across your entire IT infrastructure with Who, What, When, Where details and Before/After values.
- **Predefined reports and dashboards** with filtering, grouping, sorting, export (PDF, XLS etc.), email subscriptions, drill-down, access via web, granular permissions and ability to create custom reports.
- **AuditArchive™:** scalable two-tiered storage (file-based + SQL database) holding consolidated audit data for 10 years or more.
- **Unified platform** to audit the entire IT infrastructure, unlike other vendors with a set of hard-to-integrate standalone tools

## Common Cmdlets:

- **Enable-Mailbox** - creates a mailbox for an existing AD user
- **Disable-Mailbox** - Removes user's mailbox
- **Set-Mailbox** - modifies the settings of an existing mailbox
- **New-MailboxDatabase** - creates a new mailbox database
- **Mount(Dismount)-Database** - Mounts(dismounts) an existing mailbox database
- **Set-MailboxDatabase** - configures a variety of properties for a mailbox database
- **New-SendConnector** - creates a new Send connector
- **New-ReceiveConnector** - creates a new Receive connector
- **Add(Remove)-MailboxPermission** - adds (removes) permissions to a mailbox
- You can find full list of cmdlets here- <http://url2open.com/cmdlets>

**netwrix**  
#1 for change auditing

Try Exchange Server  
Auditing For Free:  
[netwrix.com/go/trial-es](http://netwrix.com/go/trial-es)