Disabling Active Directory Users with PowerShell (Generalized)

A guide to efficiently disabling user accounts in specific Organizational Units (OUs) using PowerShell.

Introduction

This document provides a step-by-step guide on how to disable Active Directory (AD) user accounts located within specific Organizational Units (OUs) using PowerShell. This method is non-destructive, meaning the accounts are disabled and not deleted, allowing for easy re-enablement if needed.

We will focus on disabling all users within a 'YourTopLevelOU' and a 'YourNestedOU', assuming 'YourNestedOU' is nested under 'YourParentOU' and 'YourTopLevelOU' is a top-level OU directly under your domain (e.g., 'contoso.com').

{{info}} **Prerequisites:** Ensure you are running PowerShell with administrative privileges on a Domain Controller or a machine with the Remote Server Administration Tools (RSAT) for Active Directory installed. {{/info}}

1. Understanding Distinguished Names (DNs)

To target specific OUs, you need their precise Distinguished Name (DN). The DN is a unique identifier that specifies the exact location of an object within the Active Directory hierarchy.

- **Your Domain:** `yourdomain.com` (e.g., `contoso.com`) (translates to `DC=yourdomain,DC=com` or `DC=contoso,DC=com`)
- **YourTopLevelOU:** This OU is directly under your domain. DN: `OU=YourTopLevelOU,DC=yourdomain,DC=com`
- **YourParentOU:** This OU is also directly under your domain. DN: `OU=YourParentOU,DC=yourdomain,DC=com`
- **YourNestedOU:** This OU is nested inside the 'YourParentOU'. DN: `OU=YourNestedOU,OU=YourParentOU,DC=yourdomain,DC=com`

> **Tip: Verifying DNs:** To get the exact DN for any object in Active Directory Users and Computers (ADUC), enable "Advanced Features" under the "View" menu. Then, right-click the object, go to "Properties," click the "Attribute Editor" tab, and find the `distinguishedName` attribute. Copy its value directly.

2. The PowerShell Cmdlet: `Disable-ADAccount`

The primary PowerShell cmdlet used for this operation is `Disable-ADAccount`. We will combine this with `Get-ADUser` to retrieve the target users.

- `Get-ADUser -Filter *`: Retrieves all user objects.
- `-SearchBase "Your_OU_DN"`: Specifies the starting point for the search.
- `-SearchScope Subtree`: Crucially, this ensures that not only users directly in the specified OU are found, but also users in any sub-OUs or containers beneath it.
- `| Disable-ADAccount`: The pipeline operator sends the retrieved user objects to the `Disable-ADAccount` cmdlet, which performs the disabling action.

3. Disabling Users in 'YourTopLevelOU'

To disable all user accounts within 'YourTopLevelOU' Organizational Unit, including any users in its sub-OUs, use the following command. Remember to replace `YourTopLevelOU`, `yourdomain`, and `com` with your actual OU and domain names.

PowerShell Command:

```
Get-ADUser -Filter * -SearchBase "OU=YourTopLevelOU,DC=yourdomain,DC=com" -
SearchScope Subtree | Disable-ADAccount
```

> **Important:** This command will disable ALL user accounts found within the specified OU and any OUs nested inside it. Confirm your `SearchBase` is correct before execution.

4. Disabling Users in 'YourNestedOU'

To disable all user accounts within 'YourNestedOU' Organizational Unit, including any users in its sub-OUs (assuming 'YourNestedOU' is nested under 'YourParentOU'), use this command. Remember to replace `YourNestedOU`, `YourParentOU`, `yourdomain`, and `com` with your actual OU and domain names.

PowerShell Command:

```
Get-ADUser -Filter * -SearchBase
"OU=YourNestedOU,OU=YourParentOU,DC=yourdomain,DC=com" -SearchScope Subtree |
Disable-ADAccount
```

> **Important:** This command will disable ALL user accounts found within the specified OU and any OUs nested inside it. Double-check the `SearchBase` for accuracy.

5. Verification (Optional but Recommended)

Before running the `Disable-ADAccount` part, you can test the `Get-ADUser` portion to see which users will be affected. Remove the `| Disable-ADAccount` part to just list the users:

PowerShell Command:

```
Get-ADUser -Filter * -SearchBase "OU=YourTopLevelOU,DC=yourdomain,DC=com" -
SearchScope Subtree | Select-Object Name, DistinguishedName, Enabled
Get-ADUser -Filter * -SearchBase
"OU=YourNestedOU,OU=YourParentOU,DC=yourdomain,DC=com" -SearchScope Subtree |
Select-Object Name, DistinguishedName, Enabled
```

After running the `Disable-ADAccount` commands, you can run the verification commands again to confirm that the `Enabled` status for the affected users has changed to `False`.

> **Conclusion**
>
> By following these steps, you can efficiently disable user accounts in specific Active Directory Organizational Units using PowerShell. This approach provides a quick and non-destructive way to manage user access.

Revision #14
Created 2025-07-12 17:35:26 UTC by joliveira
Updated 2025-07-12 18:35:25 UTC by joliveira