Leaving User Process

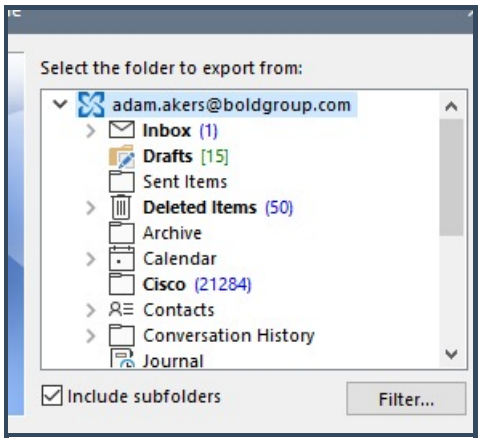
01/05/2024 6:15 pm EST

Recover Bold Property

1. Recover any property belonging to Bold Group
    a. Vertx badge
    b. Data center badge
    c. Cell phone
    d. Laptop
    e. IP Phone
2. Return badge to Data Center if applicable. If badge not recovered, call DataCenter immediately.

Export PST and Store on HDD

1. Log in to user's computer and open Outlook.
2. click File > Open and Export > Import/Export > Export to a file > Outlook Data File (.pst) > Select the user's account



3. click Next
4. Allow Duplicate Items to be created > Finish
5. Once export is finished, save to two separate external hard drives.

Reset Users Password and put in LastPass

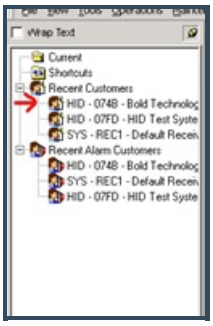
1. Generate a secure password and create a note in LastPass with password
2. Remote in to the Domain Controller
3. boldgroup.com > Bold Users > End Users > Highlight user and right click > Reset Password...
4. Use the password generated

Revoke/Re-Register MFA

1. log in to the Office365 Admin portal
2. Admin Centers > Azure Active Directory > Users > Search for the user in the search bar and click their name > Authentication Methods > Click "Revoke MFA sessions" and then "Require re-register MFA"
3. Go back to Users
4. At the top, Select Multi-Factor Authentication
5. Search for User
6. On the right, under "quick steps", click Disable then again press Enable.
7. MAKE SURE MFA IS ENABLED AFTER

Remove from HD-Vertex (Badge entry system)

1. Retrieve badge from departing user
2. Open RDP and enter 172.16.143.47 and enter password
    a. In Windows, open RDP and remote into 172.16.143.47
    b. Open Manitou Workstation and login
    c. Select “HID – 074B – Bold Technologies” in the left-hand pane

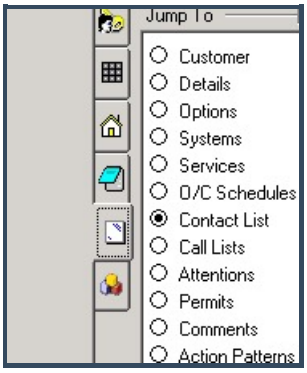


d. In the right-hand pane, select “Contact List”

e. Click “Edit” toward the top of Manitou Workstation

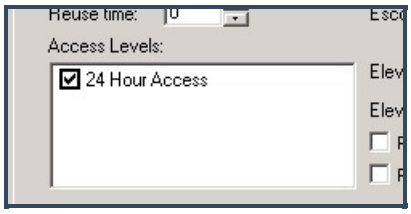
f. Click “OK” on the popup

g. Click the white card labeled “Access Cards”



h. Select the leaving user

i. Uncheck “24 Hour Access”



3. Click Save

Remove from Sonicwall

1. Disable "Sonicwall VPN" user access immediately at time of dismissal.

   a. Open Google Chrome

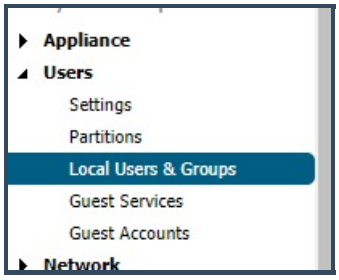
b. Enter IP addresses. Do for both Main office and

   i. 172.16.140.1 – Main Office SonicWall

   ii. 192.30.133.196 – Data Center SonicWall

      i. On the top navigation pane, select, “MANAGE”

      ii. On the left-hand navigation pane select “Local Users & Groups”



      iii. Select User, make sure their checkbox is checked

      iv. Click “Delete”

         i. DO NOT DELETE ALL

Microsoft Local Domain

Microsoft Cloud Domain

1. IF THE USER IS HIGH-LEVEL (VP, TEAM LEAD OR PM), DO NOT REMOVE OFFICE 365 LICENSE or DYNAMICS

   a. You can remove CodeTwoSignature

2. In O365 cloud, go to Admin portal >

   a. Remove from any cloud only based groups. (Azure Active Directory/ Office Admin Portal)

      i. Be sure to remove “CodeTwoSignature”

   b. Remove any product licenses (O365, Dynamics, etc…)

   c. In user Groups, be sure to remove Code Two Signature”

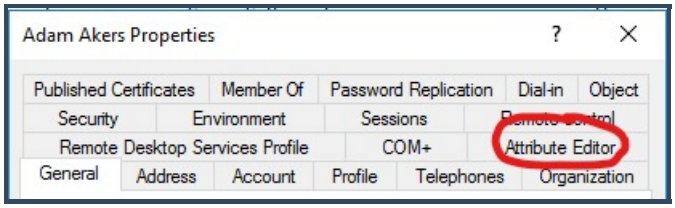
   d. Forward email to users supervisor

i. Note: The current "SMTP" account must be removed from the disabled user account and added to the managers account. The description should be modified from the disabled account to point to the employee that will continue to receive new emails for the disabled account.

ii. Log into DOM-05 domain controller and open Active Directory

   i. Select the managers account that emails will be forwarded to, right click and select Properties

   ii. Click Attribute Editor



   iii. Scroll down to the ProxyAddresses field, highlight and click Edit

   iv. In the "Value to add:" field, enter "smtp:<leaving users email address>"

   v. Click, OK, then Save

   vi. Highlight the leaving user (May now be in the "Disabled" folder instead of "End Users")

   vii. Right click and select Properties

   viii. Click Attribute Editor

   ix. Scroll down to ProxyAddresses

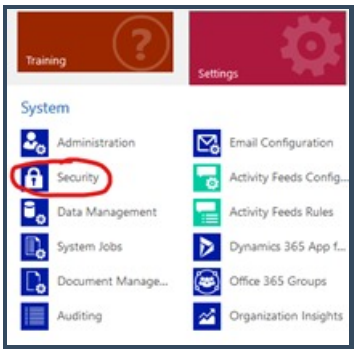
   x. remove the email address with the SMTP in all caps and save

e. Remove Roles and Permissions from CRM

   i. Go to the Dynamics 365 page in the portal

   ii. Click the down arrow next to Service, and click the right arrow to show more options

   iii. Go Settings > Security



iv. Click Users

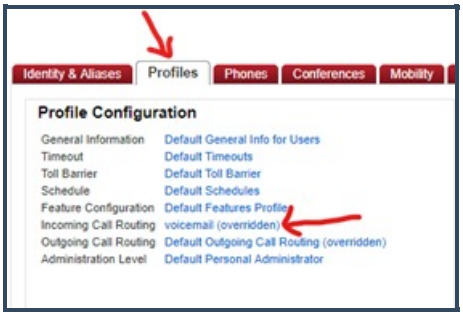
v. Find and select user

vi. On user's page, click Manage Roles on the bar toward the top

vii. Uncheck all Roles

Aeonix Phone System

1. Forward Users phone calls to supervisor
    a. Log in to the Aeonix Admin portal
        i.
    b. Go to Users > User List then click the users extension
    c. Click Profiles > voicemail



    d. Check "Forward all" and set to users supervisor. This will forward all phone calls

2. Change Users Aeonix Password

a. Go to Users > User List

b. On the right side of the Users List, the last column will be the “Change Password” button, click that.

3. Physically remove IP phone from internet by removing RJ-45
    a. Place in IT storage room with other phones and power bricks

Remove from BoldTalk

1. Login to http://lists.boldgroup.com/mailman/admindb/boldtalk_lists.boldgroup.com using admin credentials

Remove user from Security System

1. Open up the [Insert file name and location here] and find the user that is leaving
    a. Take note of their user number and add a “0” in the front.

    b. User “51” Should now be “051” and user “4” should be “004”

2. Go to the main security panel, located by the stairs heading down to support
    a. This is the only panel that can manage the system

3. To remove the user, type in the code:
    a. 3396 8 [3-digit user code] 3396

    b. 1 (to confirm deleted position)

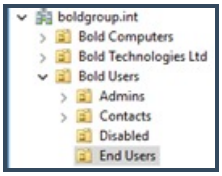
    c. Ex: 3396 8 004 3396
        i. 1 to confirm

Disable User in Active Directory

1. IF THE USER IS HIGH-LEVEL (VP, TEAM LEAD OR PM), DO NOT DISABLE USER AND REMOVE LICENSES.
    a. Instead, reset their user password
        i. Login to DOM-05

ii. Open Active Directory

iii. Go to boldgroup.com > Bold Users > End Users



iv. Right click user and click, Reset Password…

i. Store their password somewhere accessible for future reference

v. In Powershell, run the command

i. In the running PowerShell window, tap the up arrow on the keyboard.

ii. If PowerShell is not running, open and type in command

i. Start-ADSyncSyncCycle

2. If user is not VIP:

a. In the Local Domain

i. Remote into DOM-5 domain Controller (use mRemote)

i. Enter Active Directory Users and Computers.

i. Go to Bold Users > End Users

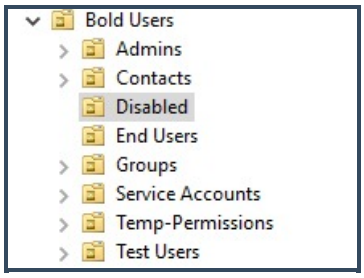
i. Select the leaving user and set the main group to the "Removal" group. Take membership out of every other group.

i. Right click user > Properties > Member Of >

ii. Remove all groups and add No Access

ii. Right click user and “Disable Account”

iii. Make sure user is in “Disabled” folder



3. In Powershell, run the command:
    a. Start-ADSyncSyncCycle
    b. You may just be able to press the up arrow in the PowerShell