Active Directory Self-Service

FAQ

General Information: info@cionsystems.com
Online Support: support@cionsystems.com

CionSystems Inc.
Mailing Address:
16625 Redmond Way,
Ste M106
Redmond, WA. 98052
http://www.CionSystems.com
Phone: +1.425.605.5235

Table of Contents

General Information

Q: How do I configure Active Directory Self-Service?

A: Before using Active Directory Self-Service administrator must configure the application. There is a 4 step configuration to Self-Service deployment.

1. Configure the application to talk to an Active Directory domain in the back end. You do this by login to the Self-Service application via "administrator page" by providing username – 'admin' (without quotes) and password 'admin' (without quotes). With first time install and configuration, you will see an option to configure "local domain". Please provide "high privilege" active directory account, preferably an account with administrative privileges. Configure the domain and the domain-controllers, mark the primary domain controller.
2. Once the Self-Service successfully connects to active directory domain you will see "dashboard" which provides insight into active directory users and Self-Service state. From here you can configure the optional Microsoft BPOS cloud by clicking on "Domain Setting option". Note: configure for cloud only if you are using Microsoft BPOS. Provide admin user name and password for the cloud. You will see a message indicating that the cloud is successfully added. In case of error, please check 'connectivity to the cloud" and credentials to ensure they are correct. The admin username typically will be in the form of name@companyname.microsoftonline.com.
3. Now you are ready to configure self-update settings, password and account unlock policy and security questions. Please refer to help file for helping configure these options.
4. Send email to user community to enroll with Self-Service. You can do this by clicking on "User Enrollment Settings" and "Enrollment". Fill out the invitation and send to the user community.

Q: How do I configure the application to use HTTPS?

A: You can configure Self-Service to use HTTPS by configuring the application in IIS for https protocol. The default install is for http. Before using https, you need to obtain a proper certificate. Refer to "ADS_SSL installation procedure.doc" document

Q: How do I allow remote users to connect the application?

A: You can expose the Self-Service URL to remote users by nat'ing the http/https traffic and redirecting it to the URL. First configure the URL and map it to a DNS

name. Then configure the NAT box to redirect the http/https traffic to Self-Service URL. You can also configure the URL and map it to a publicly accessible IP address. Our recommendation is to use https to connect to Self-Service URL from outside the firewall.

Q: What is the default administrator user name and password?

A: The Default credentials of the application are:

Username: admin
Password: admin

Q: How do I ensure that the users don't see "admin" tab on their home page?

A: Ask user community to connect to
http://localhost/ActiveDirectorySelfService/frmUserLogin.aspx

Q:How do I connect to "administrator" home page?

A: The administrator home page is
http://localhost/ActiveDirectorySelfService/frmLogin.aspx

Q: How do I configure self update settings?

A: Login to Self-Service via admin page and click on the option "User Policy Settings". There are two level of access that you can grant to the user community. Option "Self-update settings for CionGroup" is for users that with additional privileges than the regular users. For example, if you want to restrict "certain" attributes of user profile and only want this select group to be able to modify than you would configure those attribute using this option. Another example is user profile has attribute A, B and C. You want all users to view attribute A and B only but you want this special group to view and modify A, B and C attributes. Follow the following steps

- Create a "CionGroup" security group in your domain and make all users members of this security group that requires additional privileges
- Configure the 'Self-update settings for CionGroup' option by selecting attributes for Ciongroup
- Click on the 'Save' button
- Click on "Self-update" settings and select and unselect the attributes for the general user community
- Click on the 'Save' button

Q: How do I change the number of password retries?

A: Administrators can control how many incorrect retries they would like to permit before the application locks the user account. This is done to ensure no user will continuously retry and hack passwords. To configure

- Login via admin page
- Click on User Enroll Settings
- Click on Secret questions option
- Click on Maximum number of times a user can reset his password per day and enter the new retry count.
- Click on save button

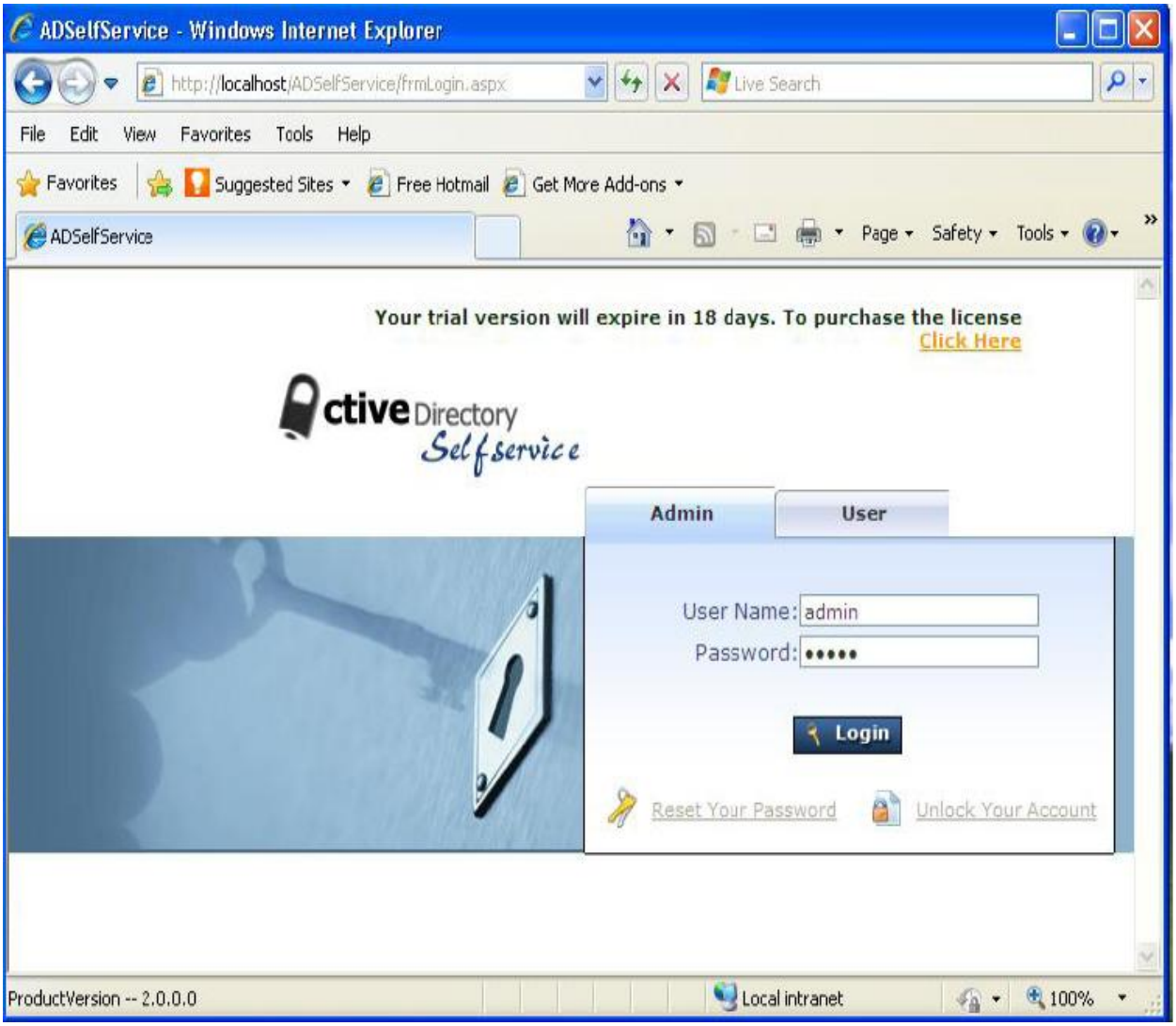
Q: How do I configure domains?

A: You can configure one or more active directory domains. To *Configure a Domain*

- Click on Start Button>All Programs> AD Self Service> AD Self Service icon.

  OR

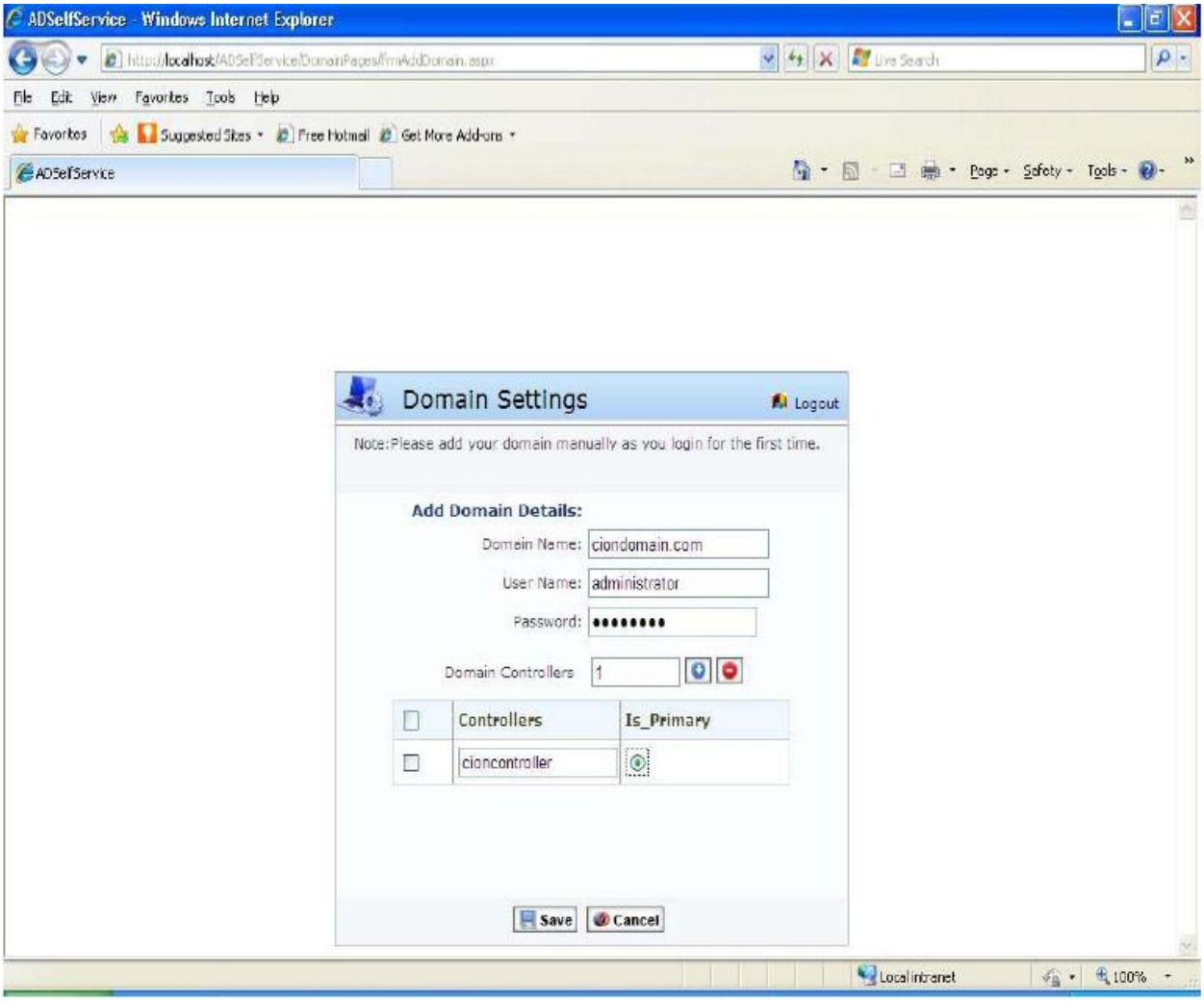
- Click AD Self Service Icon on desktop and follow the below procedure.



The login screen will open in the default web browser. When logging to the application for the first time

- Enter "admin" in the User Name dialogue box.
- Enter "admin" in the Password dialogue box.

Note: It is recommended that the user name and password should be changed after the application has launched.



3. Enter the Active Directory Self Service details of the domain.

    - Domain Name.
    - Domain User Name.
    - Domain Password.
    - Enter All Domain Controllers
        - Select Primary radio button.
        - Click on Save button

Q: Can I use multiple domains? How do I add a second domain?

A: CionSystems Self-Service application supports multiple domains.

- Login to the application via admin page
- Click on "domain settings" to add or modify the domain information.

Note: If you modify an existing backend user name and password for a domain than you must restart IIS service.

To restart IIS service,

- click on start,
- click on run
- type iisreset command.

Q: How do I configure Microsoft BPOS cloud?

A: CionSystems Self-Service provides a Self Service feature for Microsoft BPOS cloud. It allows the user community to reset and unlock accounts on BPOS | Office 365 cloud. Additionally, it provides password synchronization between on premise domain and BPOS cloud when the password is changed through Self-Service application. Self-Service application automatically recognizes users with Microsoft BPOS account before allowing password change and password resets. Follow following steps to configure BPOS cloud

- Login to the application via admin page
- Click on "domain settings" to add and or modify the cloud information.

Q: We are not signed up for BPOS cloud? Can we still use Self-Service application?

A: Yes, BPOS is optional.

Q: How do I ask a group of people to register with the application?

A: As an administrator you can send an enrollment invitation to the user community. To send an invitation email

- Log into Self-Service via admin page
- Click on "User Enrollment Settings"
- Click on "Enrollment"
- Fill out the invitation form and send it to the user community.

You can monitor the registration by clicking on Unenroll option. Note: Self-Service application encrypts the user security challenge answers before storing into the repository. Should any registered user forget their security challenge answers the 'administrator" must un-enroll them and ask the user to re-register with the application.

Q: How does the registration process works?

A: Users are required to login using their domain credentials by clicking on the 'User tab'on the Self-Service home page. Once Self-Service verifies their domain credentials a popup message box will appear asking them to register. They must click "Ok" to register. The administrator's configured security questions will then appear and the user must provide the answers to these questions to be able to reset their passwords.

Q: How does "account unlock" option work?

A: It works similar to password reset. The user is asked to provide answers to the security questions before their account is unlocked.

Q: What happens if certain user doesn't register?

A: Only registered users will be able to reset their password and unlock their accounts.

Q: How do I find out which users are registered with the application?

A: From admin page

- Click on "User Enrollment Settings"
- Select the Unenroll option to see a list of all enrolled users

Administrator

Q: How do I hide and disable the "password reset" option?

A: The administrator can disable the password reset option for all users by login via admin page.

- Go to the user policy settings tab
- Click on "Reset password settings" option
- Uncheck the checked box (i.e. Allow Reset Password)
- Click on the Save button

Q: How do I hide and disable "account unlock" option?

A: The administrator can disable the Unlock Account Settings option for all users by login via admin page.

- Go to the user policy settings tab
- Click on "Unlock Account Settings" option
- Uncheck the checked box (i.e. Allow Unlock Account)
- Click on the Save button.

Q: How do I modify the "Active Directory" user name that I am using for backend active directory connection and password?

A: You can modify the backend active directory user name and password by logging into the admin page, and through domain settings option. After modification please click on the Save button. Close AD Self-Service and restart IIS service by going to start, run and IISRESET to ensure Self-Service uses the new credential for the backend connection.

Q: What are "self-update" settings?

A: Administrators can control what attributes the user community is able to view and modify via Self-Service. Users will be able to see and modify only "selected" attributes from the self-update option.

Q: I see two links for "self-update". What is their purpose?

A: One is for normal or less privileged users who can modify a limited set of attributes. The other setting is for users who are member of the "CionGroup"

security group. The administrator can choose to give more privileges to this group so that only select few can modify certain attributes.

Q: How do I configure the self update settings so that users have access to certain attributes only?

A: From admin page, go to the User Policy Settings tab select "Self Update Settings". Here you can select and unselect the attributes check boxes. User community can view and modify only the selected attributes. Make sure to click on Save to button o save any changes.

Q: How do I give more privileges to managers?

A: Managers will be able to see profiles for all direct reports and can make modifications to their direct report profiles. Giving additional privileges to managers (make them a member of ciongroup) will allow managers to manage attributes that you do not want users to modify.

Q: What is "CionGroup"? Who should be a member of "CionGroup"?

A: This is a security group created by administrator in the active directory domain. Any user who administrator wants to give ability to modify attributes that regular users are not allowed to view and modify.

Q: How can I change the "default" admin password?

A: You can change the application administrator password by

- Login to admin page
- Click on General Settings tab
- Click on "Change Password" option
- Enter the New Password and Old password
    - Choose to use same password for the BPOS cloud
- Click on the Save button.

Q: How do I use my company's logo on the application?

A: You can customize Self-Service and add your company's logo.

- Log into Self-Service via admin page
- Go to General Settings tab
- Click on "Customization" option
- Click Browse, select your company logo
- Click on the Save button

Q: How do I configure "Server Settings" in the admin page under 'General Settings'? What is the purpose of it?

A: These setting are used for sending notification emails like registration notifications. Enter the IP address or Exchange server and email address.

Q: How do I configure "Outlook Server Settings"? What is the purpose of it?

A: From the admin page, General settings, and outlook server settings option you can configure the incoming and outgoing outlook mail server settings.

Q: How do I configure the notification schedule to receive "Locked out users" report at schedule date and time?

A: This is a very powerful Self-Service feature by which you can proactively notify users of their password expiry and mailbox storage limits. In addition, administrator has an option to receive a daily 'locked out users' report in email. To receive "Locked out users" report in email at schedule time

- Login to application via admin page
- Go to the Schedule Policy Settings tab
- Click on "create schedule" option
- Enter the schedule name of your choice
- Select the OU's of your choice
- Select "Locked out users" from the reports dropdown list
- Set the schedule frequency daily, weekly or monthly
- Select the time
- Select the "enable" radio button
- Click on the Save button

You can view the newly created notification schedule via "View Schedule" option.

Q: How do I configure to notify the user community of "mailbox storage" limit?

A: Self-Service has a powerful feature by which you can proactively notify users of their password expiry and mailbox storage limits. In addition, administrator can receive a daily report of all locked users for proactive actions. To notify users whose have hit "mailbox storage" threshold in email

- Login to application via admin page
- Go to the Schedule Policy Settings tab
- Click on "create schedule" option
- Enter the schedule name of your choice
- Select the OU's of your choice
- Select "Mailbox storage" from the reports dropdown list

- Set the schedule frequency daily, weekly or monthly
- Select the time
- Select the "enable" radio button
- Click on the Save button

Q: How do I configure to notify the user community of their near future "password expiry"?

Self-Service has a powerful feature by which you can proactively notify users when their passwords are about to expire. To notify users proactively of password expiry

- Login to application via admin page
- Go to the Schedule Policy Settings tab
- Click on "create schedule" option
- Enter the schedule name of your choice
- Select the OU's of your choice
- Select "Password expiry" from the reports dropdown list
- Set the schedule frequency daily, weekly or monthly
- Select the time
- Select the "enable" radio button
- Click on the Save button

Q: What happens if the user forgets the security "answers"?

A: In this situation administrator must un-enroll the user and inform the user to re-enroll again.

Q: How do I Un-enroll users?

A: Through the admin page

- Go to the User Enroll Settings tab
- Click on Un-enroll option
- Select the domain
- Click on search
- From the enrolled users list, select the checkbox next to the user
- Click on the Un-enroll Button.

Q: How do I setup security question? Can I create my own security questions?

A: Yes, you can create your own security questions. To setup security questions

- Login via admin page
- Go to the User Enroll settings tab

- Select secret questions option and enter the values for the first and second textbox
- Click on the Save button

From this page, you can control all the security settings for self-service including security questions.

Q: A user is getting "you can't reset the password"? What does it mean?

A: The user most likely has exceeded the password reset limit for the day. You can increase the number of retries by changing to higher number in the field "Maximum number of times a user can reset his password per day" in secret questions option in User Enroll Settings tab of the application.

Q: A user is getting "your account is blocked"? What does it mean?

A: The user is most likely blocked because they have provided incorrect security challenges more than the number of times they are allowed. Administrator can increase this count through "Reset Your Password count" by logging in via admin page.

Q: What is the "Maximum number of password synchronization retries" and what does it do?

A: This setting take into effect only if you have configured Self-Service for Microsoft BPOS also. Self-service automatically synchronizes passwords from local domain to BPOS cloud. It synchronizes only those passwords that are changed via self-service. This setting indicates to the service that the number of times it must try to synchronize with the BPOS cloud before giving up.

Q: How do I generate auditing reports?

A: Any modification made by the user and or manager for his account, group, organizational unit, contacts, exchange, passwords and account unlock are tracked in audit logs. Self service application tracks the machine_name/IP address that effected the change along with date, time and results. Administrators can generate the following audit reports:

1) Enrolled users
2) Un-enrolled users
3) Reset password audit report
4) Unlock audit report
5) User update audit report
6) Group update audit report
7) OU update audit report

8) Contact update audit report
9) Password synchronization report.

Q: I see two "password" reports? What is the difference between them?

A: Reset Password Audit Report provides results of successful password resets.

Password synchronization report provides a status of passwords that are under synchronization or have failed to synchronize.

Users

Q: How does a user log in to the Self-Service application?

A: A user can login to the Self-Service application by following the below steps

- Click on Internet Explore
- Type the administrator provided URL for Self-Service Application
- Select the "User" tab. **Note:** On this form the user will enter a valid domain user name and password. The user may have to choose a domain from the drop down list if Self-Service is configured for multiple domains.
- Click on "Login" button.

After the validation of credentials the user should see their profile settings.

Q: User is unable to perform "manager based searches". What could be wrong? How do I configure to get the results?

A: Only a manager can perform "Manager based Search". To perform "manager based searches", login with credentials of a user that has direct reports configured in active directory.

Q: If the user is unable to perform "permission based searches". What could be wrong?

A: To perform "Permission based searches" first you need to have the right permissions in the active directory for the objects you are intending to search for. Assuming that you have the right permissions follow the below procedure

- Login to the application using the user credentials
- Click on "Permission Based Search" tab
- Select "User" from the dropdown list of object class
- Select an attribute from the dropdown list and specify the value of that attribute in the textbox

- Click on "Search" button as shown in the below figure

If the user has appropriate permissions then the user details should appear and the logged in user will be able to change those attribute.

Q: How do users change their passwords?

A: User have to login to the application using their domain user credentials and follow the below steps

- Click on "Change Password" tab
- Provide the details of the "OLD Password", "NEW Password" and "Confirm New Password" fields
- Click on the "Save" button

If your user account has an account on BPOS than the option to change the password for BPOS will appear.

Q: Users can't see some of the settings in their profile when they login to Self-Service application. What could be wrong?

A: Most likely the administrator has removed access to these attributes for Self-Service.

Q: What if the user sees no attributes in the "exchange" tab, what could be wrong?

A: This may happen in two cases

i) The user account does not have an on Email account.

OR

ii) The administrator of Self-Service has not given the permission to the user to view and modify Exchange attributes.

Q: When a user tries to update settings, they receive "access denied error", what could be wrong?

A: The most likely reason is the backend connection to active directory doesn't have sufficient privileges to affect the change. Administrators must ensure the Self-Service application is configured to connect to the domain with a domain administrative level account.

Q: How can users configure their outlook via "outlook configurations" tab?

A: By following the below procedure

- Login to the application as a user using domain credentials
- Click on "Outlook configuration" tab
- From the list select an application to match the outlook version installed in your machine
- Click on "Run" button
- A dialogue box will appear, click on "Yes" button

This will configure your system to use the right outlook settings for email access.

Q: I don't see any settings in the Windows mobile tab, what could be wrong?

A: There can be several reasons for this. One of them is that the exchange server is not configured for Windows mobile or your account may not have mobile privileges or you may need to synchronize your mobile with the domain user for the settings to show up correctly.

Q: I have lost my phone, what can I do to delete data on the lost phone?

A: Self-Service provides a powerful feature to remotely delete data from lost or stolen phones.

- Login to Self-Service as a user
- Select "Windows mobile wipe" tab
- Select your mobile device
- Select "Remote wipe to clear mobile data" radio button and click on "Apply" button
- It will clear the data in your mobile device.
- Now select your mobile device,
- Select "Remove mobile device partnership" radio button to unregister your mobile device.

Q: How do I unregister my windows mobile phone?

A: In case of user mobile phone change, user can unregister the old phones themselves without calling the IT helpdesk by following the below procedure.

- Login to self-service as a user
- Select "Windows mobile wipe" tab
- Select your mobile device
- Select "Remove mobile device partnership" radio button to unregister your mobile from the application.

Q: How do I manage my group membership?

A: Self-Service also allows users to manage distribution groups, security groups, OUs, contacts and mobile devices without having to call the Helpdesk. To manage groups/OUs, click on the group which appears on left hand side to manage the membership.

Q: How do I manage my contacts?

Answer: To manage your Contact, login to the Self-Service with your domain username and password, click on "Manager based search" tab, click on the Contact which appears on the left hand side to manage.

Q: How do I perform "permission' based searches?

A: To perform "Permission based searches" first you need to have the right permissions for the objects that you want to search for in the active directory. These permissions are typically assigned to you by the administrator.

- Login to the Self-Service through a user account that has permission to access properties of another user or object.
- Click on the "Permission based Search" tab
- Select "User" from the dropdown list of object class
- Select an attribute from the dropdown list and specify the value of that attribute in the textbox
- Click on "Search" button.

Manager

Q: How does a manager login?

A: A manager logs in just like a normal user using his/her domain credentials.

Q: I see the same attributes as users but not the additional attributes the administrator has given permissions to? What could be wrong?

A: Most likely the manager is not a member of "CionGroup". If the manager is not a member of CionGroup then the manager will see same attributes as the user. However, a manager can use the "manager based search" functionality and he/she can change the attributes of their direct reports.

Q: How do I change my direct reports attributes?

A: Login to Self-Service application using your domain credentials. Click on manager based search and this should populate a tree structure on the left side with names and profile of all direct reports. Lastly, select the direct report to modify the attribute and then click on the Save button.

Q How do I manage my direct reports groups?

A: Login to Self-Service application using domain user credentials. Click on manager based search, this should populate a tree structure on the left side with names and a profile of all the groups that the logged in user have ownership.

Q: Can a manager change my direct reports password?

A: No, a manager will not be able change their direct reports password.

Q: How do I manage my security group membership?

A: Groups are two types of groups.

i) Security group.
ii) Distribution group.

To manage your Security group membership, login to the application with your username and password, then click on "Manager based search" tab, click a group on the left hand side, add or remove members to your Security Group.

Q: How do I manage my distribution list membership?

A: To manage your Distribution group membership, login to the application with your username and password, click on "Manager based search" tab, click on the listed security groups on the left hand side to add or remove members to the distribution group.

