# Table of Contents

Preface .............................................................................................................................................. 4  
   Introduction .................................................................................................................................. 4  
   Important Features ....................................................................................................................... 5  
Logging into the AIM System .......................................................................................................... 6  
Window Enlargement ....................................................................................................................... 7  
The Identity Self-Service Tab .......................................................................................................... 8  
Changing Your Password ............................................................................................................... 9  
The Work Dashboard Tab .............................................................................................................. 10  
Approving a New Provisioning Request (On-Boarding) ............................................................... 12  
Provisioning a New Non-Employee (Contractor) ........................................................................ 19  
Extending a Non-Employee CID .................................................................................................. 24  
Escalations ..................................................................................................................................... 28  
Requesting/Modifying Your AP Workflow Account ........................................................................ 29  
Requesting/Modifying the AP Workflow Account for Your Direct Report .................................... 33  
Immediate Terminations for Employees and Non-Employees ...................................................... 38  
Contractor (CID) to WIN ID Conversion ...................................................................................... 42  
Entitlement Request Workflow ....................................................................................................... 49  
Change Mailbox Type Workflow ..................................................................................................... 54  
On-Boarding Non-Legacy ITO Atos Employee Workflow ............................................................ 59  
Appendix A: AIM Field Explanations ............................................................................................ 60  
Appendix B: Troubleshooting .......................................................................................................... 62  
Appendix C: Allowed Entitlements .................................................................................................. 63  
Helpful Links .................................................................................................................................... 64  
Index ................................................................................................................................................ 65
Preface

Introduction

Access and Identity Management (AIM) is a system that Conduent uses to securely streamline the on-boarding and off-boarding of all Conduent employees and non-employees. Through this technology, you will automatically receive your new employee’s WIN ID once they have been hired. You can instantaneously on-board or off-board a person's Worldwide Identification Number (WIN) or Contractor ID (CID), and Conduent e-mail account through a series of simple clicks.

AIM performs the following tasks:

- Provision domestic accounts and synchronize passwords to Americas, Conduent, GHS, AMS, ACS-CSG, BAS and ITOC Active Directories
- Provisions ACSIND and ACS-OPS Active Directory Accounts (no password synchronization)
- Provision AP Workflow Accounts
- Provision O365 and On-Premise mailboxes
- Extend Contractor logins
- Quickly provide an initial password and WIN ID/CID for new employees and non-employees
- Provides a contractor data repository

What are the benefits of this tool?

AIM provides an interface that you can use from your web browser. From the Work Dashboard tab, you can request a CID and password for Non-employees and check the approval status of their requests. In addition to these benefits, this tool will also perform the following tasks:

- Improve password synchronization
- Automate workflows and electronic forms to streamline HR people-based activities throughout the entire employment life-cycle
- Automate processes for on-boarding/off-boarding users to improve new hire turnaround time and data security
- Present a single source of people data that is consistent and reliable across all our systems
- Decrease time, effort, and associated risks in processing terminated accounts/user access
## Important Features

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Task Notifications</td>
<td>Displays the approval tasks currently assigned to you in your workflow queue.</td>
</tr>
<tr>
<td>Make a Process Request</td>
<td>Let’s you make a request for yourself or provision a new contractor.</td>
</tr>
<tr>
<td>Requests Status</td>
<td>Displays the status of the requests made by you or for you.</td>
</tr>
<tr>
<td>Make Team Process Requests</td>
<td>Let’s you request a resource for a member of your team.</td>
</tr>
<tr>
<td>Approve</td>
<td>Allows you to give your approval to a task.</td>
</tr>
<tr>
<td>Deny</td>
<td>Allows you to explicitly deny your approval to a task. When you deny a task, the request will be cancelled.</td>
</tr>
</tbody>
</table>

*Table 1*
Logging into the AIM System

When you're ready to start using AIM, all you need is your web browser. Because it works in a browser, AIM is as easy to access as any web page.

To access AIM:

- Open your web browser
- Type aim.central.conduent.com in the address bar.
- Type your username (WIN ID or CID) and Password (i.e., your network password) to log into the AIM user application.
- Click Login.

![Login](image1.png)

• Enter a Password Hint if prompted. This will be used by the help desk to verify your identity.
• Click Submit.

![Password Hint](image2.png)
Window Enlargement

The framed window can be enlarged by dragging a corner out. Inversely, the screen can be made smaller by dragging it in.
The Identity Self-Service Tab

The Identity Self-Service tab gives you a convenient way to display and work with identity information about yourself. You can use this feature to perform the following tasks:

- Visualize how users and groups are related
- Manage your own user account directly
- Search for other users and groups in the organization

What you can see and do in AIM is determined by your level of permission. The left side of the Identity Self-Service tab displays a menu of actions that you can perform. The actions are listed by category. When you click an action, it displays a corresponding page on the right.

![Identity Self-Service Tab](image)

**Figure 5**

The following table summarizes the actions that are available to you on the Identity Self-Service tab:

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Organization Chart</td>
<td>Displays the relationships among users and groups in the form of an interactive organizational chart.</td>
</tr>
<tr>
<td>My Profile</td>
<td>Displays the detail for your user account and lets you work with that information.</td>
</tr>
<tr>
<td>Directory Search</td>
<td>Allows you to search for users or groups by entering search criteria or by using previously saved search criteria.</td>
</tr>
</tbody>
</table>

**Table 2**
Changing Your Password

Passwords should be changed through the Self-Service Password Reset Portal (SSPR) system only: https://aim.central.conduent.com/sspr

The Work Dashboard Tab

The purpose of the Work Dashboard tab is to give you a convenient way to perform workflow-based provisioning actions. These actions allow you to manage user access and make provisioning requests.

- The left side of the Work Dashboard tab displays a menu of actions you can perform. Self-service actions are accessed under *Make a Process Request*.

![Figure 6](image)

- Actions for a team member who reports to you are available under *Settings -> Make Team Process Requests*.
- When you click an action, it displays a corresponding page on the right. The page typically contains a window that shows the details for that action.

![Figure 7](image)

The following table summarizes the actions that are available to you on the Work Dashboard
<table>
<thead>
<tr>
<th>Category</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Work Dashboard</td>
<td>Task Notifications</td>
<td>Displays the approval tasks currently assigned to you in your workflow queue.</td>
</tr>
<tr>
<td>Work Dashboard</td>
<td>Resource Assignments</td>
<td>Feature Disabled</td>
</tr>
<tr>
<td>Work Dashboard</td>
<td>Role Assignments</td>
<td>Feature Disabled</td>
</tr>
<tr>
<td>Work Dashboard</td>
<td>Request Status</td>
<td>Displays the status of the requests made by or for you. The list of requests includes those for which you are the initiator or the recipient for a request that authorizes view privileges for recipients.</td>
</tr>
<tr>
<td>Settings</td>
<td>Enter Proxy Mode</td>
<td>Feature Disabled</td>
</tr>
<tr>
<td>Settings</td>
<td>Edit Availability</td>
<td>Shows your availability for approving requests.</td>
</tr>
<tr>
<td>Settings</td>
<td>My Proxy Assignments</td>
<td>Feature Disabled</td>
</tr>
<tr>
<td>Settings</td>
<td>My Delegate Assignments</td>
<td>Feature Disabled</td>
</tr>
<tr>
<td>Settings</td>
<td>Team Availability</td>
<td>Shows your teams availability.</td>
</tr>
<tr>
<td>Settings</td>
<td>Team Proxy Assignments</td>
<td>Feature Disabled</td>
</tr>
<tr>
<td>Settings</td>
<td>Team Delegate Assignments</td>
<td>Feature Disabled</td>
</tr>
<tr>
<td>Settings</td>
<td>Make Team Process Requests</td>
<td>Let’s you make a request for a resource for a member of your team.</td>
</tr>
<tr>
<td>Make a Process Request</td>
<td></td>
<td>Allows you to request a resource for yourself.</td>
</tr>
</tbody>
</table>

Table 3
Approving a New Provisioning Request (On-Boarding)

When individuals are hired for a position, they are entered into an identity repository. You (the manager) will receive two emails: New Employee or Non-Employee Password Notification and New Provisioning Request.

The New Employee or Non-Employee Password Notification email provides the password that the new employee will use when they first log in to the network.

The New Provisioning Request notification provides the WIN ID for the new employee. This email also contains a link to the AIM system where you can approve or deny the request.

If the new employee was formerly a Contractor and has an active Contractor ID (CID), please complete the Contractor to Employee Conversion process prior to approving the new provisioning request. Failure to do so may result in system access failure. Please refer to the Contractor (CID) to WIN ID Conversion process in this document.

**WARNING**: Failure to complete the New Provisioning Request (On-Boarding Employee workflow) will result in termination of the new employee. Managers must approve the On-Boarding Employee workflow within 21 days; failure to approve the workflow within 21 days will result in escalation of the workflow to the Manager’s manager. Failure of the Manager’s manager to approve the workflow within 21 days of receiving the escalation will result in termination of the employee who is being onboarded.
To approve a new provisioning request:

- Inside the notification email, click on the [here](#) link as shown below.

![Figure 9](image)

- The following dialog is displayed.

![Figure 10](image)

- Type your username (WIN ID or CID) and Password (i.e., your network password) to log into AIM.
- Click **Login**.
• Click **Claim** to work on the workflow request.

![Figure 11](image)

• Once accepted the form will display as below

![Figure 12](image)

• The field **Does the Employee have a CID that has not yet been converted?** * is a mandatory field.

• Select Yes/No for the **Does the Employee have a CID that has not yet been converted?** dropdown based on whether or not the user is converting from a CID.

![Figure 13](image)

**Important point to note:** If the employee that you are onboarding currently has an active CID, then you must close this workflow and complete the Contractor-to-Employee workflow before continuing.
• A popup message will be displayed if you answer Yes to the Does the Employee have a CID that has not yet been converted? dropdown.
• Click OK to the message below and the workflow will exit so that you may convert the user's CID. See Contractor (CID) to WIN ID Conversion.

![Message from webpage](image)

Figure 14

• Choose the appropriate domain account(s).
• Domain account fields will be enabled/disabled based on the user’s employee type.

![Form Detail](image)

Figure 15

**NOTE:** For allowed account provisioning by employee type see Appendix C: Allowed Entitlements.

• If the GHS AD Domain account is selected, a popup will be displayed.

![Message from webpage](image)

Figure 16
• If the GHS AD Domain has been selected, select the appropriate GHS location from the drop down list.

**NOTE:** A GHS location that cannot be modified must then be selected.

![Figure 17](image)

• Changes to a permanent employee’s personnel information may be updated using the Global Manager Self-Service link

![Figure 18](image)
• Mail-O365 Account and multiple other account options may be selected. Based on the option selected under Mail-O365 Account user will be receiving access to Mailbox, Skype and Office 2016 Applications.
  o Mailbox Only: A user will receive only a Conduent Remote Mailbox.
  o Mailbox and Skype: User will receive both Conduent Remote Mailbox and Skype access.
  o Mailbox, Skype & Full Office 2016: User will receive access to Conduent Remote Mailbox, Skype and Office 2016 Applications.
  o Mailbox Licensed for Full O365 & Online Office 2016: User will have Full O365 Access and online Office 2016.
  o Mailbox Licensed for Full O365 & Full Office 2016: User will get access to Full O365 and Office 2016 Applications.

![New Conduent mailboxes are now created in Office 365. Your employee’s mailbox login id will be their email address. Your employee can look up their email address by logging into AIM and selecting the My Profile link.](image)

**Figure 19**

• If you are granting the **Mail-O365 Account** for a user, you will be required to specify Mail-O365 Access either as Restricted or an Un-Restricted.
  o UnRestricted Access: A user with a Conduent Remote Mailbox has an un-restricted mailbox and can access their email even when they are not directly connected to the Conduent network.
  o Restricted Access: A user with a Conduent Restricted Mailbox can only access their email when directly connected to the Conduent network.

![New Conduent mailboxes are now created in Office 365. Your employee’s mailbox login id will be their email address. Your employee can look up their email address by logging into AIM and selecting the My Profile link.](image)

**Figure 20**

• Once the form is complete, click **Approve**.

![Please select the appropriate button to approve or reject the request.](image)

**Figure 21**

**NOTE:** If you have multiple requests to approve, you may go to [https://aim.central.conduent.com/IDMProv](https://aim.central.conduent.com/IDMProv) and select Work Dashboard -> Tasks
Notifications to work on the remaining requests.

- After approving the request, you will receive a message stating that your submission was successful. Your approved request will be routed to the Helpdesk for further processing.

![Figure 22](image)

- You will also receive an email notification verifying that a new Active Directory account (Americas, GHS, or ACS-CSG) has been created for your new employee if applicable.
Provisioning a New Non-Employee (Contractor)

Using AIM, you can request a password and CID for new non-employees (contractors).

To provision a new non-employee CID:

- Log into the AIM system.
- Click on the Work Dashboard tab.
- Click *Make a Process Request*

![Figure 23](image)

- Select *All* from the Process Request Category drop down list.
- Click *Continue*.

![Figure 24](image)

- Select *On-Boarding Non-Employee* from the Make a Process Request list.

![Figure 25](image)
• Specify the type of Non-Employee that you are onboarding. You may select Client, Contractor or Vendor. Based on your employee type selection, different accounts may be provisioned for the user.

![Figure 26](image)

**NOTE:** For allowed account provisioning by employee type see Appendix C: Allowed Entitlements.

• Select True for the Request LAN Account field if you would like to request LAN access for your new non-employee (contractor).

![Figure 27](image)

**NOTE:** If False is selected for Request LAN account, the new non-employee will receive only a CID and a Conduent AD account.
• If, you select “True” to “Request LAN Account, then you may choose the appropriate domain account(s). Based on the Non-Employee Type, the appropriate AD Domain dropdowns will be enabled.
• For allowed account provisioning by employee type, see Appendix C: Allowed Entitlements.
• If you are granting the **Mail-O365 Account** for a user, you will be required to specify the type of Mail-O365 Access you wish to grant for the user.

  **Mail-O365 Account Option**
  • Mailbox Only: User will have access only to Conduent Mailbox.
  • Mailbox and Skype: User will receive both Conduent Remote Mailbox and Skype access.
  • Mailbox, Skype &Full Office 2016: User will receive access to Conduent Remote Mailbox, Skype and Office 2016 Applications.
  • Mailbox Licensed for Full O365 & Online Office 2016: User will have Full O365 Access and online Office 2016.
  • Mailbox Licensed for Full O365 & Full Office 2016: User will get access to Full O365 and Office 2016 Applications.

New Conduent mailboxes are now created in Office 365. Your employee’s mailbox login id will be their email address. Your employee can look up their email address by logging into AIM and selecting the My Profile link.

<table>
<thead>
<tr>
<th>Mail-O365 Account:</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Mail-O365 Access:</td>
<td>(none)</td>
</tr>
<tr>
<td>Distribution List:</td>
<td>(none)</td>
</tr>
</tbody>
</table>

**Figure 28**
Mail-O365 Access Option

- Restricted Mailbox: A user with a provision Restricted Mailbox can only access their email when directly connected to the Conduent network.
- Un-Restricted Mailbox: A user with an Un-Restricted Mailbox can access their email even when they are not directly connected to the Conduent network.

![New Conduent mailboxes are now created in Office 365. Your employee’s mailbox login id will be their email address. Your employee can look up their email address by logging into AIM and selecting the My Profile link.](image)

![Figure 29](image)

- Complete the remaining fields in the non-employee provisioning form.

**NOTE:** The asterisk (*) indicates a required field.

- Click **Submit** after you have confirmed the data.

![Please click 'Submit' to provision the new user.](image)

![Figure 30](image)

- A confirmation message will be displayed to confirm the new user’s Sector Code and Cost Center.
- Click **OK** to continue, click **Cancel** to modify your choices.

![Message from webpage](image)

![Figure 31](image)
• You will receive a successful submission message followed by two email notifications.

![Figure 32]

• The first email notification contains the initial password for the new non-employee.

![Figure 33]

• The second email contains the CID.

![Figure 34]

• If an Active Directory account for the Americas, GHS, or ACS-CSG domain was requested then you will receive a *New Account Created* email notification.

![Figure 35]
Extending a Non-Employee CID

Using AIM, you can extend the login expiration date for a non-employee (contractor) who reports to you.

**NOTE:** A user’s login expiration date is not related to a user’s password expiration date. A user’s password expiration date is extended when the user resets his password.

To extend the login of a non-employee CID:

- Log into the AIM system.
- Select the Work Dashboard tab.
- Click the **Settings > Make Team Process Requests** link.

![Figure 36](image1)

- From the **Select a team** drop-down list box, select **Direct Reports**.
- Click **Continue**.

![Figure 37](image2)
- Select **All** from the *Process Request Categories* dropdown.
- Click *Continue*.

![Figure 38](image1)

- Select **CID Login Extension** from the *Make a Process Request* list.

![Figure 39](image2)

- Click on the magnifying glass to select the employee for who the login will be extended (the recipient).

![Figure 40](image3)
• You may search for the recipient by name or by WIN ID. Enter your search criteria and click Search.

![Figure 41](image1.png)

• Click on the row containing the correct employee to select.

![Figure 42](image2.png)

• Click **Continue**.

![Figure 43](image3.png)
• Confirm the information for the recipient.
• Click **Submit**.

![Figure 44](image)

• A final confirmation dialog is displayed.
• Click **Close**.

![Figure 45](image)
Escalations

If you (as a manager) do not act on a new provisioning request within 21 days, the request will automatically escalate to your Manager. Your manager will receive an escalation email and can log into the AIM user application to approve the request. If your manager is a C-level executive, the request will be sent to the Conduent Identity Management team for approval.

To approve an escalated new employee request

- To access AIM, use the here link in the escalation email notification.
- Type your username (WIN ID) and Password (i.e., your network password) to log into the AIM user application.
- Click Login.
- Click Claim to work on the provisioning request.
- Select any additional access needed (i.e. Americas AD Domain).
- Click Approve after you have completed the form.
Requesting/Modifying Your AP Workflow Account

Using AIM, Employees and Managers may request a new APW account for themselves or modifications to their existing AP Workflow account. Managers may also request new AP Workflow accounts and modifications for their direct reports (see Requesting/Modifying the AP Workflow Account for Your Direct Report).

To request/modify an AP Workflow account for yourself

- Log into the AIM system.
- Click the Work Dashboard tab.
- Click Make a Process Request.

![Figure 47](image)

- Select All from the Process Request Category drop down.
- Click Continue.

![Figure 48](image)

- Select APWorkflow Request from the Make a Process Request list.

![Figure 49](image)
• If you already have an AP Workflow account existing values will be pre-selected.
• Enter the appropriate request information.

![Figure 50](image)

**Note:** Fields marked with an * are required.

**Note:** If the email entered into the AP-Workflow Email Address field is already associated to a different AP Workflow user, your request will not be processed. Please ensure that the AP Workflow Email Address field contains your own email.

• Once all the information is correct, click **Submit** to complete the request.

![Figure 51](image)
• You will receive a confirmation email that your request was submitted.
• The email will contain instructions for checking the status of your request.

![Figure 52](image1.png)

• If the request is for you, an email will be sent to your Manager requesting approval.

![Figure 53](image2.png)
• If your request is rejected, you will receive an email stating that your request was rejected and the name of the approver who rejected your request.
• You may contact the approver for more information as to why the request was rejected.

![Figure 54](image.png)

• You may check the status of your request at any time by viewing the comments on your request.
• To view the comments on your request:
  o Log into AIM ([https://aim.central.conduent.com/IDMProv](https://aim.central.conduent.com/IDMProv)).
  o Click on Work Dashboard -> Request Status.
  o Click on the Request.
  o Select Comment and Flow History.
• If the comments show a reviewer who has been assigned to your request but there is not a comment showing that this reviewer has approved your request, then your request is still in progress and you may contact the reviewer/approver to ask if they can approve it.
• If the comments show a reviewer who has been assigned to your request and this reviewer has denied your request, then your request could not be completed, and you can contact the reviewer/approver if you have questions as to why your request was denied.
• If the comments show a line labeled “New Values” then your request has been approved by the AIM system.
• Once your request has been processed by the AIM system you will receive an email stating that your request has completed in AIM.
• After your request has completed in AIM, your account will need to be enabled by the AP Workflow team before you can log into the AP Workflow system.
• Once your account is enabled in AP Workflow, you will receive an email from the AP Workflow team. You may then go into SSPR ([https://aim.central.conduent.com/sspr/private/Login](https://aim.central.conduent.com/sspr/private/Login)) and reset your password so that your AP Workflow password is in sync with your network password.
Requesting/Modifying the AP Workflow Account for Your Direct Report

If you are a manager, you can use AIM to request a new AP Workflow account or make modifications to an existing AP Workflow account for your direct reports.

To request/modify an AP Workflow account for your direct report.

- Log into the AIM system.
- Click the Work Dashboard tab.

![Figure 55](image)

- Click Settings > Make Team Process Requests.

![Figure 56](image)

- Select All from the Process Request Category drop down.
- Click Continue.

![Figure 57](image)
• Select APWorkflow Request from the Make a Process Request list.

![Figure 58](image1.png)

• You will be prompted to select the user for whom you are making the request. Use the magnifying glass to select your employee.

![Figure 59](image2.png)

• You may search for your employee by name or by WIN ID. Enter your search criteria and select Search.

![Figure 60](image3.png)
• Click on your user in the search results list to select.

Figure 61

• Click **Continue**.
• If the user already has an AP Workflow account, existing values will be pre-selected.
• Enter the appropriate request information.

**Note:** Fields marked with an * are required.

**Note:** If the email entered on the AP-Workflow Email Address field is already associated to another user in AP Workflow, your request will not be processed. Please ensure that the AP Workflow Email Address field contains the user’s email.

• Once all the information is correct, click **Submit** to complete request.
• You will receive a confirmation email that your request was submitted.
• The email will contain instructions for checking the status of your request.

![Email Example](image)

**Figure 65**

Once your request has been processed by the AIM system you will receive an email stating that your request has completed in AIM.

- Before the user can log into the AP Workflow system, the account will need to be enabled by the AP Workflow team.
- Once the account is enabled in AP Workflow by the AP Workflow team, the user will receive an email from the AP Workflow team with the AP Workflow login. The user can then use SSPR (https://aim.central.conduent.com/sspr/private/Login) to reset his password so that his AP Workflow password is in synch with his network password.
Immediate Terminations for Employees and Non-Employees

The off-boarding process may be executed in three ways:

1. A scheduled termination which is triggered for future date processing.
   You can log into GMSS (Global Manager Self Service) and enter the scheduled separation date. Normal workflow notification and de-provisioning of access to systems will occur after that date.

2. All of a user’s entitlements are revoked in AIM using the All Access (for Revoke action only) option on the Entitlement Request Workflow (see the Entitlement Request Workflow).

3. A user’s access to systems is immediately disabled using the Off Boarding Workflow (this option does not apply to users with a WINID or users who have CID which was not generated by AIM).

To immediately disable a Non-Employee’s access

- This process only applies to users who have a CID which was generated by AIM.
- Log into AIM.
- Select the Work Dashboard tab.
- Select Settings -> Make Team Process Requests link.
• Click **Continue**.

![Figure 67](image)

• Select **All** from the Process Request Category drop down.
• Click **Continue**.

![Figure 68](image)

• Select **Off Boarding** from the Make a Process Request list.

![Figure 69](image)

• Click on the magnifying glass to select your recipient.
• You may search for your user by name or by CID. Enter your search criteria and select **Search**.

![Figure 70](image)
• Click **Continue**.

![Figure 71](image1)

• Verify the employee data.

• Click **Submit**.

![Figure 72](image2)
• You will receive a message stating that your submission was successful. If your employee was granted an Americas, GHS, or ACS-CSG Active Directory account, you will receive an *Account Disabled* email notification.

![Image](image1.png)

*Figure 73*

• You will also receive an email that contains important information regarding the terminated employee along with a termination checklist.

• This checklist ensures that you have completed processes to terminate accounts not controlled by AIM such as local applications or client accounts.

![Image](image2.png)

*Figure 74*

**NOTE:** Be sure to disable the user in HR using Manager Self-Service to prevent the user from being reactivated in AIM.
Contractor (CID) to WIN ID Conversion

The Contractor (CID) to WIN ID Conversion workflow allows the manager to convert logins that were provisioned to a user as a contractor (CID) to a user’s new WIN ID once they are hired as a permanent employee. The conversion process must be completed **AFTER** the user has received their WIN ID and **BEFORE** the manager completes the onboarding workflow.

To convert a CID to a WINID

- Before beginning, notify the employee who is being converted to log off while the conversion is completed. This will ensure that his/her accounts do not get locked.
- Log into AIM.
- Select the Work Dashboard tab.
- Select Settings -> Make Team Process Requests link.

![Image 1](image1.png)

**Figure 75**

- If prompted to select a team, click **Continue**.

![Image 2](image2.png)

**Figure 76**
• Select All from the Process Request Category drop down.
• Click Continue.

![Figure 77](image)

• Select Contractor-to-Employee Conversion from the Make a Process Request list.

![Figure 78](image)

**FIRST: Search for the Win-ID to be converted:**

• Click on the magnifying glass to select your recipient’s WIN-ID.

![Figure 79](image)
• Select WinID/CID in the search type dropdown.
• Enter the new **WIN ID** in the WIN ID/CID field.
• Click on **Search**.

![Figure 80](image)

• Click on the row containing the correct employee to select.

![Figure 81](image)

• Click **Continue**.

![Figure 82](image)
• If accounts have been provisioned to the WINID you will not be able to proceed. This usually occurs if the WINID was onboarded via AIM prior to starting the conversion process. The error message below will be displayed.

![Error Message](image)

• If you receive the error above, please contact the Help Desk to have a ticket opened so that the user can be converted manually.

**SECOND: Select the C-ID under the Contractor field.**

• On the displayed form click on the magnifying glass next to the Contractor field to enter the C-ID.

![Form](image)

Figure 83
• Select WinID/CID in the search type dropdown.
• Enter the user’s **CID** in the WIN ID/CID field.
• Click on **Search**.

![Figure 84](image1)

- Click on the row containing the correct employee to select.

![Figure 85](image2)
• Confirm all of the employee information. Ensure that the Transfer User Information FROM section contains the user’s Contractor ID (CID). Confirm that the Transfer User Information TO section contains the user’s WIN ID.

• Click Submit.

Figure 86

• After the workflow has completed, a confirmation email notification will be sent to you. Approval of the workflow is no longer required.

Figure 87
• Once the ID conversion and email are converted the manager needs to complete the Employee On-boarding workflow (see Approving a New Provisioning Request (On-Boarding)) for the WIN ID.

• After approval, the user will access the following systems using the noted ID’s if they previously had access with their CID.
  o   Dallas network & VPN: WIN ID
  o   Atlanta: WIN ID
  o   SharePoint: WIN ID
  o   Infobank: WIN ID
  o   Password Reset, SSPR (https://aim.central.conduent.com/sspr/private/Login): WIN ID
Entitlement Request Workflow

If you are a manager, you can use AIM to grant/revoke access on one of the AIM entitlement systems for your direct reports.

To add/remove access to an AIM Entitlement System for your direct report

- Log into the AIM system.
- Click the Work Dashboard tab.

Figure 88

- Click Settings > Make Team Process Requests.

Figure 89

- Select Entitlements from the Process Request Category drop down.
- Click Continue.

Figure 90
• Select *Entitlement Request* from the *Make a Process Requests* list.

![Figure 91](image1.png)

• You will be prompted to select the user for whom you are making the request. Use the magnifying glass to select your employee.

![Figure 92](image2.png)

• You may search for your employee by name or by WIN ID. Enter your search criteria and select *Search*.

![Figure 93](image3.png)
• Click on your user in the search results list to select.

Figure 94

• Click **Continue**.

Figure 95
• Select the **Entitlement System** that you wish to add to or remove from the user (AD: Americas, Email: Conduent Mailbox, etc.)

• To remove all access for a user, select **All Access (for Revoke action only)** for the **Entitlement System**. This will disable the user’s access on any system associated to the user in AIM.

• Upon selection of Email: Conduent Mailbox you need to select the Mail-O365 Account and Mail-O365 Access.

• To add access, select **Grant** for the **Entitlement Action**. This will create an account for the user on the selected **Entitlement System**.

• To remove access, select **Revoke** for the **Entitlement Action**. This will remove the user’s account on the selected **Entitlement System**.

![Figure 96](image)

• If you are granting the **Conduent Mailbox** for a user, you will be required to specify Mail-O365 Account and Access either as Restricted or an Un-Restricted.
  - Restricted Mailbox: A user with a Restricted Mailbox can only access their email when directly connected to the Conduent network.
  - Un-Restricted Mailbox: A user with an Un-Restricted Mailbox can access their email even when they are not directly connected to the Conduent network.

![Figure 97](image)
**Note:** The Mailbox Type dropdown will only be enabled if the Entitlement System is Conduent Mailbox.

- Confirm the information selected.
- Click *Submit*.

![Figure 98](image)

- A final confirmation dialog is displayed.
- Click *Close*.

![Figure 99](image)
Change Mailbox Type Workflow

If you are a manager, you can use AIM to change the mailbox type for one of your direct reports.

Five Mail-O365 Account and two Mail-O365 Access types are allowed:

**Mail-O365 Account:**

- Mailbox Only: User will have access only to Conduent Mailbox.
- Mailbox and Skype: User will receive both Conduent Mailbox and Skype access.
- Mailbox, Skype & Full Office 2016: User will receive access to Conduent Mailbox, Skype and Office 2016 Applications.
- Mailbox Licensed for Full O365 & Online Office 2016: User will have Full O365 Access and online Office 2016.
- Mailbox Licensed for Full O365 & Full Office 2016: User will get access to Full O365 and Office 2016 Applications.

**Mail-O365 Access:**

- Un-Restricted Mailbox: A user with an Un-Restricted Mailbox can access their email even when they are not directly connected to the Conduent network.
- Restricted Mailbox: A user with a Restricted Mailbox can only access their email when directly connected to the Conduent network.

To change the mailbox type for your direct report

- Log into the AIM system.
- Click the *Work Dashboard* tab.

![Image of AIM system](image.png)
• Click Settings > Make Team Process Requests.

![Figure 101](image1.png)

• Select All from the Process Request Category drop down list.
• Click Continue.

![Figure 102](image2.png)

• Select Change Mailbox Type from the Make a Process Requests list.

![Figure 103](image3.png)

• You will be prompted to select the user for whom you are making the request. Use the magnifying glass to select your employee.

Note: To use the Change Mailbox workflow, the employee must already have a mailbox provisioned. For provisioning of a new mailbox, please see Entitlement Request Workflow.
You may search for your employee by name or by WIN ID. Enter your search criteria and select Search.

Click on your user in the search results list to select.
• Click **Continue**.

![Figure 107](image)

• The user’s current mailbox type is displayed in the Original Mailbox Type drop down.
• Specify the change to the user’s mailbox by selecting the appropriate value in the New Mailbox Type dropdown.
• Click **Submit** after you have confirmed the selection.

![Figure 108](image)

![Figure 109](image)
• You will receive a successful submission message.
• Click Close.

Figure 110
On-Boarding Non-Legacy ITO Atos Employee Workflow

The On-Boarding Non-Legacy ITO Atos Employee workflow is used by automated processes only. Atos employees are onboarded into AIM using an automated feed from Atos.

Figure 111

- If you attempt to access the On-Boarding Non-Legacy ITO Atos Employee workflow, the following message will be displayed.
- Click **OK**.
- The workflow will be cancelled.

Figure 112
## Appendix A: AIM Field Explanations

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User</td>
<td>Employee's name</td>
</tr>
<tr>
<td>Win ID</td>
<td>Employee’s Worldwide Identification Number</td>
</tr>
<tr>
<td>User Type</td>
<td>Defaults to Employee</td>
</tr>
<tr>
<td>New Americas AD Domain</td>
<td>Request an Americas Active Directory account</td>
</tr>
<tr>
<td>New GHS AD Domain</td>
<td>Request a GHS Active Directory account</td>
</tr>
<tr>
<td>New ACS-CSG AD Domain</td>
<td>Request an ACS-CSG Active Directory account</td>
</tr>
<tr>
<td>Title</td>
<td>The Employee's job title</td>
</tr>
<tr>
<td>Telephone</td>
<td>The employee's telephone number (and extension, if applicable)</td>
</tr>
<tr>
<td>Business Group</td>
<td>Defaults to manager’s group</td>
</tr>
<tr>
<td>Business Unit</td>
<td>Defaults to manager’s unit</td>
</tr>
<tr>
<td>Department</td>
<td>Defaults to manager’s department</td>
</tr>
<tr>
<td>Cost Center</td>
<td>Defaults to manager’s cost center</td>
</tr>
<tr>
<td>Location</td>
<td>Defaults to manager’s location</td>
</tr>
<tr>
<td>Address</td>
<td>Defaults to manager’s address</td>
</tr>
<tr>
<td>City</td>
<td>Defaults to manager’s city</td>
</tr>
<tr>
<td>State</td>
<td>Defaults to manager’s state</td>
</tr>
<tr>
<td>Postal Code</td>
<td>Defaults to manager’s postal code</td>
</tr>
<tr>
<td>Country</td>
<td>Defaults to manager’s country</td>
</tr>
<tr>
<td>Primarily works from</td>
<td>Select a Business Address, Home, or Client Site</td>
</tr>
<tr>
<td>Physical Office Address</td>
<td>Enter the address where the employee is located</td>
</tr>
<tr>
<td>Company (contractors only)</td>
<td>Enter the name of the company supplying the contractor</td>
</tr>
<tr>
<td>Mail-O365 Account</td>
<td>If the employee needs an email account, choose the appropriate mailbox type.</td>
</tr>
<tr>
<td>Mail-O365 Access</td>
<td>Enter the Restricted or UnRestricted Mailbox Access</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Distribution List</td>
<td>Enter the email distribution list to which the employee should belong.</td>
</tr>
<tr>
<td>RACF</td>
<td>Request a Resource Access Control Facility (RACF) account for this employee. RACF is IBM’s security package.</td>
</tr>
<tr>
<td>SharePoint</td>
<td>Request a SharePoint account for this employee. The Microsoft Office SharePoint Portal is the ACS standard for connecting people, teams, and knowledge across business processes.</td>
</tr>
<tr>
<td>Live Link</td>
<td>Request a Live Link account for this employee. Live Link is a document repository.</td>
</tr>
<tr>
<td>Quick Place</td>
<td>Request a QuickPlace account for this employee. QuickPlace is the component of Lotus Notes containing the Sametime Connect Client, the Instant Messaging application for employee use.</td>
</tr>
<tr>
<td>UltiPro</td>
<td>Request an UltiPro account for this employee. For new employees, an account is created in UltiPro, the U.S payroll database.</td>
</tr>
<tr>
<td>Corporate Internal Metaframe</td>
<td>Request a metaframe account for this employee.</td>
</tr>
<tr>
<td>VPN Access</td>
<td>Request a VPN account for this employee. A Virtual Private Network account allows an employee to login securely to the corporate network. <strong>Note: Employees with Americas accounts will already have a VPN account.</strong></td>
</tr>
<tr>
<td>RSA Token Access</td>
<td>Request RSA Token Access for this employee. Some clients require a secure token to login to their servers.</td>
</tr>
<tr>
<td>Citrix Access</td>
<td>Request a Citrix account for this employee. Citrix is a client for secure remote access.</td>
</tr>
<tr>
<td>Network Folder(s) Access</td>
<td>Include the full data path of the folder to which this employee needs access.</td>
</tr>
<tr>
<td>Specify Access Needed</td>
<td>Set the file access rights for this employee (e.g., Read Only, Write, Modify, or Owner)</td>
</tr>
</tbody>
</table>

*Table 4*
Appendix B: Troubleshooting

Listed below are troubleshooting tips to assist you if you have problems with the AIM system.

<table>
<thead>
<tr>
<th>Problem</th>
<th>System</th>
</tr>
</thead>
<tbody>
<tr>
<td>My Active Directory account is locked out after I changed my password.</td>
<td>1. Log out of Outlook and your workstation. 2. Change your password once more. 3. Try your new password. 4. Should it fail, allow up to 15 minutes for the new password to propagate through the system.</td>
</tr>
<tr>
<td>My Active Directory accounts get locked out repeatedly.</td>
<td>1. Remove or update all iPhone, iPad, network drives, or virtual desktops with old passwords 2. Try to log off network and re-login to confirm correct password locally.</td>
</tr>
<tr>
<td>Some of my passwords fail</td>
<td>1. Identify breakdown point. 2. If any AD password fails, try resetting with a non-default password. Repeated resets with same password is usually accepted in AIM but rejected in AD. 3. Try logging into each environment separately to narrow break down: Infobank/Americas (AIM), iProcurement/ePay (S3), Email. Try old password also? Has S3 ID been activated? 4. Delayed by congested network traffic. Try to change password later in day</td>
</tr>
<tr>
<td>The password change does not show up in Infobank or my AD account, even though I can log into AMP or AIM with my new password.</td>
<td>1. Your AIM profile does not have the necessary 2. Active Directory entitlement. 3. Open a Help Desk ticket assigned to the AIM team to add the correct entitlement for your profile.</td>
</tr>
<tr>
<td>The email notifications are going to my Junk Mail folder.</td>
<td>1. Open Outlook. 2. On the Tools menu, click Options. On the Preferences tab, under E-mail, click Junk E-mail. 3. Click the Safe Senders tab. 4. Click Add. 5. In the Enter an e-mail address or Internet domain name to be added to the list box, enter acs-inc.com, and then click OK. 6. Repeat Steps 5 and 6 for conduent.com and any other name or address that you want to add.</td>
</tr>
<tr>
<td>I received the AIM notification, but I no longer see the request in my queue.</td>
<td>1. The AIM On-Boarding workflow has been escalated to your manager. 2. If you need to process immediately, open a Help Desk ticket assigned to the AIM team to reassign the request back to you.</td>
</tr>
</tbody>
</table>

Table 5
Appendix C: Allowed Entitlements

The chart below specifies the access that is allowed by target system for each employee type in AIM.

<table>
<thead>
<tr>
<th>Target System</th>
<th>Client</th>
<th>Contractor</th>
<th>Employee XS</th>
<th>GEMS Contractor</th>
<th>Partner</th>
<th>Vendor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active Directory ACS-CSG</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Active Directory ACSIND</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Active Directory ACS-OPS</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Active Directory Americas</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Active Directory BAS</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Active Directory CaMMIS</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Active Directory Client</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Active Directory DOL</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Active Directory GHS</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Active Directory ITOC</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Active Directory Partners</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Active Directory US Coopers</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Conduent Mailbox / Mail-O365 Account</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td></td>
</tr>
</tbody>
</table>
Helpful Links

Conduent IT Support

https://itsupport.central.conduent.com

Conduent Connect

https://www.conduentconnect.com
Index

AP Workflow Accounts, 29, 33
Approving a request, 12
Benefits, 4
Changing your password, 9
Definitions, 60
Escalations, 28
Extending a Non-Employee CID, 24
Features, 5
Helpful Links, 64
Logging into AIM, 6
On-Boarding Non-Employee, 19
Password Hint, 6
Self-Service tab
   Actions, 8
Team Request, 10
Terminations, 38, 42
The Identity Self-Service tab
   Overview, 8
The Work Dashboard tab
   Actions, 11
   Overview, 10
Troubleshooting, 62