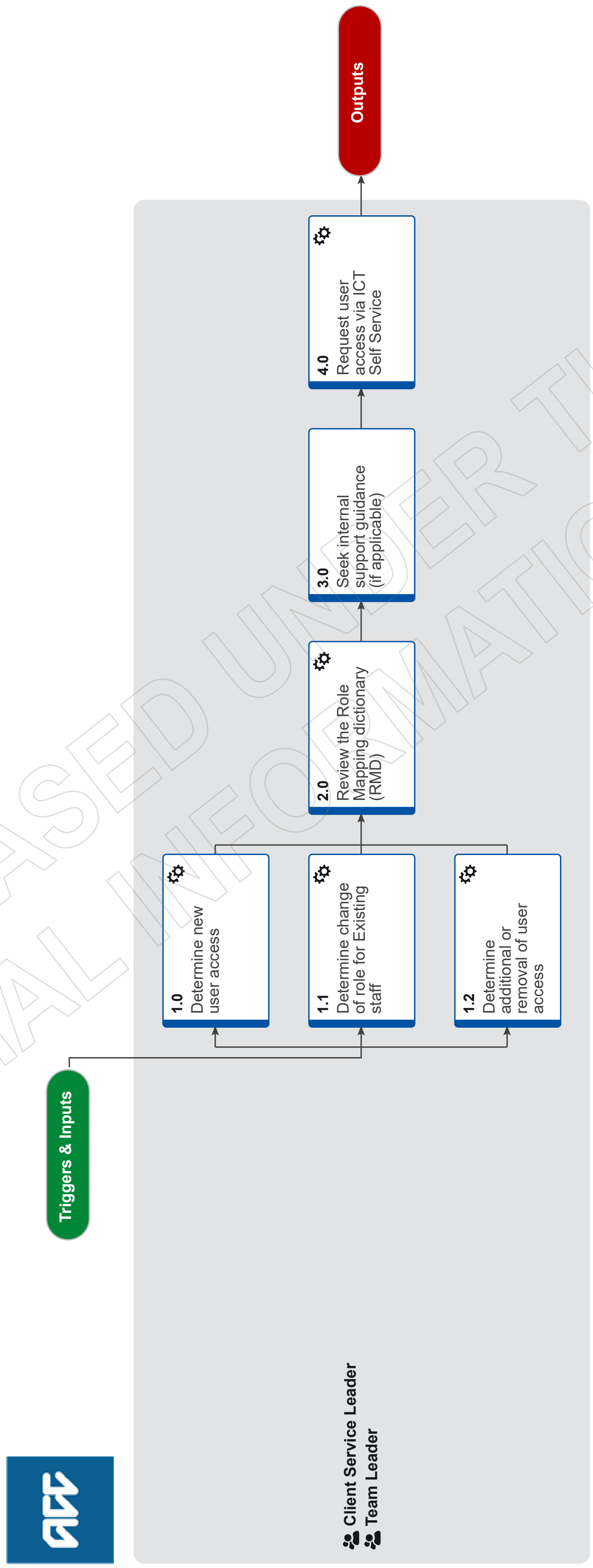
GOV-028268

Request Access to Eos and MFP v3.0



Request Access to Eos and MFP v3.0

Summary

Objective
To on-board and request Eos and MFP system access for an employee through the ICT self service, including updating the employee role and system access.

Background
Within two days of the candidate completing onboarding, hiring Leaders receive an email to approve the creation of a New User account for system access.

Once the user is created, Leaders can access any additional system requirements through ICT Self Service. Leaders can use the Role Mapping Dictionary to identify the access required for Eos/MFP, Telephony, Salesforce, Shared inboxes and Heartbeat.

Owner [Out of Scope]

Expert

Procedure

1.0 Determine new user access

Client Service Leader, Team Leader

a Identify the type of role that the staff member requires to do their core role.

NOTE **How do you identify the type of role that the staff member requires to do their core role?**
Review the Te Kahu checklist to find the role type.

NOTE **What if the staff member requires Remote Claims Unit (RCU) access?**
Contact the RCU team leader via remoteclaims@acc.co.nz to discuss the need for RCU access. RCU access will be managed outside of this process.

Review activity 1.0 of the below process to determine what information you need to provide when requesting access to RCU. This process ends.

PROCESS Manage Remote Claims Unit (RCU) Access to Eos

NOTE **What if the staff member requires Third Party Administration (TPA) access?**
Contact the TPA team leader to discuss the need for TPA access. TPA access will be managed outside of this process.

Review activity 1.0 of the below process to determine what information you need to provide when requesting access to TPA. This process ends.

PROCESS Manage Third Party Administrator (TPA) Access to Eos

1.1 Determine change of role for Existing staff

Client Service Leader, Team Leader

a Identify the type of role that the staff member requires to do their core role.

NOTE **How do you identify the type of role that the staff member requires to do their core role?**
Review the Te Kahu checklist to find the role type.

NOTE **What if you want to check the users current Eos access.**
Review the 'Check & Confirm Eos Access - System Steps' to determine your current user access.

If you are a leader, review the system access report below.

Check & Confirm Eos Access - System Steps

System Access Report

NOTE **What if the user is an existing MFP or EOS user?**
Request for the existing access to be removed to ensure that the user has got the correct access and can only access the information that they require to complete their role.

NOTE **What if the user is an existing MFP or EOS user but no longer require access?**
Request for the access to Eos and MFP be removed. Go to step 4.0 to complete the request. This process ends.

NOTE **What if you want to update the Employee profile on HRIS in addition to Eos access?**
Go to the '(NGCM) Request and update change in reporting line/roles' process for further instruction on how to update the Employee profile on HRIS.

PROCESS (NGCM) Request and update change in reporting line/roles

---

1.2 Determine additional or removal of user access

Client Service Leader, Team Leader

a Check your current Eos user access by reviewing the 'Check & Confirm Eos Access - System Steps' to determine your current user access, if applicable.

Check & Confirm Eos Access - System Steps

NOTE **What if you discover that you have more access than the RMD indicates for your role?**
Go to 4.0 and submit an ICT request to have the additional access removed.

For more information go to 2.0 Review the Role Mapping Dictionary.

NOTE **What if you discover that you have less access than the RMD indicates for your role?**
Go to 4.0 and submit an ICT request to have the missing access added.

For more information go to 2.0 Review the Role Mapping Dictionary.

2.0 Review the Role Mapping dictionary (RMD)

Client Service Leader, Team Leader

a Review the Role Mapping Dictionary to identify the access required for Eos/MFP.

Role Mapping Dictionary

NOTE **What if the role you are searching for is not on the RMD?**
Go to 3.0 'Seek internal support guidance'.

NOTE **What if the access you require is not part of the standard role access in the RMD?**
Go to 3.0 'Seek internal support guidance'.

NOTE **What if you require additional system requirements compared to the Role Mapping Dictionary?**
Refer to the Delegations framework to check if the additional access is appropriate for the user access request and role.

If the additional access is appropriate Go to 3.0 Seek internal support guidance to request the access.

Delegations framework - sharepoint

Check & Confirm Eos Access - System Steps

NOTE **What if you are unsure if the additional access request is appropriate?**
Go 3.0 'Seek internal system support' for advice on the correct and appropriate additional access.

3.0 Seek internal support guidance (if applicable)

Client Service Leader, Team Leader

a Review the self-service guide to determine if the query can be resolved without an ISST request.

Self-service guide - requesting Eos and MFP access

NOTE **What if you were unable to resolve your query by reviewing the Self-service guide?**
Continue with 3.0 b and seek internal systems support guidance.

b Complete the Internal System Support Team (ISST) Microsoft form and ensure you complete all the fields.

Request Internal Systems Support form

c Submit the form to the ISST for review.

4.0 Request user access via ICT Self Service

Client Service Leader, Team Leader

a Log into ICT Self Service, locate the application/system that the new staff member needs access to.

ICT Self Service

b Complete all the relevant sections by copying and pasting the correct information from the Role Mapping dictionary.

NOTE **Please disregard the instructions on the ICT Self Service EOS and MFP request form and follow the relevant system steps below instead.**

Request Eos & MFP Access for a New User – System Steps

Request Updated Eos & MFP Access for an Existing User - System Steps

NOTE **What if you require access to NGCM Salesforce, Shared mailboxes, Skype/telephony set up with regional hunt group information?**
Go to the ICT User Setup Guide for further guidance on how to request access to NGCM Salesforce, Shared mail-boxes, Skype/telephony set up with regional hunt group information etc.

NOTE **What if my previous request for Eos and MFP access have been declined?**
Your request may have been declined because:

· The access request does not match the access in the RMD
· The request may have been unclear
· You may not be entitled to the access you have requested.

ICT User Setup Guide

c Submit the ICT request for management approval and processing.

ACCESS MONITORING CRITERIA

Appropriate Access Assessment

We are committed to respecting the personal information and privacy of ACC's clients, employees, and stakeholders. To achieve this, we must manage the information entrusted to us by adhering to the legislative and policy framework outlined below:

POLICY/GUIDELINE	DESCRIPTION
Personal Information and Privacy Policy	This policy sets out how ACC collects, stores, uses, discloses, retains, and protects personal information in line with the Privacy Act 2020 and the Health Information Privacy Code 2020.
Personal Information and Privacy Guidelines	These guidelines supplement ACC's Care of Personal Information Policy.
Integrity Policy	This policy sets out the standards of integrity and conduct that ACC's people must comply with, together with how ACC will manage and investigate potential integrity breaches.
Integrity Guidelines	These guidelines supplement ACC's Integrity Policy.
Code of Conduct	This policy governs the behaviours of all employees of ACC, to enable us to meet the expectations placed upon us as a Crown Entity. These standards incorporate the standards that apply to all State Servants, detailed in the State Services Standard of Integrity and Conduct.

Aligned to this framework, the criteria below have been developed to use as part of the Access Monitoring Check.

Access Assurance Rating:

After discussing the access of each claim with the team member, an Access Assurance Rating must be applied to each instance of access. The options are:

- **Assurance:** This rating should be applied when you are confident that there is a valid business reason for the access and evidence has been identified that supports that the access is in-line with our policies and guidelines.

- **Low Assurance:** This rating should be applied when you have been unable to confirm a valid business reason for the access and/or cannot identify any evidence that would support that the claim access was in-line with our policies and guidelines.

BUSINESS REASON FOR ACCESS	EVIDENCE OF ACCESS	ASSURANCE RATING	COMMENTARY
YES	YES	ASSURANCE	NO
YES / NO	NO	LOW ASSURANCE	YES

A rating of Low Assurance would indicate that second tier validation may be required, including supplying supporting commentary into the Client Information Access Validation Tool.

Ultimately, Team Leaders will need to apply some judgement when determining the Access Assurance Rating and whether second tier validation is required. It's about the reasonableness of the access and subsequent inquiries to decide as to the appropriateness of that access. It may not be definitive, but we need to demonstrate that reasonable steps have been taken (and documented) to verify the access.

The 'business reasons' listed in the criteria below have been identified by frontline staff as valid reasons for accessing a claim. These criteria will be updated over time as more information about valid reasons for access are identified.

Access Evaluation Criteria

Reasons for access that can be evidenced on the claim

BUSINESS REASON	DESCRIPTION	EXAMPLE	EVIDENCE
Claim establishment	Registration of a claim or client record	• Claim registration • Upload or update client/claim information as part of lodgement	• Logs in Eos
Request for information from party to claim	The team member receives a request for information for (or from?) a claim party (eg client, ATA, or provider)	• Phone call requesting information • Feedback received from client • Complaint received from client • Emailed document • Client Administration task • MyACC setups • Responding to live chats • Email responses	• Contacts in Eos • Email filed away • Task details logged • Logs in Salesforce • Document added to claim
Planned task or intervention	Action was required to complete a planned task	• EOS task or Salesforce intervention	• Logs in Eos or Salesforce
Allocate work	Team member receives a request internally to perform an action on a claim	• Workforce management allocate claim to department or team member • Workforce management/Team Leader allocate task	• Contacts in Eos • Case Owner field • Task details

Internal work request		• Entitlement task to Recovery Admin • Recovery Support – Hotline or written guidance • Request from Payment team to extend a PO • Managing CC task queues • Managing a colleagues inbox	• Contacts in Eos • Logs in Salesforce • Task details

Reasons for access that may not be evidenced on the claim

BUSINESS REASON	DESCRIPTION	EXAMPLE	POSSIBLE EVIDENCE (IF ANY)
Advice or Guidance	Team member accessed the claim to provide support, or guidance for learning purposes	• Seeking advice from a colleague • Providing training • Buddying • Floorwalking • Supporting with threatening calls • Reception cover queries where access is restricted re sensitive claims	• Induction material • Support plan • Floorwalker tracker • Buddy feedback
Review previous claim(s)	Reviewed previous claim to assess cover, duplication or entitlement for a new claim	• Mental Injury claims • Surgery requests • Previous Rehab • Consequential injuries	• Written guidance • Recovery plan • Duplicate tab
Service or quality review	Action was required to provide quality or service assurance	• Side-by-sides • CXQ • Quality assurance reviews • Access Monitoring	• Side-by-side feedback forms

Other requests	A request required action that falls outside of the norm	• Responding to a Ministerial • System maintenance • Provide anonymised information for analysis/ training	
Locate correct claim	Claim accessed to identify the correct claim to action a request or information	• Uploading a document (without claim number) to the correct claim • Accessing multiple claims to find P/O • Client unable to recall claim number • Entering an incorrect claim # in the search	• Logs in Eos • Duplicate tab
Request or information from party to claim	Team member received a request/information from a party to the claim (eg provider)	• Provider may call or email querying an invoice that has not released or a purchase order	• Evidence could sit in MFP or in the Genesys Engage system