



DoD Mobility Unclassified Capability (DMUC)

Implementation and Sustainment Processes

As of 29 April 2016

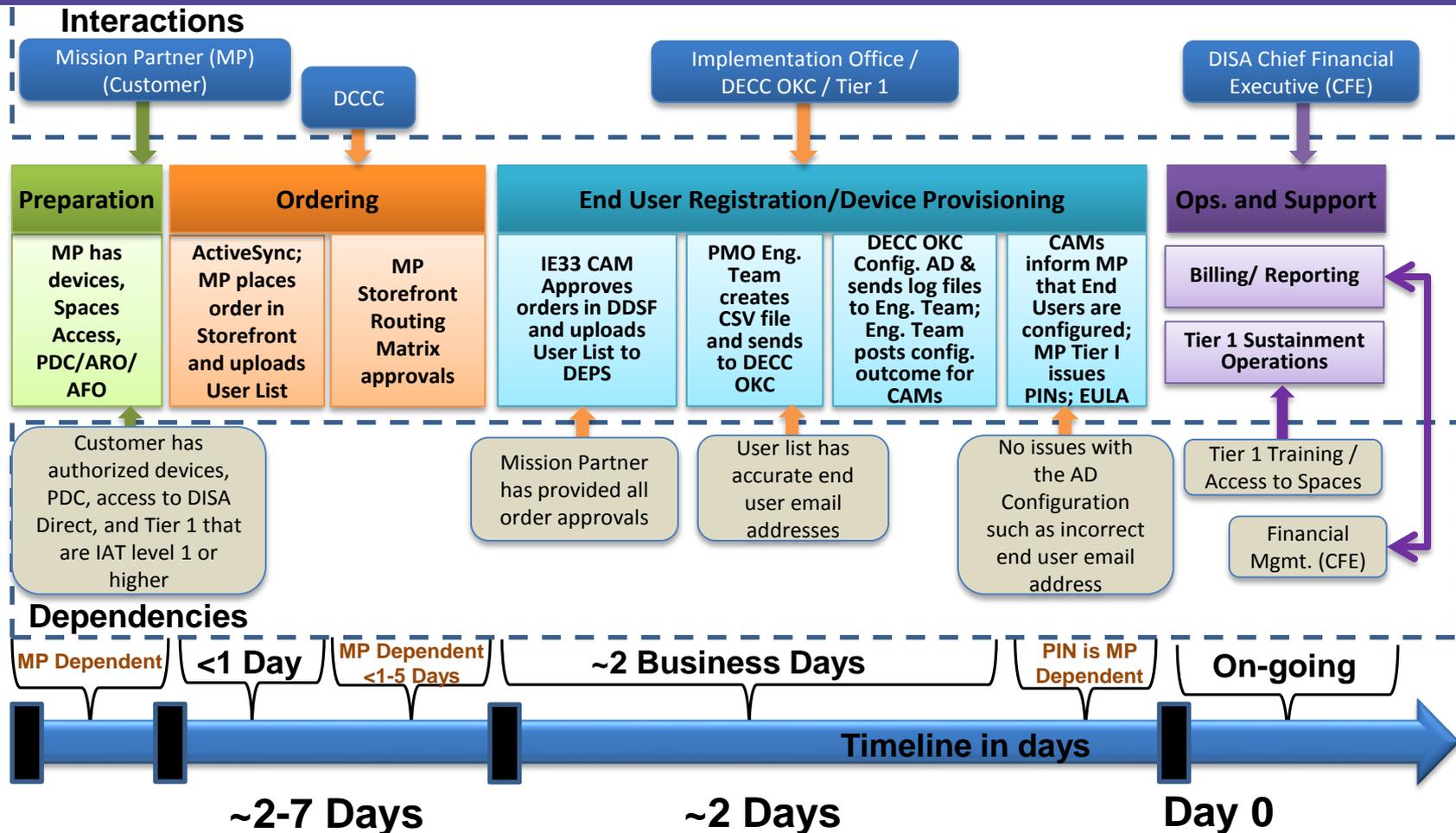


Agenda

- **New Mission Partner Implementation Overview (Slides 3-5)**
- **Preparation (Slides 6-17)**
- **Ordering (Slides 18-22)**
- **End User Configuration (Slides 23-25)**
- **Device Provisioning an EULA (Slides 26-28)**
- **Service Desk Roles and Responsibilities (Slides 30)**
- **Ordering Do's and Don't (Slide 31)**
- **Sustainment Use Cases (Slides 32-37)**
- **Sustainment End User Recording Template Modification Examples (Slide 38)**



New Mission Partner Process Overview (Enterprise Baseline)



Request Fulfillment durations for existing Mission Partners is approximately 2-7 business days based on a daily configuration schedule Monday-Friday, but is dependent on the Mission Partner approving orders in DISA Direct and issuing PINs after end users are configured



On-boarding Process

Preparation

- Mission Partner (MP) procures devices, and carrier service plans (if required)
- MP Tier I admins review MobileIron (Core) Spaces training, and submits 2875s and Spaces training review and copy of IAT cert for Mobility console/Spaces access
- MP obtains Program Designator Code (PDC) to fund Mobility Infrastructure Service
- MP obtains DISA Direct Authorized Requesting Official (ARO) role to access Storefront, and has established routing

Ordering

- MP create Telecommunications Requests (TRs) in DISA Direct Store Front (DDSF) and uploads User List spreadsheet with key attributes (e.g., end users' Enterprise Email, device unique identifier, Customer Job Order Numbers [CJONs], POC to notified when AD LDS configurations are complete)
- MP enables ActiveSync for user receiving device via DEPO by selecting the "MOBILITY_ACTIVATESYNC" under Mobile Service Class



On-boarding Process (Continued)

End User Registration

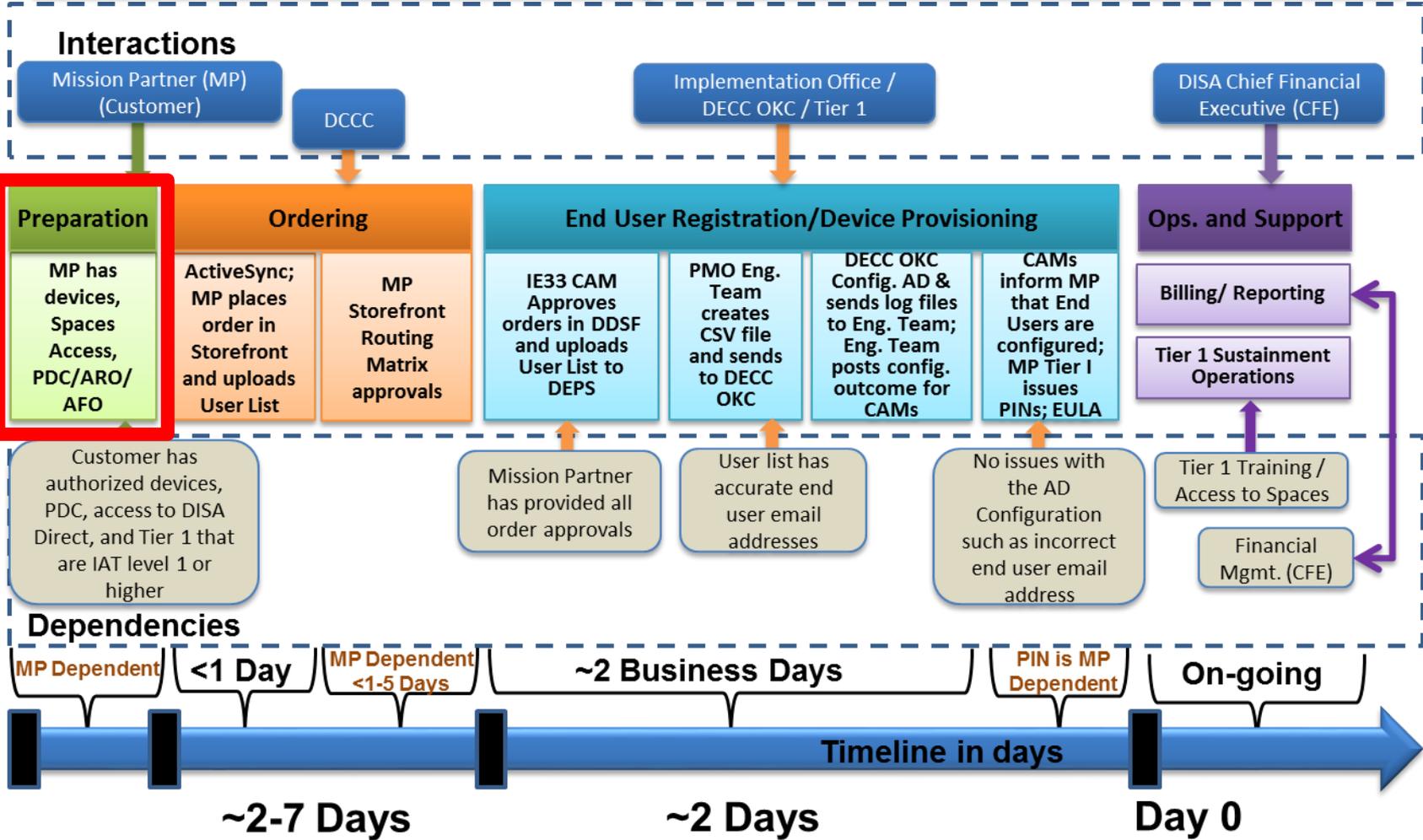
- DISA Mobility CAM Team provides final Storefront TR approval and uploads User List to internal DEPS (SharePoint) for end user configuration in AD LDS for MobileIron
- DISA Mobility Engineering Team applies policies on the User List List_Values tab to end user email addresses and submits to DMUC Tier II, DECC OKC
- DISA DECC OKC implement end user configurations in the production environment
- DISA Mobility CAMs inform Mission Partner of successful/unsuccessful configurations
- MP requests/issues PINs from their Tier 1 for successfully configured end users; Correct any email addresses that were not found during configuration and resubmit affected rows/end users only to the CAM Team (Disa.meade.ie.mbx.dod-mobility-cam-team@mail.mil) for configuration resubmission

Device Provisioning

- MP's Tier 1 issues MobileIron PINs from MobileIron console
- End User signs DMUC End User License Agreement (EULA) - maintained locally
- MP provisions device in accordance with DMUC device Setup guide (operating systems dependent) from the Mobility User Corner (click on the appropriate device to locate)



Preparation





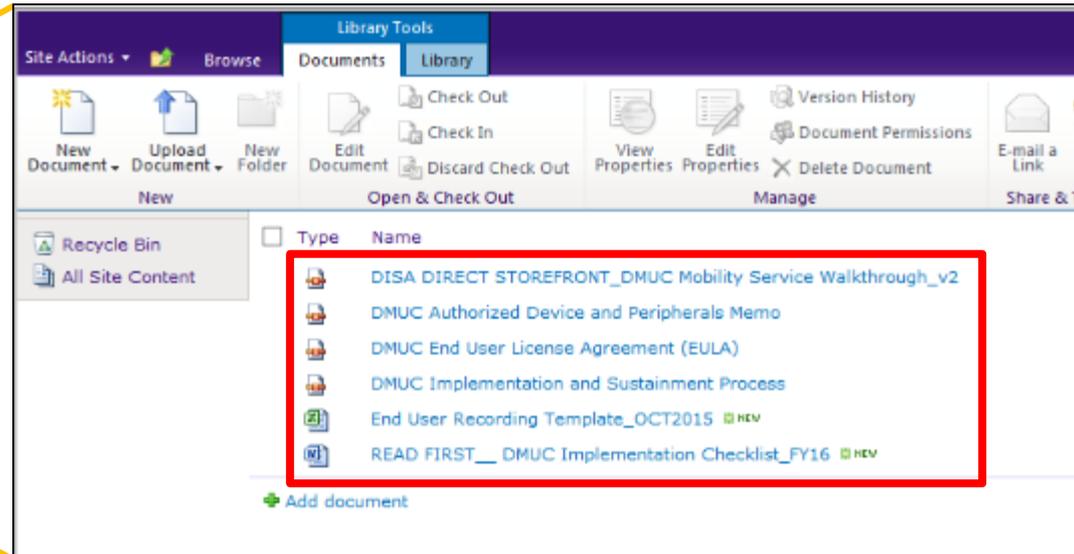
Mobility User Corner – Getting Started

Preparation

Use Email Cert to Login Unless Dual Persona

https://disa.deps.mil/ext/cop/dod_mobility/SitePages/UserCornerHome.aspx

- Select “Prospective & Onboarding DMUC Customers”
- Download and review the DMUC Implementation Checklist, DDSF DMUC Mobility Service Walkthrough and End User Recording Template





MobileIron Spaces Access

Preparation

- The Mobility Implementation goal is to have each Mission Partner stand up a CC/S/A-wide Level 1 Mobility Service Desk – Tier I for Army is AESD only
- Mission Partner completes provided spreadsheet with System Admins and submits to the Implementation Team for the DMUC Tier I Help Desk DEPS site, which contains the MobileIron Spaces Access documentation
- Mission Partner's administrators leverage MobileIron Spaces Access documentation to obtain Out of Band (OOB) VPN and MobileIron credentials to manage their own devices

Submit Spaces Access System Admin List to Mobility Implementation

System Admins (SA) given Service Operations Portal Permissions

Download DMUC Spaces Account Access SOP & DD2875 Templates

SA Review Spaces Tier I Training on Service Operations Portal

SA submits 2875, IAT Cert and training review verification to Mobility Team email in SOP

SA submits 2875 to DECC MONT for OOB

DECC OKC creates and sends Spaces credentials to SA



Ordering Components

Preparation

Device*

- Purchased by organization before entry into DMUC Program
- List of currently approved devices may be viewed in the DMUC Device Memo
- Devices must be GFE and can be purchased through organizational contracting office or another Blanket Purchase Agreement (BPA)

Carrier Service Plan*

- Optional, Wi-Fi only devices are approved for use
- Contracted by organization before entry into DMUC Program
- Carrier agnostic
- Carrier service plans must be on a Government contract and can be coordinated through organizational contracting office or another BPA



Infrastructure Service

- Defense Capital Working Fund service provided by DISA
- Provides for Mobile Device Management (MDM) and Mobile Application Store (MAS)
- DoD App Store provides a secure app solution, tailorable to organizational needs
- FY16 cost is \$7.54 per month per device (includes 2.5 % DITCO fee)

* Paid for by Mission Partners separate and apart from DWCF Service listed on right

Mission Partners procure these before subscribing.....



....to this DWCF service through DISA Direct.



DMUC Infrastructure Service

Preparation

- Device management through a Mobile Device Manager (MDM) – MobileIron
- Access to DoD-controlled Mobile Application Store (MAS)
- Access to secure DoD Enterprise Email (DEE), Calendar, Contacts, Tasks, and Notes (iOS only)
- Secure browser to access public-facing CAC-enabled (e.g., DEPS) web sites
- Tier 1 service desk training
- Level 2 Tier 2 & 3 Service Desks
- Dedicated Mobility Gateway
- Official Billing Rate document (“DWCF Price Book”) is on DISA Direct:
- https://www.disadirect.disa.mil/products/asp/BillingRates/FY16_DWCF_Rate_Letter_Draft_Final.pdf



Purchasing Devices and Carrier Service

Preparation

- Mission Partners purchase devices and carrier services based on their existing procedures
- Army can use the NETCOM Next Generation:
 - <https://portal.netcom.army.mil/apps/wem/>

WEM Portal Steps:

1. Create account
 2. Submit requirements
 3. Requirements go to all BPA vendors
 4. Receive quotes in six (6) business days
 5. Order devices and carrier service
- W91RUS-11-A-0005 (Sprint) – Expires 31 July 2016*
 - W91RUS-11-A-0006 (Verizon) – Expires 31 July 2016*
 - W91RUS-11-A-0007 (AT&T) – Expires 2 August 2016*
 - W91RUS-11-A-0008 (T-Mobile) – Expires 2 August 2016*
- *Before these expiration dates, a task order can be placed against the BPA for up to a 12-month period of performance.



Purchasing Devices and Carrier Service (Continued)

Preparation

- **GSA offers Federal Strategic Sourcing Initiative (FSSI) Wireless BPA:**
- **<http://www.gsa.gov/portal/category/100931#contractors>**
 - **GSA Schedule 70:**
 - GS-35F-0119P (Verizon)
 - GS-35F-0297K (AT&T)
 - GS-35F-0329L (Sprint)
 - GS-35F-0389Y (Vodafone)
 - **GSA FSSI BPAs* (Based on GSA IT Schedule 70 SIN 132-53):**
 - GS00Q13NSA3000 (AT&T)
 - GS00Q13NSA3001 (Sprint)
 - GS00Q13NSA3002 (T-Mobile)
 - GS00Q13NSA3003 (Verizon)
- **Task orders may not exceed more than 5 years beyond the term of the BPA. Task order option periods, if included at initial issuance of the task order, may be exercised after the expiration date of the BPA, but may not extend beyond five (5) years after the expiration of the BPA.**



Receiving Devices

Preparation

- Obtain IMEI, Serial number or Wi-Fi MAC Address from all devices
- Populate device info on the End User Recording Template
- Ensure all email addresses are complete and accurate – email addresses are the most important component of the spreadsheet since the email address is used to configure end users in Active Directory for MobileIron

End User Last Name	End User First Name	End User Rank/Grade	Entire E-mail Address (do not leave off @mail.mil)	CC/S/A	Major Command & Unit	Apple VPP Email Address (if applicable)	Mobile Device Make and Model	Carrier	Mobile Device OS Version	Device Information: IMEI, Serial # or WiFi MAC
Example 1	John	SES	john.p.doe8.civ@mail.mil	Army	HQDA - USACRC	N/A	Galaxy S5	Verizon	5.1	C0:BD:D1:34:00:00
Example 2	Jane	LTC	jane.z.doe4.mil@mail.mil	Army	HQDA - USACRC	Example_VPP@mail.mil	iPad Air 1	Verizon	9.3.1	C0:BD:D1:40:7E:00
End User Info				Unit Info			Device Info			

DO NOT CHANGE THE FORMAT OF THIS SPREADSHEET
List Values tab highlighted cells I 4-5 & 8 must be complete



End User Recording Template List Values

Ordering

- The second worksheet/tab, titled "List_Values", of the spreadsheet contains the MobileIron labels/policies applied to end users during the Active Directory configuration process
- User Lists missing these selections may be rejected by the CAM Team

A	B	C	D	E	F	G	H	I
1	Mission Partner Level 1			Camera Policies			Mission Partner Device Configurations	
2	AF_AMC_M	Air Mobility Command		DoD_Open_P			Group Type	Group Name
3	AF_ESD_M	Air Force General					Customer Group	
4	AF_GSC_ESD_M	Global Strike Co					Mission Partner Level 1 Service Desk	
5	AF_ACC_M	Air Combat Com					DISA Level 2 Tier II Service Desk	DISA_DECC_OKC_M
6	AF_ANG_ESD_M	Air National Guard					DISA Level 2 Tier III Service Desk	DISA_MA_MPMO_M
7	ARMY_ESD_M	Army General - Includes AFRICOM and SOUTHCOM					Camera Policies	
8	ARMY_ITA_M	Army Pentagon Only - Going Away					App Group(s)	DoD_A
9	CENTCOM_ESD_M	Central Command						
10	DISA_CIO_M	Defense Information Systems Agency						
11	EITSD_ESD_M	WHS/Enterprise Information Technology Services Directorate						
12	EUCOM_ESD_M	Europe Command						
13	JS_ESD_M	Joint Staff						
14	NAVY_ESD_M	Navy General						
15	NORTHCOM_ESD_M	Northern Command						
16	PACOM_ESD_M	Pacific Command						
17	SOUTHCOM_ESD_M	Southern Command						
18	STRATCOM_ESD_M	Strategic Command						
19	TRANSCOM_ESD_M	Transportation Command						
20	DARPA_ESD_M	Defense Advanced Research Projects Agency						
21	DECA_ESD_M	Defense Commissary Agency						
22	DCAA_ESD_M	Defense Contract Audit Agency						

Free-text field that contains CC/S/A and MACOM (e.g., ARMY_AMC_M)

End Users require correct Tier I to be visible in Spaces

DoD_Open_P = Camera On
DISA_P = Camera Off

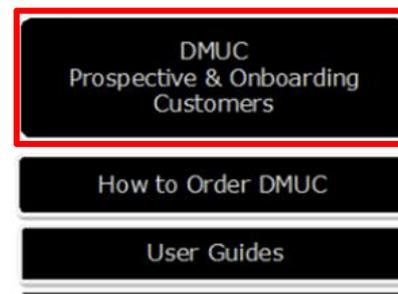
List Values



Funding Mobility Infrastructure Service

Preparation

- Mission Partners must have or obtain a Program Designator Code (PDC) to order Mobility Infrastructure Service in DISA Direct
- The PDC is a 1-6 character code which is authorized by DISA/Chief Financial Executive (CFE) relating to a Line of Accounting
- PDCs are used to outline payment for the product and/or service being ordered
- PDC is billed in arrears at the end of the month for the number of orders in DISA Direct
- Army Mission Partners contact NETCOM G8 (Nancee R. Horn/Elizabeth A. Ashworth) to obtain a PDC
- Other Mission Partners contact CFE to obtain a PDC (see the DMUC Implementation Checklist in the [Mobility User Corner](#) under DMUC Prospective & Onboarding Customers





Obtaining DISA Direct Account

Preparation

- Creating a DISA Direct Account is still done in DISA Direct Order Entry
 - Open a web browser and go to <https://www.disadirect.disa.mil>
 - Click the “CREATE USERID” link under "Registration Center"
 - Complete the information as indicated on the page and click “SUBMIT”

2

- **Registration Center**
 - **Create Userid**
 - Registration
 - Change User Info
 - Central Address Directory

3

DISA Direct
Department of Defense

DISA Direct Home TR Home Track TR CAD ASD

Create Userid

Complete the following and click Submit to establish a userid.

(M) Type Customer:

(M) Agency:

(M) Organization:

If your Agency/Organization is not listed please contact the [DISA Direct Team](#)

(M) Rank/Title:

(M) Last Name: (M) First Name: M:

(M) Password:

(M) Verify Password:

Phone Number: (Enter the phone number components without hyphens, dashes, or special characters.)

Intl Access (6) Area/City (4) Exchange (6) Phone (6) Extension (10)

(M*) Cntrl. Phone:

(M*) DSN Phone:

Pager:

Fax:

(M*) User E-mail:

(M*) Org E-mail:

Class. User E-mail:

Class. Org E-mail:

Select if International Address (Do not select if using an APD, FPO, or US Zip4 Code)

For US Addresses, enter a 5-digit Zip code to retrieve the corresponding city and state.

(M) Address Line 1:

Address Line 2:

City/Institution:

State:

(M) Zip: -

(M) Mandatory field
(M*) One is mandatory for the following
- Cntrl or DSN phone number
- User or Org E-mail

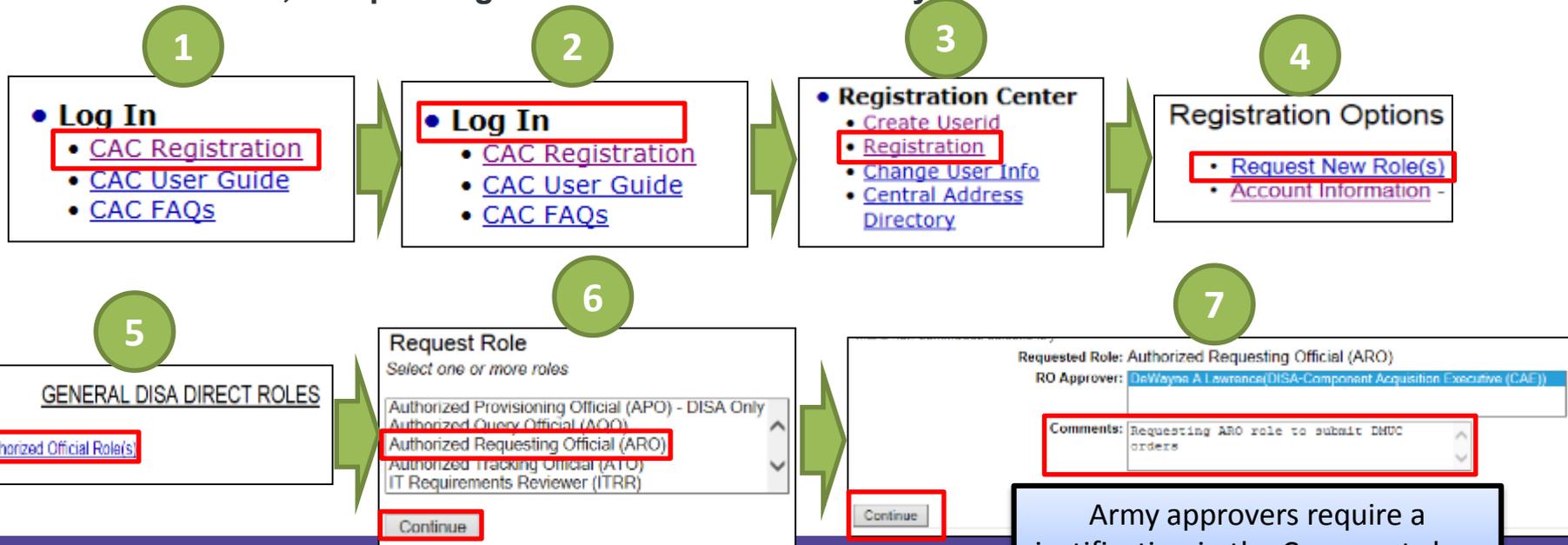
If you do not see your org/unit, contact the DCCC Service Desk 1-844-DISA-HLP (347-2457), option 2 DSN: 312-850-0032, option 2
disa.dccc@mail.mil
disa.scott.conus.mbx.dccc@mail.smil.mil



Obtaining a DISA Direct Role

Preparation

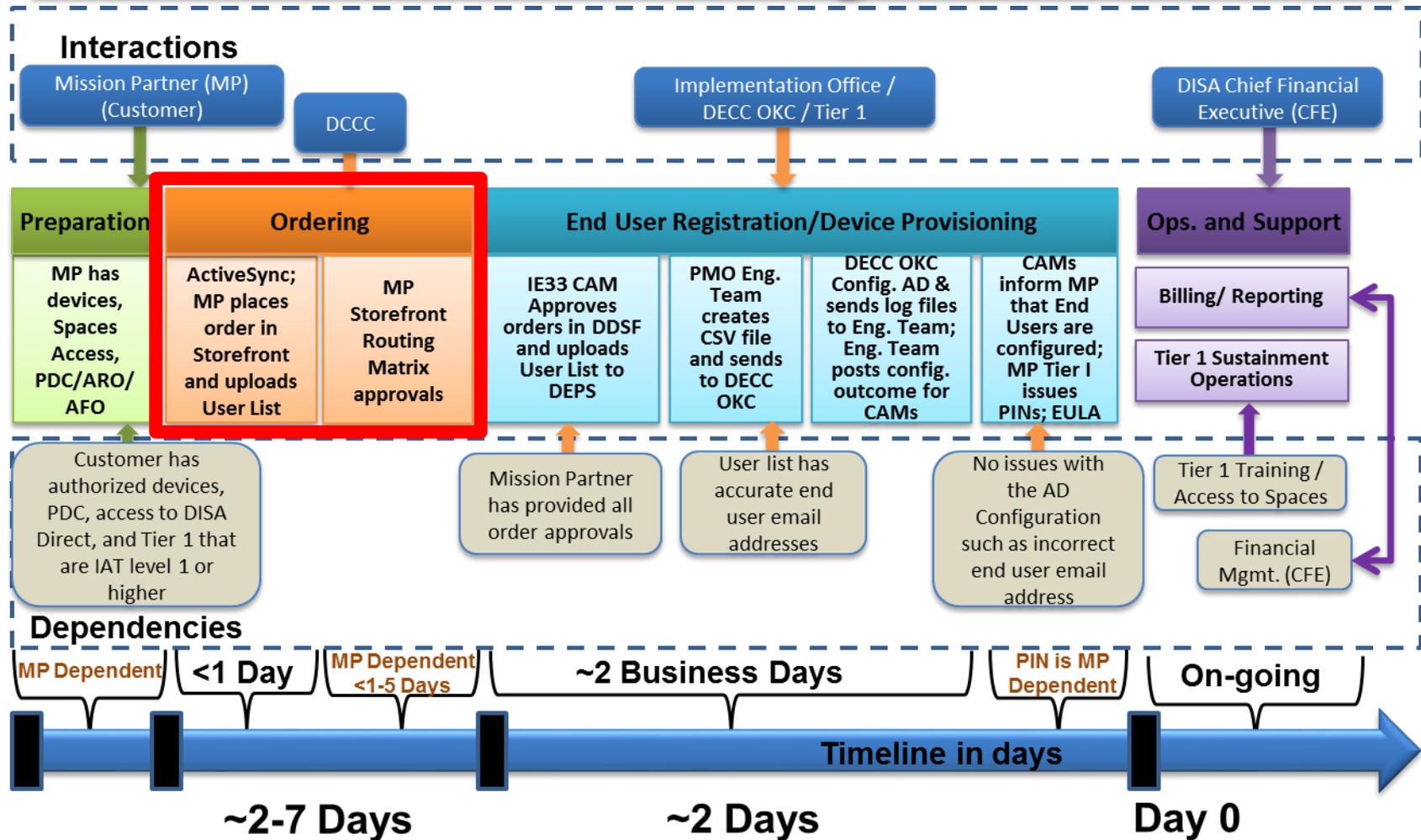
- **Selecting a role to submit Telecommunication Requests in DDSF**
 - Register CAC with DISA Direct
 - Click the “LOG IN” link
 - Click on the “REGISTRATION” link below "Registration Center"
 - Click on “REQUEST NEW ROLE” under "Registration Options"
 - Click on “REQUEST AUTHORIZED OFFICIAL ROLE(S)” under “General DISA Direct Roles”
 - Click on “AUTHIRZED REQUESTING OFFICIAL (ARO)” under “Request Role” and click “CONTINUE”
 - Add comment, “Requesting ARO role to submit Mobility orders” and select “CONTINUE”



Army approvers require a justification in the Comments box



Ordering





DISA Direct Store Front (DDSF) Order

Ordering

- **DDSF allows bulk orders/approvals up to 999 at a time**
- **DDSF DMUC Mobility Service Walkthrough guide is on the User Corner under DMUC Onboarding Customers**



**Contact DCCC Service Desk
for Assistance with DDSF Orders:**
 DCCC Service Desk
 1-844-DISA-HLP (347-2457), option 2
 DSN: 312-850-0032, option 2
disa.dccc@mail.mil
disa.scott.conus.mbx.dccc@mail.smil.mil



End User Recording (User List) Template

Ordering

- When you start the order in Storefront it will generated the Customer Job Order Number (CJON)
- Mission Partner adds the CJON to the spreadsheet and uploads it into DDSF during the Telecommunications Request (TR) process

ARMY - HQDA - USACRC													
DO NOT CHANGE THE FORMAT OF THIS SPREADSHEET													
List_Values tab highlighted cells I 4-5 & 8 must be completed													
End User Last Name	End User First Name	End User Rank/Grade	Entire E-mail Address (do not leave off @mail.mil)	CC/S/A	Major Command & Unit	Apple VPP Email Address (if applicable)	Mobile Device Make and Model	Carrier	Mobile Device OS Version	Device Information: IMEI, Serial # or WiFi MAC	PDC	Customer Job Order Number (CJON)	Notifications: Email addresses to receive end user configuration outcomes from the DISA CAM Team
Example 1	John	SES	john.p.doe8.civ@mail.mil	Army	HQDA - USACRC	N/A	Galaxy S5	Verizon	5.1	C0:BD:D1:34:00:00	A12ABC	SFDDMONYRXXXX	usacrc_helpdesk@mail.mil
Example 2	Jane	LTC	jane.z.doe4.mil@mail.mil	Army	HQDA - USACRC	Example.VPP@mail.mil	iPad Air 1	Verizon	9.3.1	C0:BD:D1:40:7E:00	A12ABC	SFDDMONYRXXXX	usacrc_helpdesk@mail.mil

Order Info

POCs to be notified of configuration outcome



Tracking DISA Direct Storefront Orders

Ordering

- If you enabled email notifications in DISA Direct, you'll get an automated email after each approval
- You can also manually check the approval status:
 - Find your order and select “Addressing and Routing”

page

Type Action	Date Created	Date Modified	Actions
START	29 Jul 2015 11:59:20 UTC	29 Jul 2015 15:17:09 UTC	Addressing and Routing History Manage User List View
START	29 Jul 2015 11:55:02 UTC	29 Jul 2015 15:16:56 UTC	Addressing and Routing History Manage User List View
START	28 Jul 2015 07:17:45 UTC	29 Jul 2015 15:14:41 UTC	Addressing and Routing History Manage User List View
START	29 Jul 2015 12:44:20 UTC	29 Jul 2015 14:38:41 UTC	Addressing and Routing History Manage User List View

- Expand “Routing” to see the approval status

Addressing and Routing

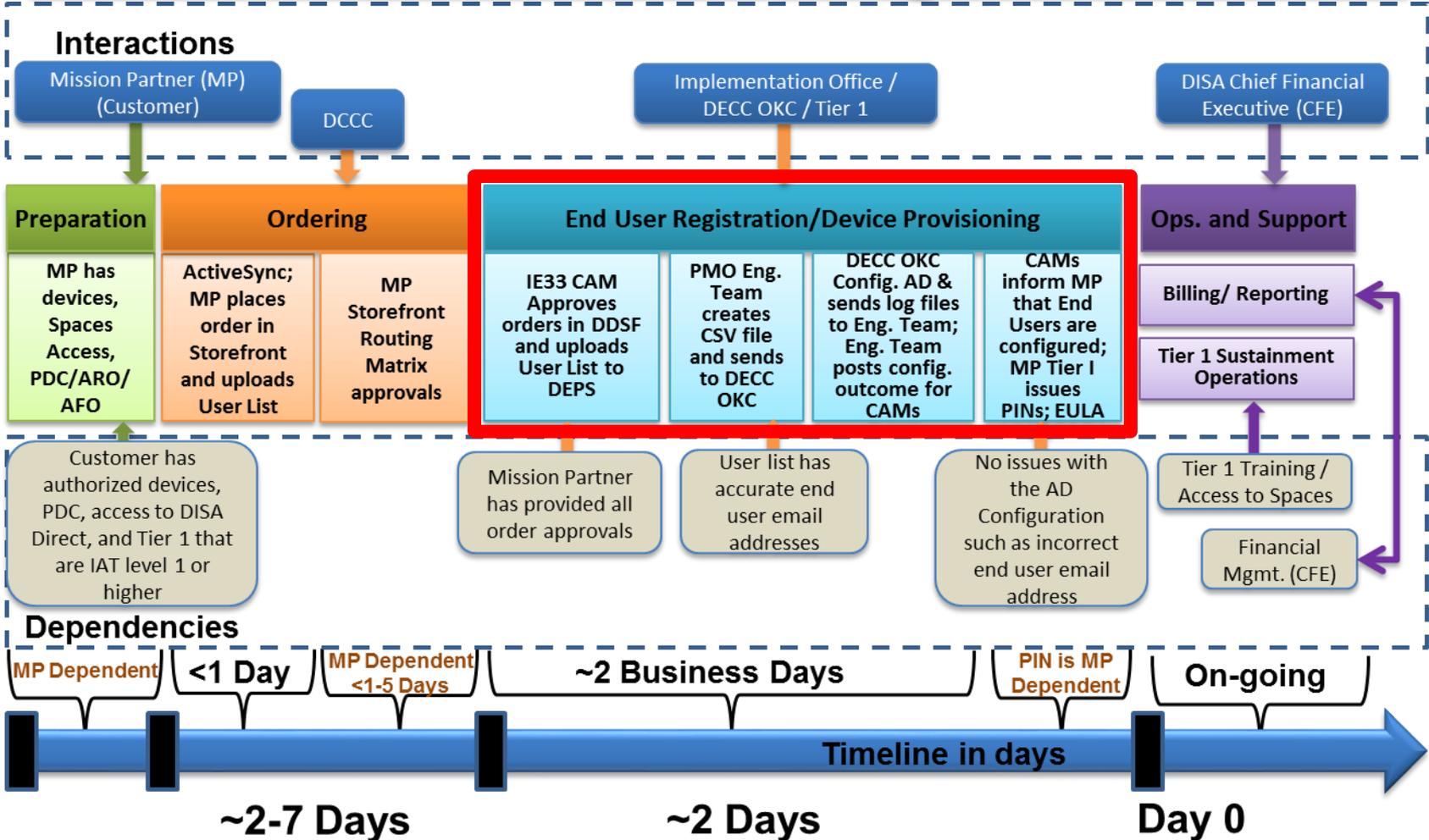
▸ Addressing

▾ **Routing**

- Approval Office #1 - BASECOM - Wireless - Approved: Friday, June 12, 2015 12:42:43 PM
- Approval Office #2 - ARMY-AFO - Approved: Monday, June 15, 2015 11:29:04 AM
- Approval Office #3 - Mobility PMO - Pending: Monday, June 15, 2015 10:29:04 AM



End User Registration/Device Provisioning





End User Configuration Schedule

End User Reg./Device Prov.

- Mobility Customer Account Manager (CAM) is final approver of TR in DDSF and submits End User Recording Template for end-user configuration. Note: the DISA Direct approved message means that your order has been funded and will be submitted for configuration which can take 1 to 2 business days after DDSF order is approved by DISA**

	Monday	Tuesday	Wednesday	Thursday	Friday
Example A	1. CAM: Approve TRs and upload spreadsheet 2. Eng. Team: Pull all lists from across DoD and send configurations (.csv file) to DECC OKC by 1700 hours EST	3. DECC OKC: Implement end user configurations 4. Eng. Team: Receive logs back from DECC OKC, verify logs, and post for CAMs by 1700 hours EST	5. CAM: Inform submitter of end user configuration outcome 6. Customer works with their Tier I Service Desk to obtain PINs (duration is Tier I dependent)		
Example B		1. CAM: Approve TRs and upload user spreadsheet 2. Eng. Team: Pull all lists from across DoD and send configurations (.csv file) to DECC OKC by 1700 hours EST	3. DECC OKC: Implement end user configurations 4. Eng. Team: Receive logs back from DECC OKC, verify logs, and post for CAMs by 1700 hours EST	5. CAM: Inform submitter of end user configuration outcome 6. Customer works with their Tier I Service Desk to obtain PINs (duration is Tier I dependent)	



End User Configuration Schedule (Cont.)

End User Reg./Device Prov.

	Monday	Tuesday	Wednesday	Thursday	Friday
Example C			1. CAM: Approve TRs and upload spreadsheet 2. Eng. Team: Pull all lists from across DoD and send configurations (.csv file) to DECC OKC by 1700 hours EST	3. DECC OKC: Implement end user configurations 4. Eng. Team: Receive logs back from DECC OKC, verify logs, and post for CAMs by 1700 hours EST	5. CAM: Inform submitter of end user configuration outcome 6. Customer works with their Tier I Service Desk to obtain PINs (duration is Tier I dependent)
Example D	5. CAM: Inform submitter of end user configuration outcome 6. Customer works with their Tier I Service Desk to obtain PINs (duration is Tier I dependent)			1. CAM: Approve TRs and upload spreadsheet 2. Eng. Team: Pull all lists from across DoD and send configurations (.csv file) to DECC OKC by 1700 hours EST	3. DECC OKC: Implement end user configurations 4. Eng. Team: Receive logs back from DECC OKC, verify logs, and post for CAMs by 1700 hours EST
Example E	3. DECC OKC: Implement end user configurations 4. Eng. Team: Receive logs back from DECC OKC, verify logs, and post for CAMs by 1700 hours EST	5. CAM: Inform submitter of end user configuration outcome 6. Customer works with their Tier I Service Desk to obtain PINs (duration is Tier I dependent)			1. CAM: Approve TRs and upload spreadsheet 2. Eng. Team: Pull all lists from across DoD and send configurations (.csv file) to DECC OKC by 1700 hours EST



Orgs (Army, SOUTHCOM, AFRICOM and certain others on Army bases) Supported by AESD Only:

End User Reg./Device Prov.

- Once the CAM Team informs you that your end users are configured, you'll need to request PINs for the end users from the Army Enterprise Service Desk (AESD)
 - Go to <https://esd-crm.csd.disa.mil/app/ask>
 - Enter your name and email address
 - Subject: "DMUC New PIN Request"
 - Question: "DMUC New PIN Request [provide your org name]"
 - Upload End User Recording Template you uploaded into Storefront
 - Select "Enterprise Mobility" and "New Device MobileIron PIN Request"
 - Select "OK"
 - Select "Continue" to submit ticket
- PINs issued for end users not configured in Active Directory for MobileIron are not viable
- AESD may require up to 48 hours to issue PINs
- PINs expire after 10 days/240 hours

Submit a ticket to our support team.

First Name *

Last Name *

Email Address *

Subject *

Question *

Attach Documents

 Uploading...

Product



Device Provisioning

End User Reg./Device Prov.

- Mission Partner's local technical person or end user provisions device
- Navigate to the Mobility User Corner (use email cert):
https://disa.deps.mil/ext/cop/dod_mobility/SitePages/UserCornerHome.aspx
- Click on any of the appropriate device type (iOS or Android)
- Download and follow the DMUC Android or iOS Device Setup guide, and EULA

DMUC Prospective & Onboarding Customers	
How to Order DMUC	
User Guides	
DMUC Approved Devices	
iOS Smart Phones	Android Smart Phones
iPhone 4S	Samsung Galaxy S4
iPhone 5/5C/5S	Samsung Galaxy S5
iPhone 6/6 Plus	Samsung Galaxy S6/S6 Edge
iPhone 6S/6S Plus	
iOS Tablets	Android Tablets
iPad 2/3/4	Samsung Note Pro 2.2
iPad Air/Air 2	Samsung Galaxy Note 10.1
iPad Mini/Mini 2 Mini 3/Mini 4	



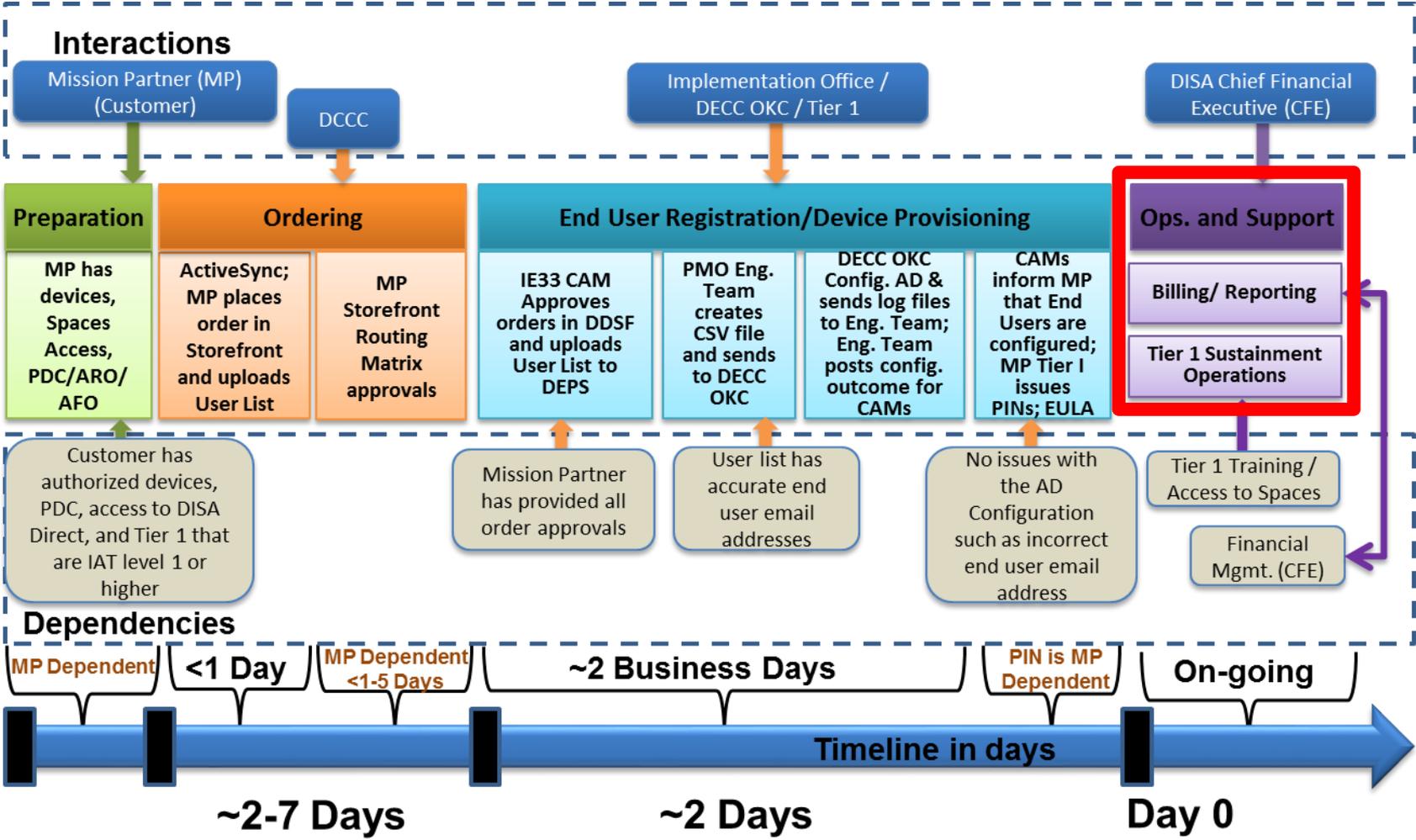
EULA Highlights

End User Reg./Device Prov.

- Obtain a signed DMUC EULA before an end user is given a provisioned device(s) and is stored locally by the Mission Partner
- EULA Highlights:
 - The Apple App Store is not blocked, but only whitelisted apps should be downloaded
 - Downloading 3rd party applications will result in the erasure of the Device memory and applications
 - Bluetooth is permitted, but must use encryption
 - You are not authorized to connect the U.S. Government provided mobile device to any computer/laptop
 - The Cisco AnyConnect VPN must always be enabled and used for all network connections – **only available to DISA personnel at this time**
 - You must adhere to the password complexity policy when you provision the device and this feature must remain enabled
 - Commercial Wi-Fi networking is allowed, if enabled; however, it must be a trusted Wi-Fi network that uses WPA2 security – no open networks



Operations & Support





Service Desk Roles and Responsibilities

Op. & Sup.

- **Mission Partner Level 1 Tier I Service Desk Spaces actions**
 - **Device Management**
 - View Dashboard
 - View Device
 - View Device Details
 - Retire Device
 - Other Device Actions
 - Force Device Check-in
 - Check Compliance
 - Lock Device
 - Unlock Device
 - Unlock Behavior on Android
 - Re-Provisioning Device
 - Android-Only Sub-Menu
 - iOS-Only Sub-Menu
 - Windows-Only Sub-Menu
 - Wipe Device
 - Cancel Wipe
 - Cancel Device Wipe for iOS Devices
 - Cancel Device Wipe for Android Devices
 - Add Device
 - Add a Single Device
 - Registration [PIN] Window
 - Register Multiple Devices
 - Sample .CSV File
 - Add Multiple Devices
 - Export to .CSV for [PINS] Recommended Approach
 - Export to .CSV
 - **Privacy Control**
 - View dashboard
 - View device
 - View device details
 - View apps in device details
 - Locate device
- **Level 1 Tier I escalates to Level 2 Tier II (DECC OKC) for advanced troubleshooting**
- **Level 2 Tier III escalates to Level 2 Tier III (Mobility PMO) as needed**



Ordering Do's and Don'ts

Op. & Sup.

- You do NOT need to contact DISA for approval to implement DMUC
- As of 29 July 2015, End User Recording Template spreadsheets for new orders in Storefront do not need to be submitted to the CAM Team group email
- Each End User Recording Template should only have one bulk order (CJON) in Storefront since it gets uploaded into the system
- You cannot mix PDCs for one bulk order in Storefront – the system is not designed to accept more than one PDC per bulk order
- Additional devices/user end users can be added to an existing CJON by doing a "Change action" as long as the total of devices on spreadsheet is reflected in the order subscription quantity. Highlight the rows in yellow for all additions/changes to the spreadsheet



Sustainment

Op. & Sup.

- **Procedures for changing end users on a device:**
 1. Ensure the Find my iPhone/iPad feature is turned off on Apple devices; wipe device
 2. Mission Partner contacts their Level 1 Tier 1 with Spaces access and requests old device/end user record be retired from the MobileIron console
 3. Mission Partner Level 1 Tier 1 administrator retires the device record
 4. Mission Partner puts old end user in the Notes/Comments column (see example on slide 38), adds new end user, highlight all the rows that have changes, and send the entire spreadsheet for your order the DISA Mobility CAM Team (Disa.meade.ie.mbx.dod-mobility-cam-team@mail.mil)
 5. DISA CAM Team confirms CJON is still being billed in DISA Direct and submits new only end user(s) for configuration
 6. CAM Team notifies submitter that the new end user(s) have been reconfigured
 7. Mission Partner request PIN from their Tier 1 Service Desk
 8. Mission Partner Level 1 Tier 1 issues PIN
 9. End user signs DMUC EULA
 10. Local technical support and/or end user provision the device



Sustainment

Op. & Sup.

- **Procedures in the event a device is lost or stolen:**
 1. End user determines that device is missing
 2. End user or local tier contacts Tier 1 admin to see if device can be located using MobileIron Spaces (location services/GPS must have been enabled for MobileIron during provisioning and be enabled on the device)
 3. If Mission Partner Level 1 Tier 1 administrator with Spaces access cannot locate device, then send a wipe device command via Spaces
 4. Mission Partner Level 1 Tier 1 retires old device/end user record from Spaces
 5. End user or local tier contacts carrier to cancel or suspend service
 6. If not replacing the device, ARO amends total order subscriptions in DDSF order - process ends
 7. If replacing the device, ARO puts old device information in the Notes/Comments column of End User Recording Template, adds the new device information (see example on slide 38), highlights all the rows that have changes, and sends the entire spreadsheet for your order the DISA Mobility CAM Team (Disa.meade.ie.mbx.dod-mobility-cam-team@mail.mil) - the end user is already configured in AD LDS so PIN can immediately be issued
 8. Mission Partner requests PIN from their Tier 1 Service Desk
 9. Mission Partner Level 1 Tier 1 issues PIN
 10. Local technical support and/or end user provision the device



- **Procedures for upgrading or changing device for current end user when TR exists in DISA Direct:**
 1. **ARO puts old device information in the Notes/Comments column of End User Recording Template, adds the new device information (see example on slide 38), highlights all the rows that have changes, and sends the entire spreadsheet for your order the DISA Mobility CAM Team (Disa.meade.ie.mbx.dod-mobility-cam-team@mail.mil) - the end user is already configured in AD LDS so PIN can immediately be issued**
 2. **Mission Partner requests PIN from their Tier 1 Service Desk**
 3. **Mission Partner Level 1 Tier 1 issues PIN**
 4. **Local technical support and/or end user provision the new device**
 5. **Mission Partner contacts their Level 1 Tier 1 with Spaces access and requests the old device/end user record be retired from Spaces**
 6. **Mission Partner Level 1 Tier 1 administrator retires the device account from Spaces**



Sustainment

Op. & Sup.

- **Procedures for discontinuing service for a single device:**
 1. **Mission Partner's Tier 1 Service Desk retires the device from MobileIron**
 2. **Mission Partner Discontinues entire DDSF order if a single subscription order, or does a Change to reduce the number of subscriptions by one for a bulk order in Storefront. If doing a Change, remove the device row from the End User Recording Template spreadsheet and upload into DDSF**



Sustainment

Op. & Sup.

- **Procedures in the RARE event an end user falls out of Active Directory (this happens when an email account is deprovisioned) and loses MobileIron functionality on their device:**
 1. **Mission Partner contacts their Level 1 Tier 1 with Spaces access and requests the old device/end user record be retired from Spaces**
 2. **Mission Partner Level 1 Tier 1 administrator retires the old device/end user record from Spaces**
 3. **Mission Partner highlights the row with impacted end user and send to the entire End User Recording Template to DISA CAM Team (Disa.meade.ie.mbx.dod-mobility-cam-team@mail.mil)**
 4. **DISA CAM Team confirms CJON and device information (IMEI, Serial Number or Wi-Fi MAC Address) is still in a billing status and resubmits end user for configuration**
 5. **CAM Team notifies submitter that the end user has been reconfigured**
 6. **Mission Partner request PIN from their Tier 1 Service Desk**
 7. **Mission Partner Level 1 Tier 1 issues new PIN**
 8. **Local technical support and/or end user provision the new device**



Sustainment Scenarios

Op. & Sup.

1. Existing Device, New End User

New end user needs configured (never had Mobility device)

Remove old end user from spreadsheet, add new end user (see example on next slide)

Send sustainment action to CAM Team; End user is configured (1-2 business days)

Tier I retires old end user/device record; Tier I issues PIN; New End User Signs EULA

2. Existing Device, Existing End User

New end user does not need configured – has/had Mobility device

Remove old end user from spreadsheet, add new end user (see example on next slide)

Send sustainment action to CAM Team – no order approval needed; no configuration needed

Tier I retires old end user/device record; Tier I issues PIN

3. Existing End User, New Device

Order already approved in DISA Direct

No action in DDSF; Update device info on spreadsheet (see example on next slide)

Send sustainment action to DISA CAM Team; no end user configuration required

Tier I retires any old end user/device record; Tier I issues PIN



Sustainment User List Modifications

Op. & Sup.

- End User Recording Template modifications for changing out end users on a current device

1	DO NOT CHANGE THE FORMAT OF THIS SPREADSHEET						
2	DO NOT CHANGE THE FORMAT OF THIS SPREADSHEET						
3	<u>End User Last Name</u>	<u>End User First Name</u>	<u>End User Rank/Grade</u>	<u>Entire E-mail Address (do not leave off @mail.mil)</u>	<u>CC/S/A</u>	<u>Notifications: Email addresses to receive end user configuration outcomes from the DISA CAM Team</u>	<u>Notes/Comments</u>
4	Example 1	John	SFS	john.p.doe8.civ@mail.mil	Army	usacrc_helpdesk@mail.mil	
5	Example 2	Rusty	LTC	rusty.a.nail.mil@mail.mil	Army	usacrc_helpdesk@mail.mil	Old End User: Jane.z.doe4.mil@mail.mil

- End User Recording Template modifications when changing devices for current end user

ARMY - HQDA - USACRC									
DO NOT CHANGE THE FORMAT OF THIS SPREADSHEET									
_Values tab highlighted cells I 4-5 & 8 must be completed									
<u>Major Command & Unit</u>	<u>Apple VPP Email Address (if applicable)</u>	<u>Mobile Device Make and Model</u>	<u>Carrier</u>	<u>Mobile Device OS Version</u>	<u>Device Information: IMEI, Serial # or WiFi MAC</u>	<u>PDC</u>	<u>Customer Job Order Number (CJON)</u>	<u>Notifications: Email addresses to receive end user configuration outcomes from the DISA CAM Team</u>	<u>Notes/Comments</u>
HQDA - USACRC	N/A	Galaxy S5	Verizon	5.1	C0:BD:D1:34:00:00	A12ABC	SFDDMONYRXXX	usacrc_helpdesk@mail.mil	
HQDA - USACRC	Example_VPP@mail.mil	iPad Air 2	Verizon	9.3.1	DD:BD:D1:40:7E:22	A12ABC	SFDDMONYRXXX	usacrc_helpdesk@mail.mil	Old Device: iPad Air 1 C0:BD:D1:40:7E:00



Questions?

- **Email Mobility Customer Account Manager (CAM) Team:**
Disa.meade.ie.mbx.dod-mobility-cam-team@mail.mil
- **CAM Team Commercial Number: 301-225-2390**



DEFENSE INFORMATION SYSTEMS AGENCY
The IT Combat Support Agency

UNITED IN SERVICE TO OUR NATION