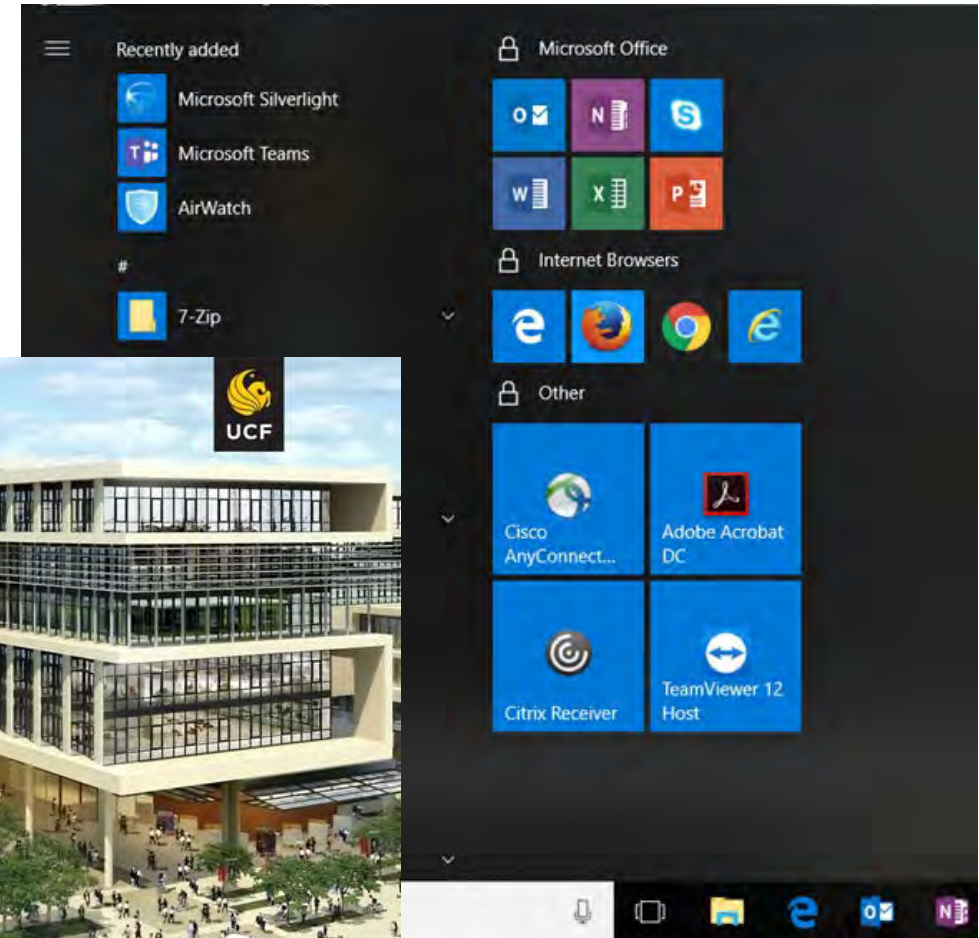
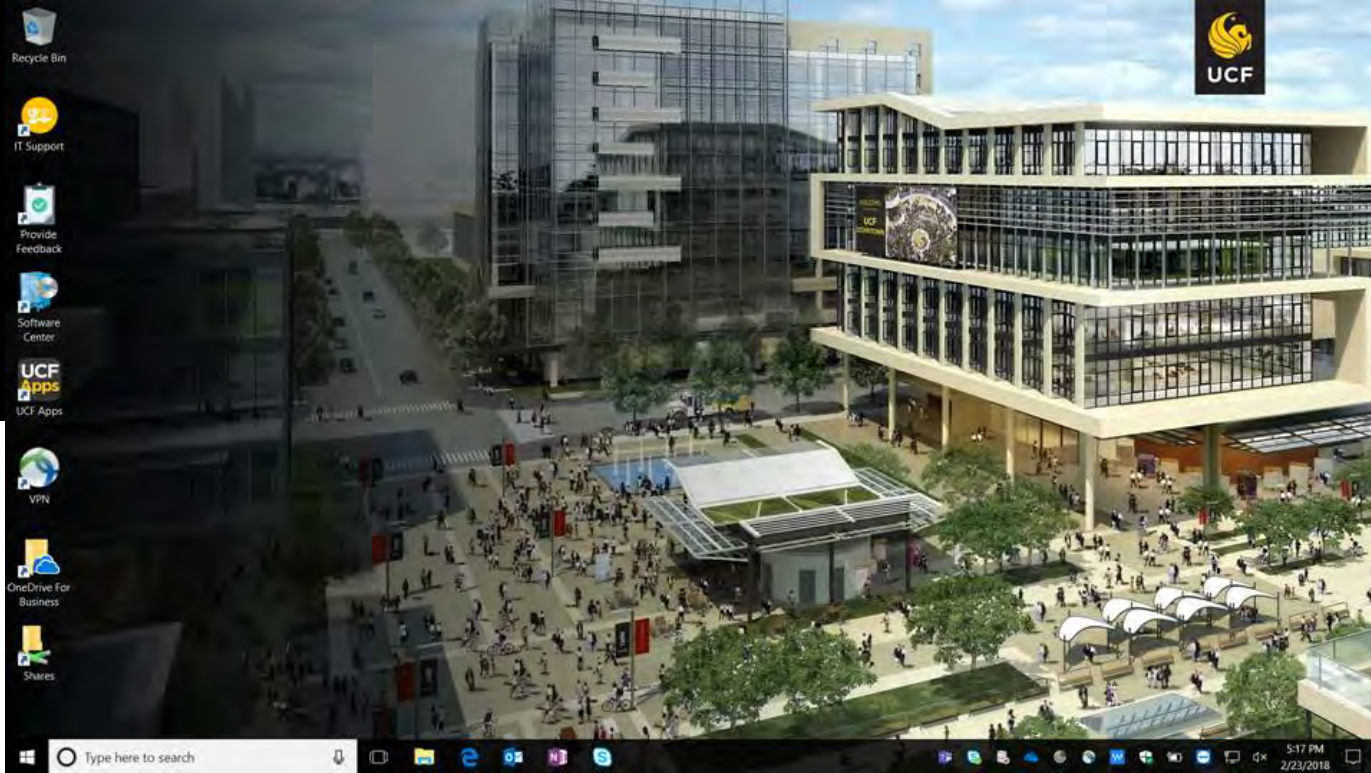
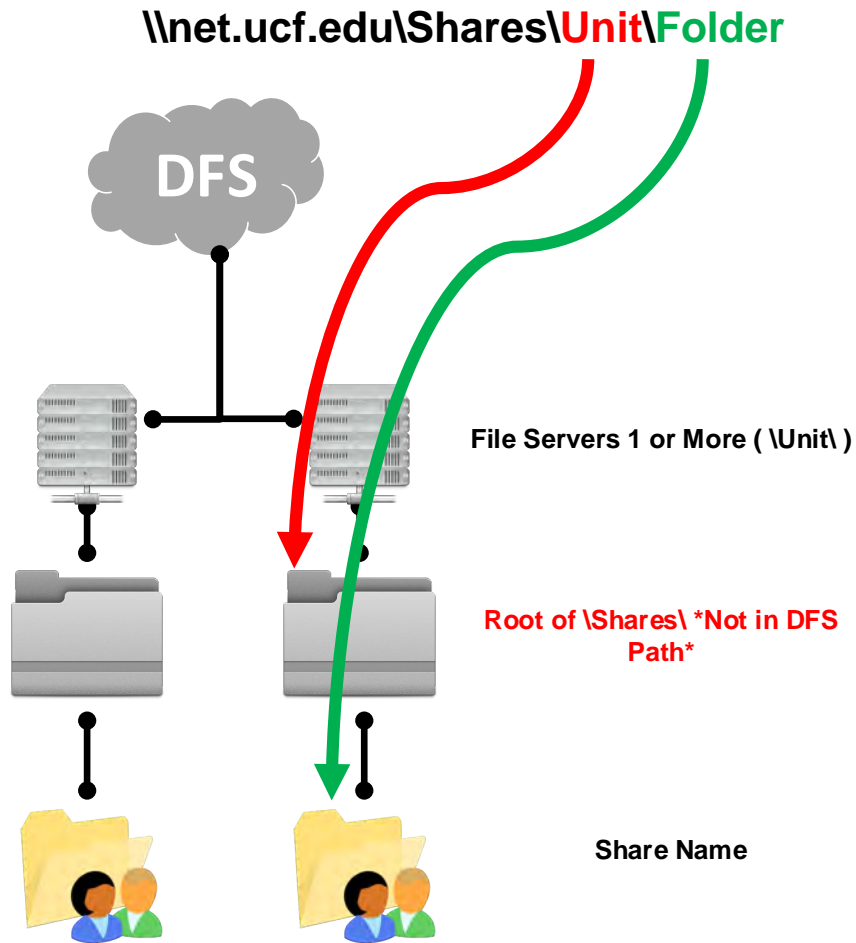


All content on the following slides are for technical reference and are not part of the Kickoff Meeting Presentation

Branding Example



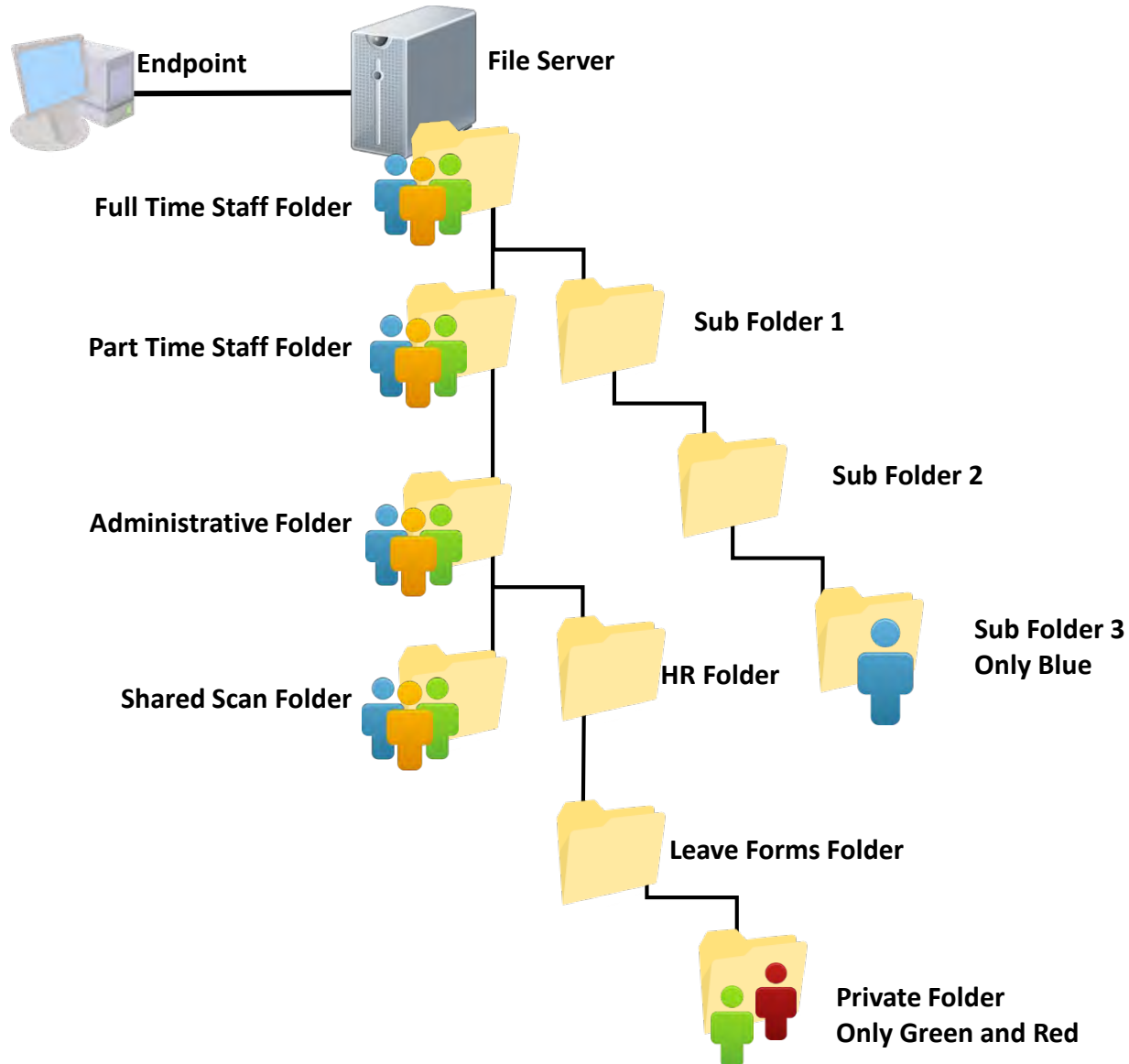
File Structure for Shares



Technical Specifications

- `\\net.ucf.edu\Shares\Unit\Dept Prefix - Folder Share`
 - Department Prefix can be omitted in the folder if it is for multi-departmental use
 - Inter-unit shares will be under a “UCF” namespace.
`\\net.ucf.edu\Shares\UCF\Project or Folder Name`
- **Permissions will only exist at root of each Folder Share**
- Single, Shared GPO *can* be used that creates Desktop Shortcut to “`\\net.ucf.edu\Shares`”
 - Desktop Shortcut Name will be “Shares”
- No Mapped Drives unless approved
- Default Quota Size will be 50GB per root level share
 - Can be adjusted as desired by Unit that is financially responsible for the storage being used.
- Quota Warnings and Email Messages will be automatically to Engineering team for follow up action
- Access Based Enumeration will be enabled by default
- Quota and Usage Reporting can be requested at any time, or set to automatically be sent via email at desired intervals
- VSS options will be available (cost permitting) for self-service data recovery by the client
- Only inherited permissions on subfolders and files
- Default Security Groups will be Created : “Read Only” and “Read, Write, Delete”
- No ‘Full Control’ rights to clients (Deny ability to change permissions)

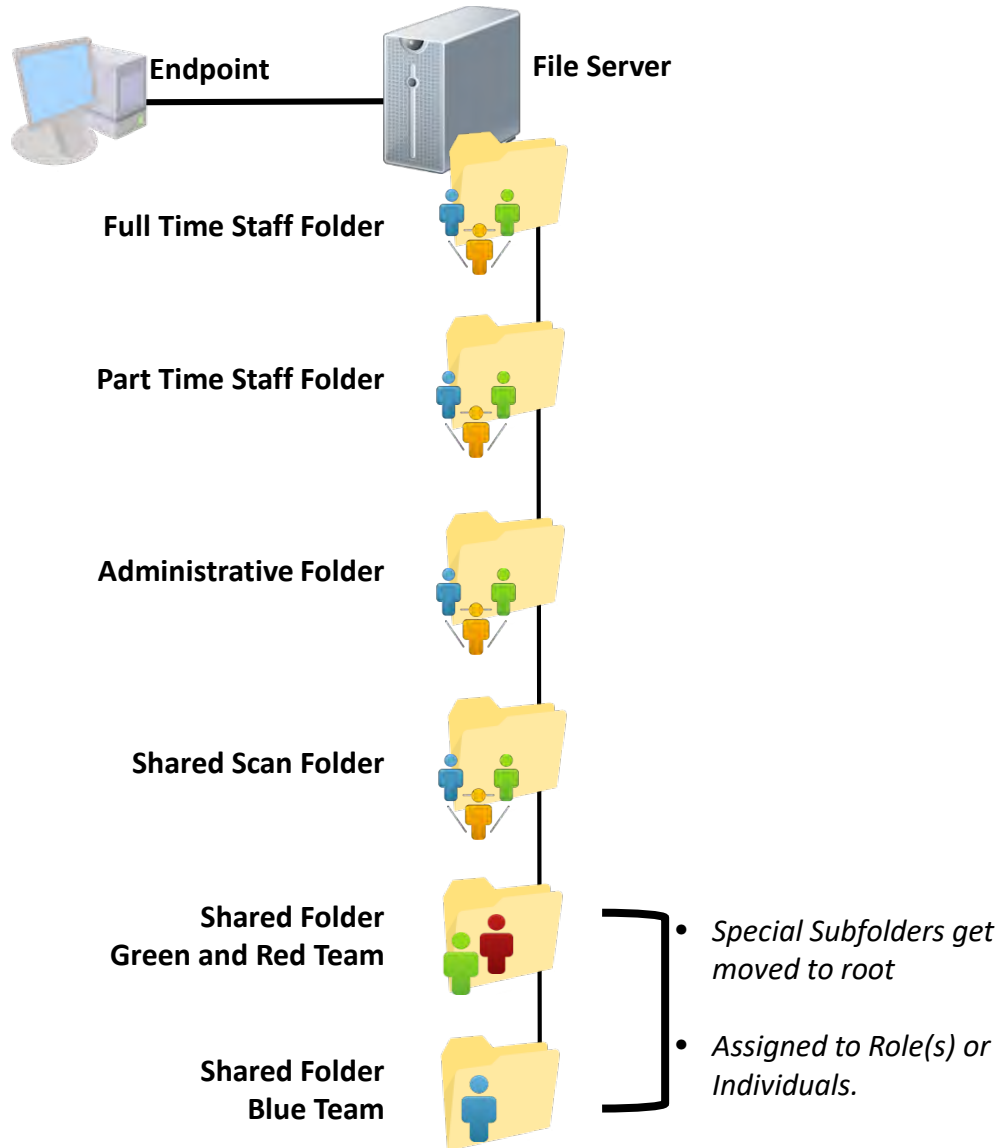
File Structure for Shares - Existing



Some of the concerns for Existing Shared or Group Folder structures include:

- Complex and Undocumented user permissions
- Unstructured and individually provisioned folders
- Higher likelihood of duplicate data.
 - Occupying additional storage incurs additional cost
- Lack of standardization in the method used to implement the shared environments results in increased response time for any related incidents or request tickets submitted.

File Structure for Shares - Recommended

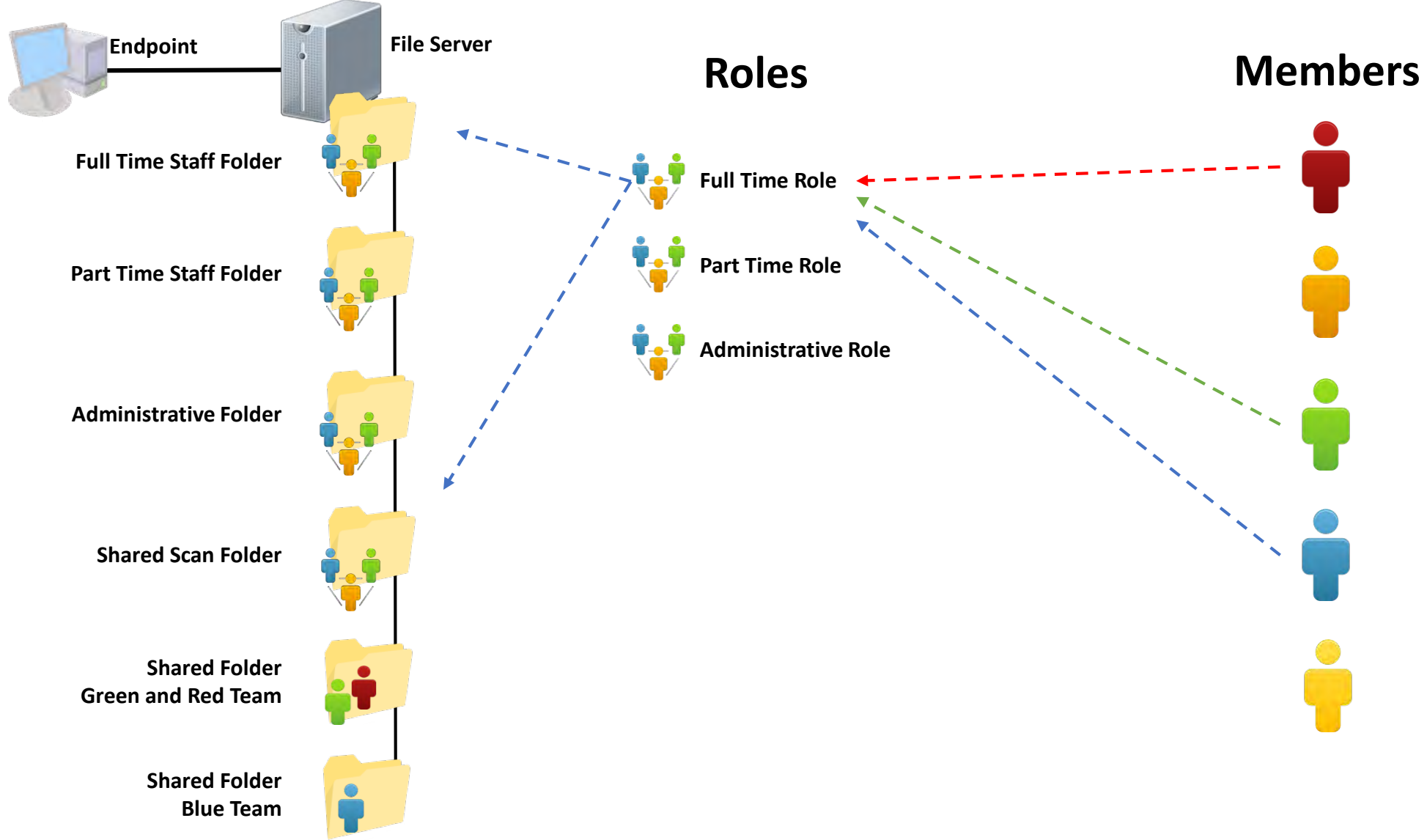


Some of the benefits for the recommended Shared or Group Folder structures include:

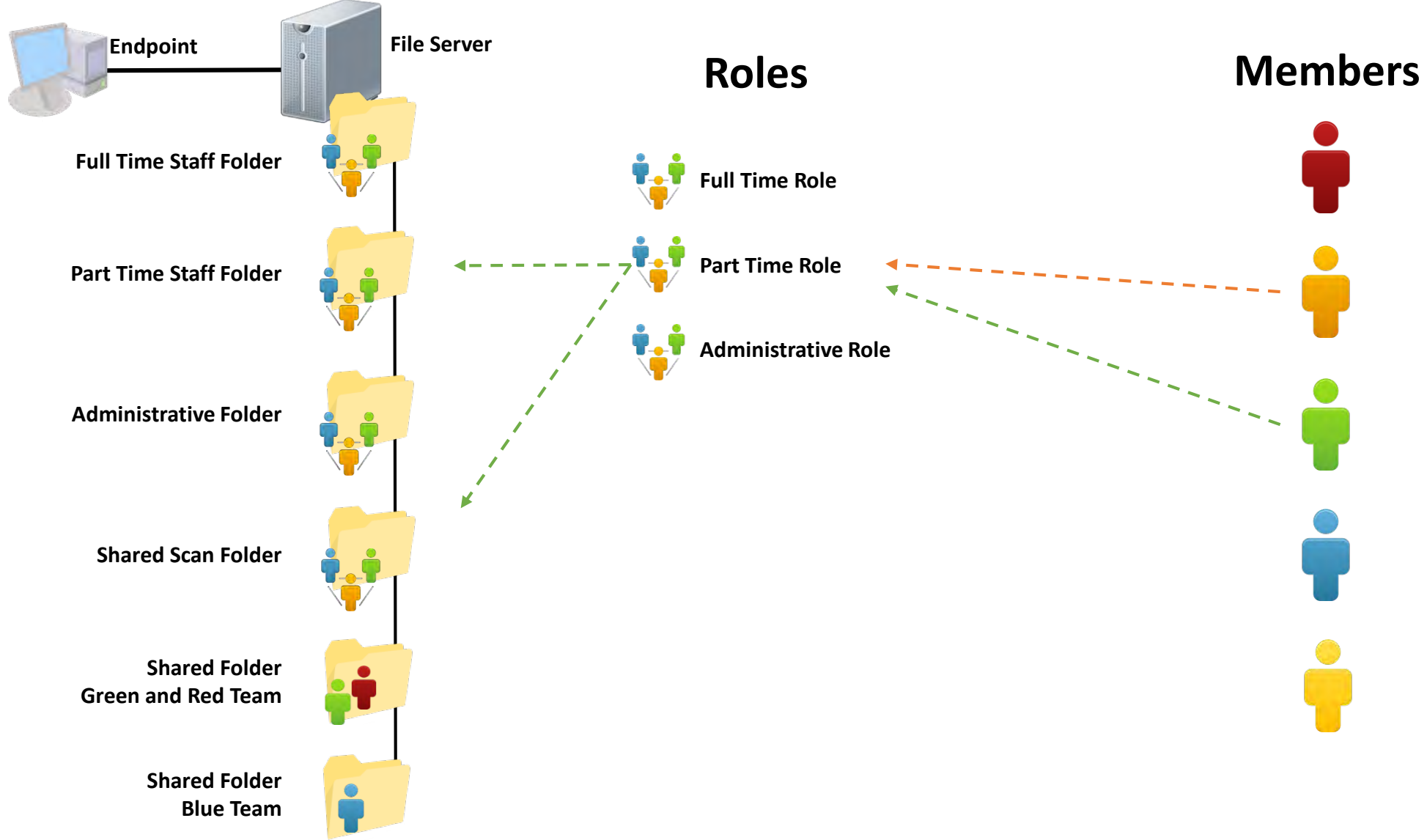
- Simplified and Flat Permission Structure
- ★ Role-Based Access (***Role Names Defined by the Business***)
 - “Role-First” approach. Increases efficiency when hiring new staff or adding new root-level folders
 - **Individual Folder Access (Read/Write, Read Only) can still be given if a role doesn’t apply.***
- Structured and Automated Provisioning
- Self-Documenting based on Security Group Descriptions
- Standardized method will lead to increased response time with a new request or incident is submitted.
- Access Based Enumeration (ABE)
 - You will only see the folders you have access to.

****Enough Individuals assigned to a folder may get transitioned into a role***

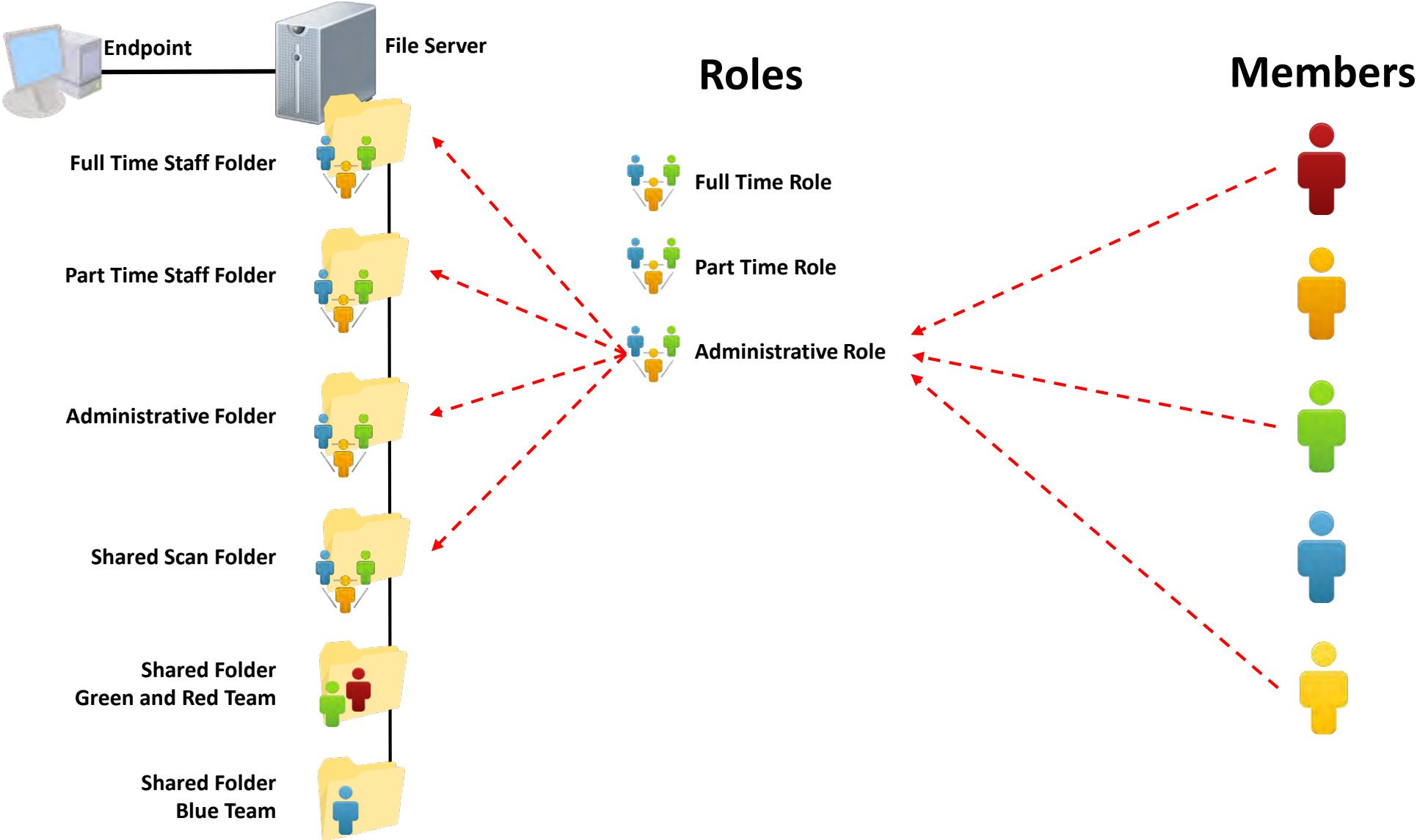
Full Time Role Example



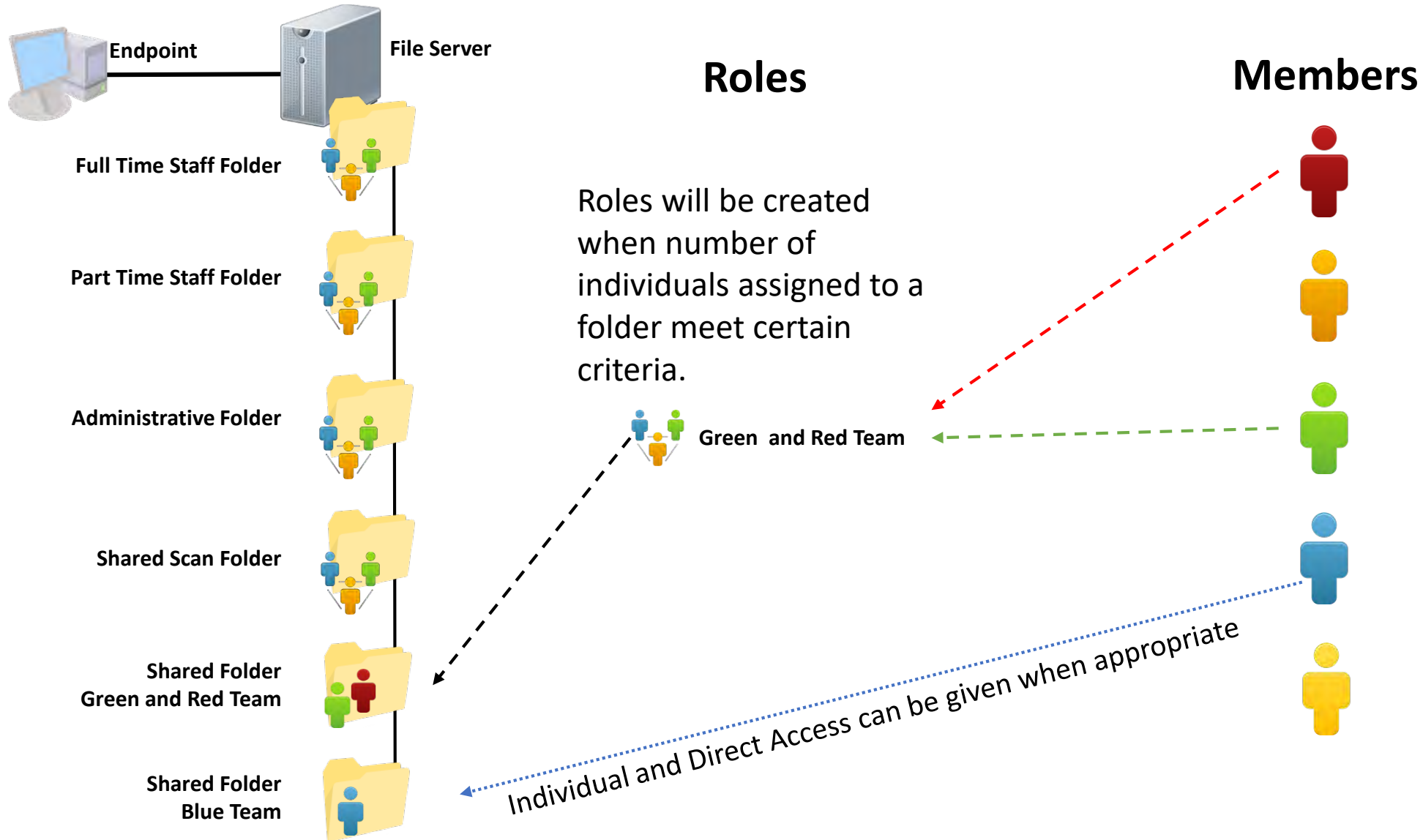
Part Time Role Example



Administrative Role Example



Individuals or New Roles Example



Roles & Resources Info Capture

Format Painter | Clipboard | Font | Alignment | Number | Formatting | Table | Styles | Cells | Filter | Select | Clear | Editing

113

Information Technology UCF

Roles & Resources Organization Tool

Auto Create Sheets From Selection

Note: Please save the file as a "macro-enabled worksheet" before use.

Roles	Description	Folder Resources	Location	Printer Resources	Location	Other
Example Role 01	Demo Role Description	Example 1	\\net.ucf.edu\dept\server\share\1	printer 1	\\printershare1	Test Resource 1
Example Role 02	Demo Role Description	Example 2	\\net.ucf.edu\dept\server\share\2	printer 2	\\printershare2	
Example Role 03	Demo Role Description	Example 3	\\net.ucf.edu\dept\server\share\3	printer 3	\\printershare3	
Example Role 04	Demo Role Description	Example 4	\\net.ucf.edu\dept\server\share\4	printer 4	\\printershare4	
Example Role 05	Demo Role Description	Example 5	\\net.ucf.edu\dept\server\share\5			
		Example 6	\\net.ucf.edu\dept\server\share\6			

Roles & Resources Organization Tool

Example Role 04

Role Member Name	NID	Folder Resources	Access	Printer Resources	Access
User Red	rd985872	Example 1	Read-Write	printer 1	Quota Access
User Blue	bl4932243	Example 2		printer 2	
User Green	gr8392245	Example 3	Read-Write	printer 3	Monochrome Only
		Example 4		printer 4	
		Example 5			
		Example 6	Read Only		

Master Resource List | Example Role 04

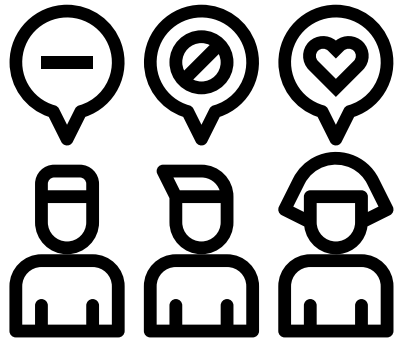




OneDrive
for Business

Migration Options

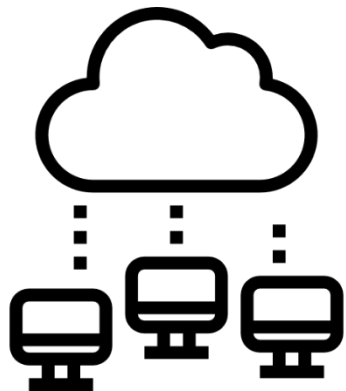
Migration Options (Preview)



Option 1 - User Based Migration



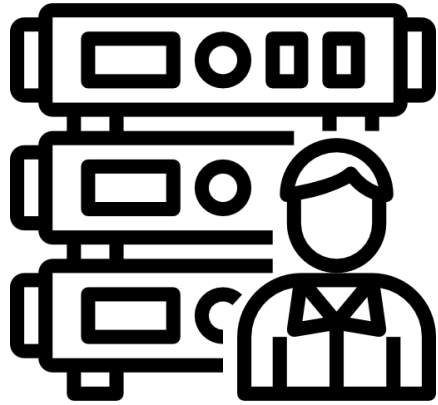
-  • Can be done by the user (manually)
- SharePoint Migration Tool availability for semi-auto migration
-  • Not Scalable
- Assistance may not be immediately available
- If Scheduled with Technical staff, can take years to complete

Option 2 - Device Based Migration



-  • Automated
- Little-to-no user interaction required
- Ideal for Non-Redirected Data
-  • Hardware Storage Requirements on Endpoint
- OS Version Requirements on Endpoint
- Risk of Data loss in Transfer from File Server back to Endpoint

Proof of Concept (Preview)



Option 3 – Server Based Migration



- SharePoint Migration Tool
- Direct from Source Migration
- Scalable and Sustainable



- Will Require Workflow to be Developed Internally (UCF IT)
- Permission Changes will be required
- Requires Testing and POC for Validity

Streamlined Client Experience Project

- Unified Task Sequence (SDP) (R1)
- DHCP Reservations / Dynamic Areas (SDP) (R1)
- Microsoft Office Click-to-Run (C2R) (R1)
- Jamf Management for macOS (R1)
- Print Server Naming Standards & Papercut (SDP) (R2)
- Hardware Refresh Plan or Implementation (SDP) (R2)
- Software Refresh Plan or Implementation (SDP) (R2)
- Remote Support Tool Implementation (SDP) (R2)
- “Mobile First” User Experience when possible (R2)
- AD Reorg or Move (Moran) (R3)
- File Redirection for Desktop and Docs (SDP) (R3)
- Baseline DDS Managed GPOs (SDP) (R3)
- Baseline DDS Managed SCCM Client Settings (R3)
- *MDM management for iOS devices when possible*
- *PST Migration to Exchange Online*
- *Standardized DFS paths Users & Shares (SDP)*
- *Removal of non-approved client admin access (SDP)**
- *Migrate Data to Secret Server*
- *Migration to SCCM U08*
- *Import all Zone Specific Information into Knowledge*
- *All new hardware from UCF IT Product Catalog (SDP)*
- *Service Now Catalog Item Consolidation*
- **Minimum .25 FTE commitment to DDS*

Streamlined Client Experience Project

Round 1

1. **Unified Task Sequence (SDP) (R1)**
2. **DHCP Reservations / Dynamic Areas (SDP) (R1)**
3. **Microsoft Office Click-to-Run (C2R) (R1)**
4. **Jamf Management for macOS (R1)**

Round 2

5. **Print Server Naming Standards & Papercut (SDP) (R2)**
6. **Hardware Refresh Plan or Implementation (SDP) (R2)**
7. **Software Refresh Plan or Implementation (SDP) (R2)**
8. **Remote Support Tool Implementation (SDP) (R2)**
9. **“Mobile First” User Experience when possible (R2)**

Round 3

10. **AD Reorg or Move (Moran) (R3)**
11. **File Redirection for Desktop and Docs (SDP) (R3)**
12. **Baseline DDS Managed GPOs (SDP) (R3)**
13. **Baseline DDS Managed SCCM Client Settings (R3)**

Established Standard / Already Approved

14. *MDM management for iOS devices when possible*
15. *PST Migration to Exchange Online*
16. *Standardized DFS paths Users & Shares (SDP)*
17. *Removal of non-approved client admin access (SDP)**
18. *Migrate Data to Secret Server*
19. *Migration to SCCM U08*
20. *Import all Zone Specific Information into Knowledge*
21. *All new hardware from UCF IT Product Catalog (SDP)*
22. *Service Now Catalog Item Consolidation*

**Minimum .25 FTE commitment to DDS*

Round 1

1. Unified Task Sequence (SDP) (R1)

- Establish and Standardize all of the endpoint operating system deployment with a single task sequence to be adopted by all of Cohort 1 and 2 within UCF IT. All of the deskside zones will need to participate in it's creation, provide input on future improvement as well as work together to adopt the standard process, procedure and technology.

2. DHCP Reservations / Dynamic Areas (SDP) (R1)

- Per the Service Design Package (SDP) Document, All of the Cohort 1 and Cohort 2 areas should have clearly defined VLAN and DHCP Scopes, with a focus on locking down and securing the Faculty and Workstation areas with reservation-only IPs. Adoption is expected of all UCF IT Supported endpoint areas

3. Microsoft Office Click-to-Run (C2R) (R1)

- As part of the Streamline Client Experience Project (SCEP), It is important that all of the UCF IT Supported Endpoints are using the latest version of Office (Office 365 Pro Plus) before Fall of 2019. The Skype 2019 voice services will only function properly with the latest build of Office on the endpoint. This project is designed to assist the Cohort 1 and 2 deskside zones with migrating from previous builds of office (2016 MSI and Previous) to the latest Office 365 version using Click-to-Run installation technology

4. Jamf Management for macOS (R1)

- JAMF is up for renewal and renegotiation with the vendor, in which moving the platform to the cloud is currently a possibility. Aside from moving the JAMF management platform to the cloud, it will be important to provide parity of services and settings to JAMF devices the same as we are providing currently with SCCM or will provide with Intune in the future. JAMF is the primary management platform for macOS and Apple devices.

Unified Task Sequence (SDP) (R1)

SDP Alignment

- Supported OS (p.19)
- Data Encryption (p.38)
- Software Delivery Methods (p.20)
- Software Lifecycle (p.17)
- Automated Software Deployment Criteria (p.21)

Unified Task Sequence (SDP) (R1)

UTS Onboarding Process

- **DDS presents the onboarding unit with information about the UTS**
 - Summary of UTS and its limitations
- **Information is gathered from the unit**
 - *Qualtrics Survey*
 - Brief description of onboarding unit's entire deployment process
 - Staging OU for onboarding unit
 - Onboarding unit's software requirements (3 tiers)
 - Other Unit/zone/departmental specific post OS deployment steps

- *Automated information Gathering (SCCM report or PowerShell Script)*
 - List of PC models to be managed
 - Software titles (supplemental to survey)
- *Onboarding unit action required*
 - Grant DDS team access to current task sequences
- **DDS makes appropriate changes to begin managing the unit's OSD**
 - DDS Internal Checklist

Unified Task Sequence (SDP) (R1)

Software and Driver Deployment

- **3 Tiers**
 - Tier 1 – Required for all UCF IT
 - *Adobe Acrobat Pro DC 2018 , Microsoft Office 365 Pro Plus C2R*
 - *Cisco AnyConnect VPN Client for Mobile Devices*
 - Tier 2 – Required for onboarding unit
 - Tier 3 – Optional for support zone (Software catalog)
 - **Recommended Required Deployments to Staging or All Unit Device Collection**
- Auto Apply Drivers in conjunction with Dell Command Update
- User State Migration Tool (USMT)

Unified Task Sequence (SDP) (R1)

```
Host Name:                MININT-79H9VKM
Computer:                 Dell Inc. OptiPlex 7060 (1.0.20)
Serial #:                 J8MLCP2
BIOS UUID:                4C4C4544-0038-4D10-804C-CAC04F435032
Processor:                Intel(R) Core(TM) i5-8500 CPU @ 3.00GHz
System RAM:               8192 MB
IPv4 Address:
MAC Address:              54:BF:64:5C:E1:43
Network Cards:            Intel(R) Ethernet Connection (7) I219-LM
Fixed Disk Model (Size):  KXG50ZNV256G NVMe TOSHIBA 256GB (238 GB)
```

Unified Task Sequence (SDP) (R1)

UCF | **Information Technology**

Microsoft System Center Configuration Manager

Task Sequence Wizard

Welcome to the Task Sequence Wizard

This media is not password protected. Click next to continue.

Password:

< Previous Next > Cancel

Host Name:
Computer:
Serial #:
BIOS UUID:
Processor:
System RAM:
IPv4 Address:
MAC Address: (none)
Network Cards: (none)
Fixed Disk Model (Size): KXG50ZNV256G NVMe TOSHIBA 256GB (238 GB)

Unified Task Sequence (SDP) (R1)

UCF Information Technology

Microsoft System Center Configuration Manager

Task Sequence Wizard

Select a task sequence to run.

Task sequences:

Name	Description
UCF Unified Task Sequence	
UCF Unified Task Sequence - DEV	

Host Name:
Computer:
Serial #:
BIOS UUID:
Processor:
System RAM:
IPv4 Address:
MAC Address: (none)
Network Cards: (none)
Fixed Disk Model (Size): KXG50ZNV256G NVMe TOSHIBA 256GB (238 GB)

< Previous Next > Cancel

Unified Task Sequence (SDP) (R1)

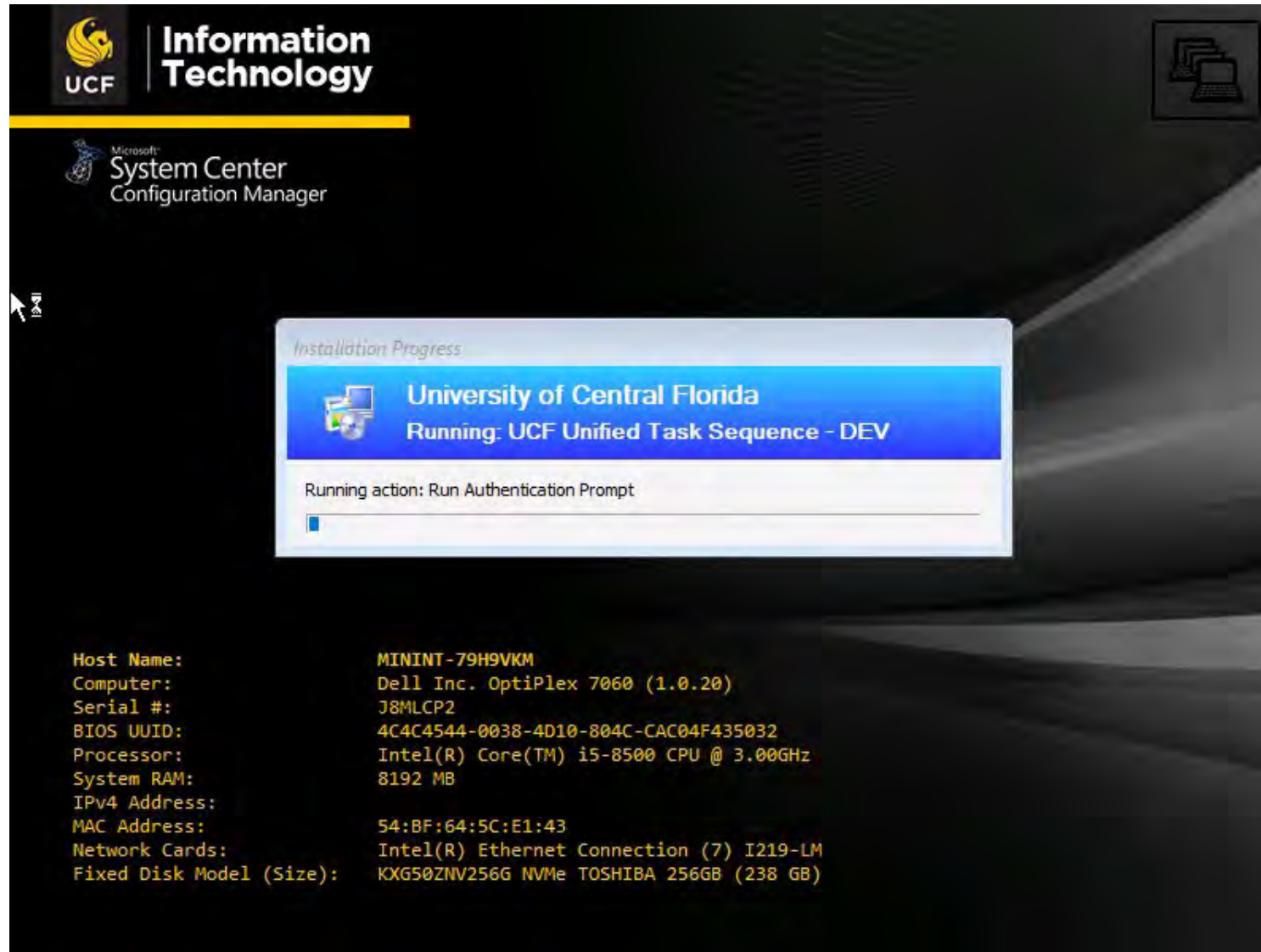
The screenshot shows a Windows Task Sequence Wizard dialog box titled "Task Sequence Wizard" with a close button (X) in the top right corner. The main heading is "Resolving Task Sequence Dependencies". Below the heading, the text reads "Wait while the policy is downloaded and content location is verified". A progress bar is visible, with the text "Resolving selected task sequence dependencies ..." above it. At the bottom of the dialog box, there are three buttons: "< Previous", "Next >", and "Cancel".

UCF Information Technology

Microsoft System Center Configuration Manager

Host Name:
Computer:
Serial #:
BIOS UUID:
Processor:
System RAM:
IPv4 Address:
MAC Address: 54:BF:64:5C:E1:43
Network Cards: Intel(R) Ethernet Connection (7) I219-LM
Fixed Disk Model (Size): KXG50ZNV256G NVMe TOSHIBA 256GB (238 GB)

Unified Task Sequence (SDP) (R1)



UCF | **Information Technology**

Microsoft System Center Configuration Manager

Installation Progress

University of Central Florida
Running: UCF Unified Task Sequence - DEV

Running action: Run Authentication Prompt

Host Name: MININT-79H9VKM
Computer: Dell Inc. OptiPlex 7060 (1.0.20)
Serial #: J8MLCP2
BIOS UUID: 4C4C4544-0038-4D10-804C-CAC04F435032
Processor: Intel(R) Core(TM) i5-8500 CPU @ 3.00GHz
System RAM: 8192 MB
IPv4 Address:
MAC Address: 54:BF:64:5C:E1:43
Network Cards: Intel(R) Ethernet Connection (7) I219-LM
Fixed Disk Model (Size): KXG50ZNV256G NVMe TOSHIBA 256GB (238 GB)

Unified Task Sequence (SDP) (R1)

The screenshot shows the SCCM OS Deployment Authenticator dialog box. The dialog box has a title bar that reads "SCCM OS Deployment Authenticator". Below the title bar, the main text says "SCCM OS Deployment Authenticator" and "Enter valid credentials and FQDN, hit Submit to continue, or hit Cancel to quit". There are three input fields: "Username:" with the value "nidadmin", "Password:" with a masked password of ten dots, and "Domain:" with the value "net.ucf.edu". At the bottom right of the dialog box are two buttons: "Submit" and "Cancel".

In the background, the Microsoft System Center Configuration Manager console is visible. The top left corner shows the UCF Information Technology logo. Below it, the Microsoft System Center Configuration Manager logo is present. At the bottom left, there is a list of system information:

```
Host Name:  
Computer: Dell Inc. OptiPlex 7060 (1.0.20)  
Serial #: J8MLCP2  
BIOS UUID: 4C4C4544-0038-4D10-804C-CAC04F435032  
Processor: Intel(R) Core(TM) i5-8500 CPU @ 3.00GHz  
System RAM: 8192 MB  
IPv4 Address:  
MAC Address: 54:BF:64:5C:E1:43  
Network Cards: Intel(R) Ethernet Connection (7) I219-LM  
Fixed Disk Model (Size): KXG50ZNV256G NVMe TOSHIBA 256GB (238 GB)
```

Unified Task Sequence (SDP) (R1)

UCF Information Technology

Microsoft System Center Configuration Manager

Task Sequence Wizard

Welcome to the Task Sequence Wizard

This media is not password protected. Click next to continue.

Password:

< Previous Next > Cancel

Host Name:
Computer:
Serial #:
BIOS UUID:
Processor:
System RAM:
IPv4 Address:
MAC Address: (none)
Network Cards: (none)
Fixed Disk Model (Size): KXG50ZNV256G NVMe TOSHIBA 256GB (238 GB)

Unified Task Sequence (SDP) (R1)

The screenshot displays the Microsoft System Center Configuration Manager interface. At the top left, the UCF Information Technology logo is visible. Below it, the 'System Center Configuration Manager' title is shown. The main content area features a blue 'Installation Progress' window. This window has a header with the UCF logo and the text 'University of Central Florida Running: UCF Unified Task Sequence - DEV'. Below the header, it indicates the current action: 'Running action: Use Toolkit Package'. A progress bar shows three blue segments. Below the progress bar, it states 'Downloading ServerManager.xml (2% complete)' with a single blue segment in its progress bar. At the bottom of the screen, system information is listed in a key-value format.

Host Name: MININT-79H9VKM
Computer: Dell Inc. OptiPlex 7060 (1.0.20)
Serial #: J8MLCP2
BIOS UUID: 4C4C4544-0038-4D10-804C-CAC04F435032
Processor: Intel(R) Core(TM) i5-8500 CPU @ 3.00GHz
System RAM: 8192 MB
IPv4 Address:
MAC Address: 54:BF:64:5C:E1:43
Network Cards: Intel(R) Ethernet Connection (7) I219-LM
Fixed Disk Model (Size): KXG50ZNV256G NVMe TOSHIBA 256GB (238 GB)

Unified Task Sequence (SDP) (R1)

Operating System Deployment (OSD) Wizard

Microsoft Deployment Toolkit

UCF IT OS Deployment

Enter the Computer Name

Summary

OS Refresh

New Computer (Bare-metal deployment or computer does not exist in AD)

Use USMT to backup/restore user data

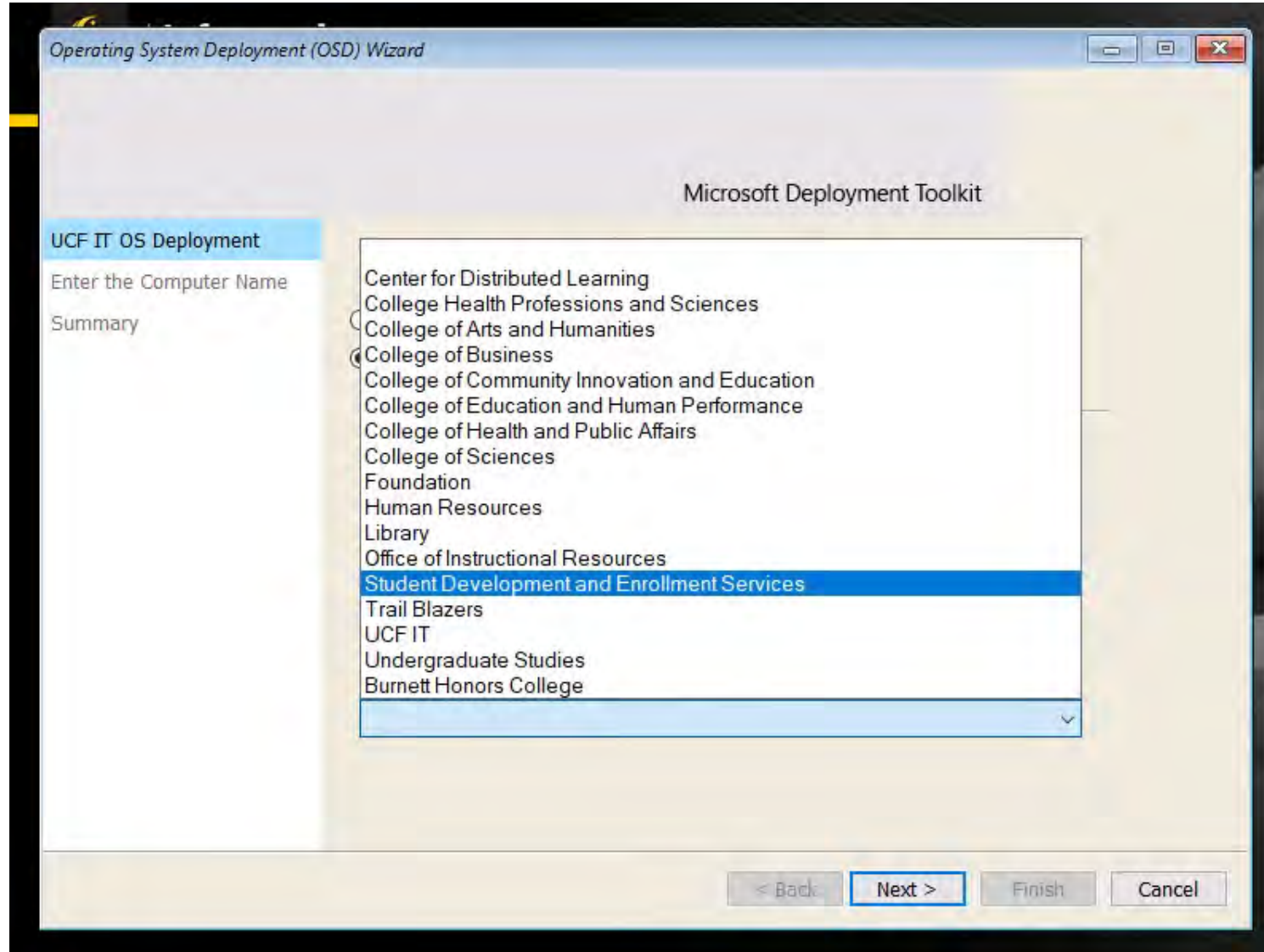
OS Only (Do not install any applications)

Enable BitLocker

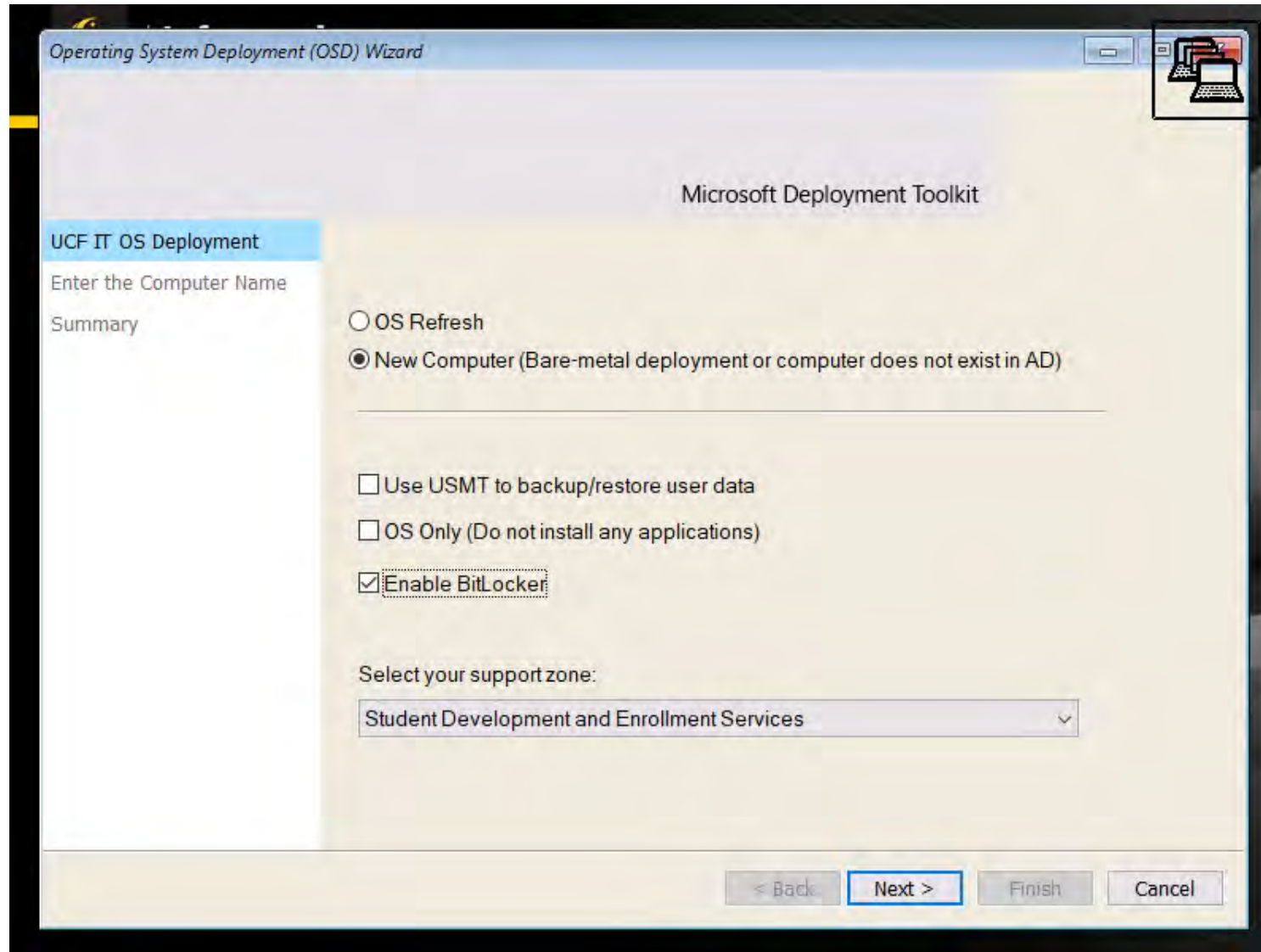
Select your support zone:

< Back Next > Finish Cancel

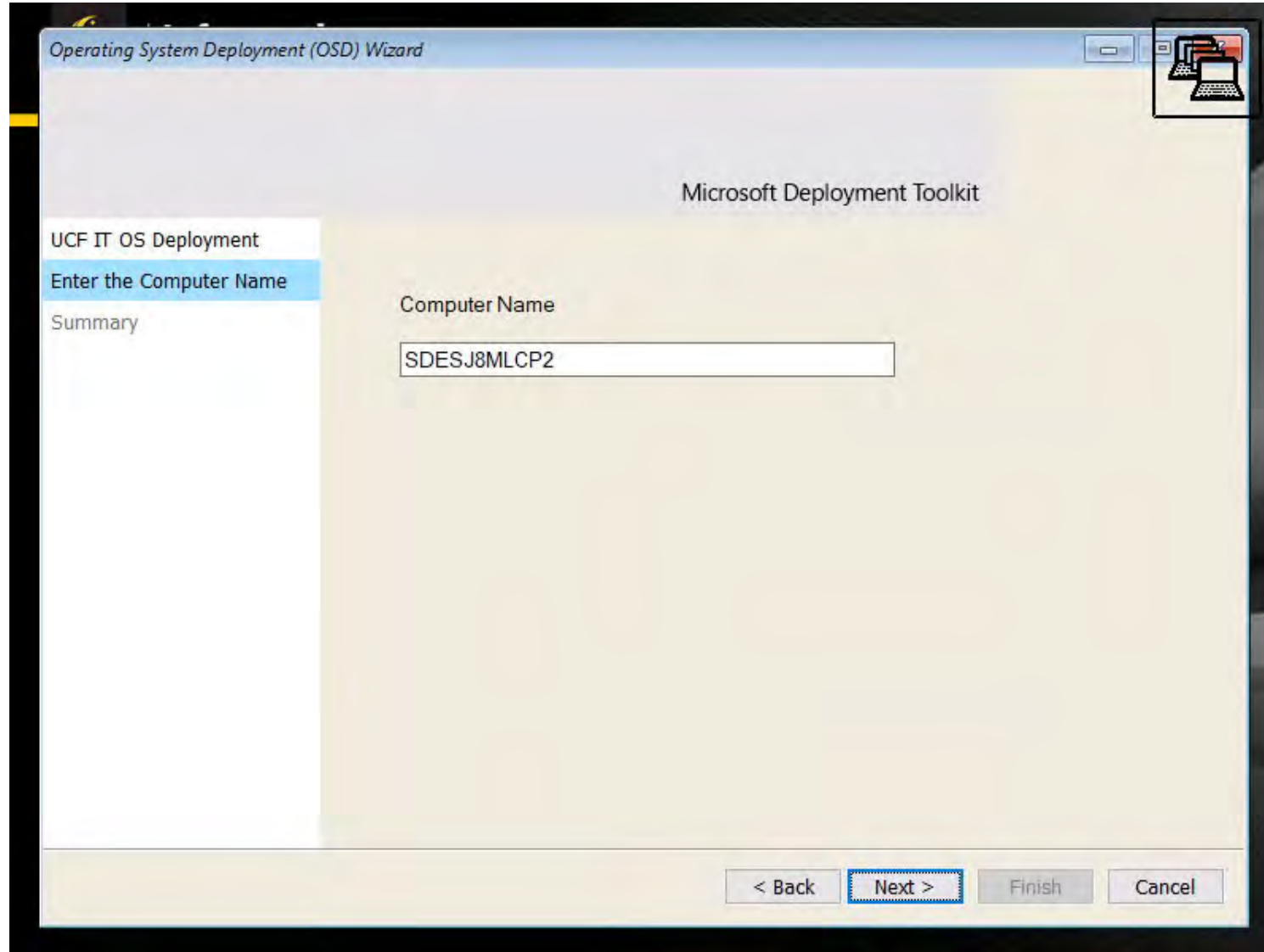
Unified Task Sequence (SDP) (R1)



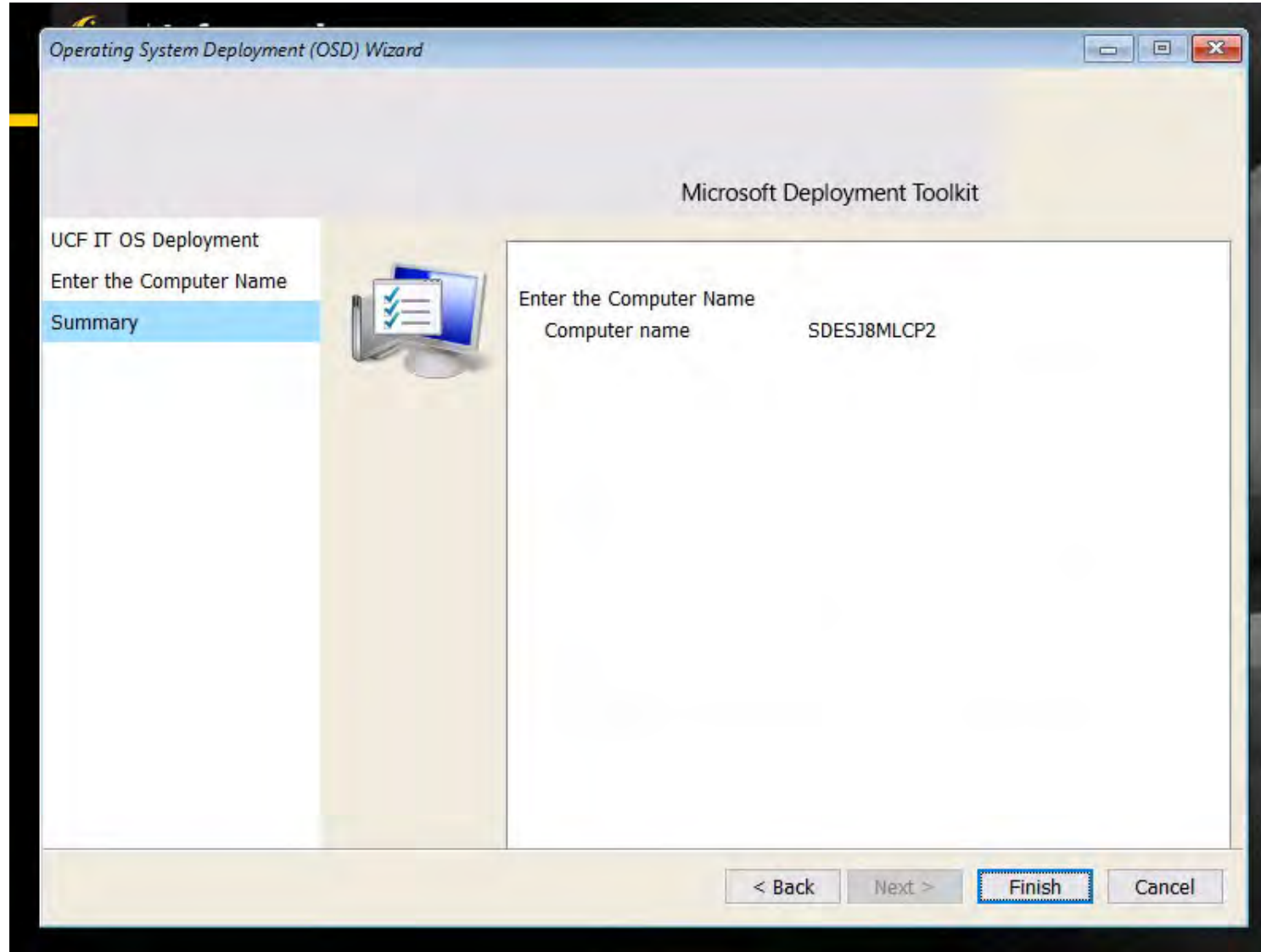
Unified Task Sequence (SDP) (R1)



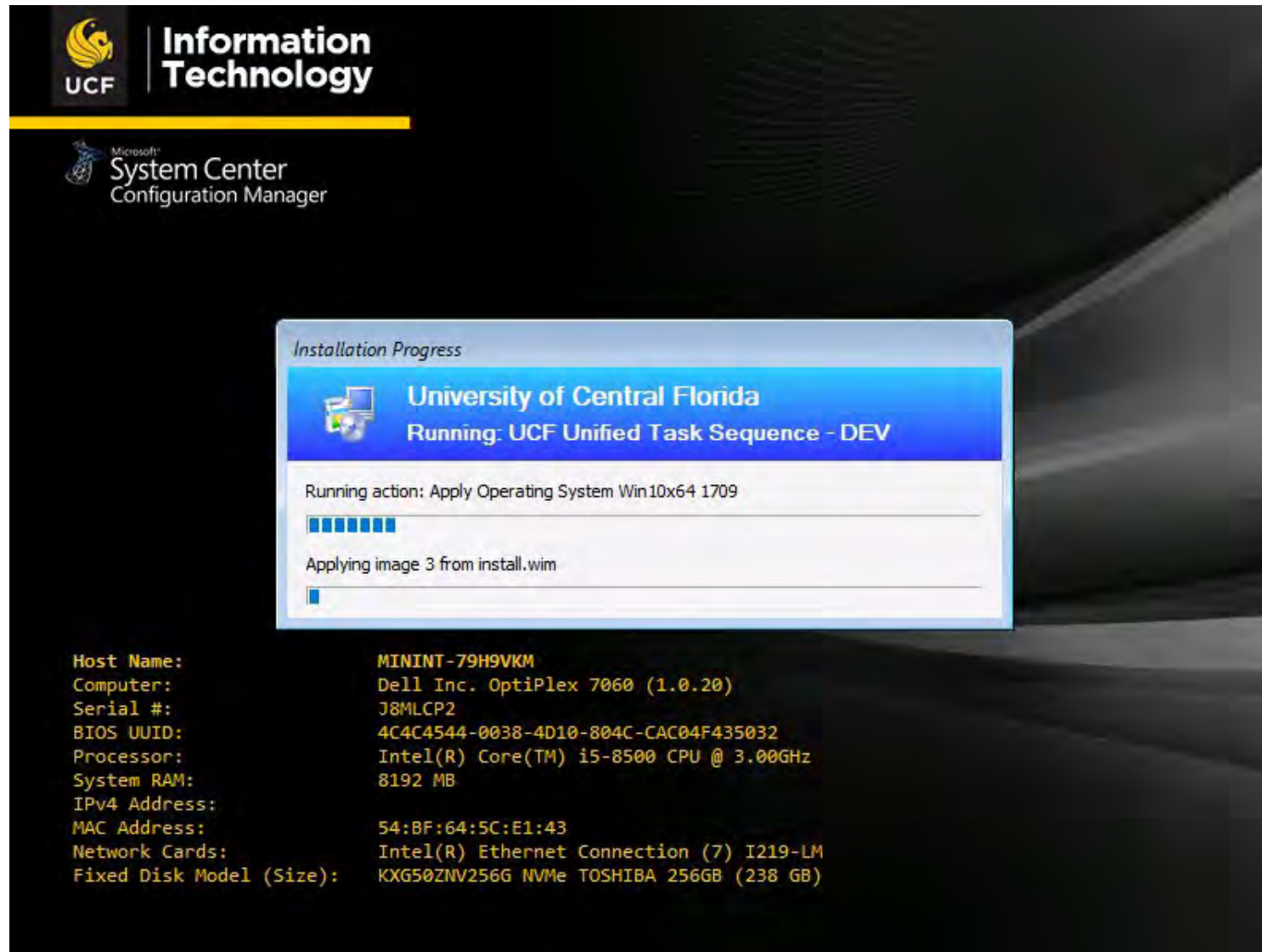
Unified Task Sequence (SDP) (R1)



Unified Task Sequence (SDP) (R1)



Unified Task Sequence (SDP) (R1)



The screenshot displays the Microsoft System Center Configuration Manager interface. At the top left, the UCF Information Technology logo is visible. Below it, the text 'Microsoft System Center Configuration Manager' is shown. The main content area features a blue 'Installation Progress' dialog box. The dialog box header reads 'University of Central Florida' and 'Running: UCF Unified Task Sequence - DEV'. The current action is 'Apply Operating System Win10x64 1709', with a progress bar showing approximately 10% completion. Below this, it states 'Applying image 3 from install.wim' with a smaller progress bar. At the bottom of the dialog, system information is listed in a key-value format.

Host Name: MININT-79H9VKM
Computer: Dell Inc. OptiPlex 7060 (1.0.20)
Serial #: J8MLCP2
BIOS UUID: 4C4C4544-0038-4D10-804C-CAC04F435032
Processor: Intel(R) Core(TM) i5-8500 CPU @ 3.00GHz
System RAM: 8192 MB
IPv4 Address:
MAC Address: 54:BF:64:5C:E1:43
Network Cards: Intel(R) Ethernet Connection (7) I219-LM
Fixed Disk Model (Size): KXG50ZNV256G NVMe TOSHIBA 256GB (238 GB)

Unified Task Sequence (SDP) (R1)

UCF Unified Task Sequence Task Sequence Editor

The screenshot shows the 'Task Sequence Steps' in the UCF Unified Task Sequence Task Sequence Editor. The steps are organized into folders and include:

- Authentication**
 - ✓ Create Authentication Variable
 - ☐ Bypass Authentication
 - ✓ Run Authentication Prompt
- Unified Task Sequence**
- UDI Wizard**
 - ✓ Use Toolkit Package
 - ✓ Gather
 - ✓ UDI Wizard
- Capture Computer Settings (OS)**
 - ✓ Disable BitLocker
 - ✓ USMT Capture Windows Settings
 - ✓ USMT Capture Network Settings
- User State Migration Capture**
 - ✓ USMT Set Local State Location
 - ✓ USMT Capture User Files and Settings (OS)
 - ✓ USMT Capture User Files and Settings (WinPE)
- Install Operating System**
 - ✓ Restart in Windows PE
 - ✓ Partition Disk 0 - BIOS
 - ✓ Partition Disk 0 - UEFI
 - ✓ Pre-provision BitLocker
 - ✓ Apply Operating System Win10x64 1709
 - ✓ Apply Operating System Win10x64 1803

The screenshot shows a list of tasks under the 'Apply Pre-OS Dept Setting' folder. The tasks are:

- ☐ TBHC**
- ☐ CDL
- ☐ CHPS**
- ☐ CAH
- ☐ CBA**
- ☐ CCIE**
- ☐ CEDHP
- ☐ COHPA
- ☐ COS
- ☐ FND
- ☐ HR
- ☐ Library
- ☐ OIR**
- ☐ SDES
- ☐ APPS
- ☐ IT
- ☐ UGS**
- ☐ No Zone Selected
- ✓ Auto Apply Drivers
- ✓ Setup Windows and Configuration Manager

Unified Task Sequence (SDP) (R1)

- Power Management
 - Set Power Scheme - High Performance
 - Set Power Scheme - Monitor Timeout
 - Set Power Scheme - Standby
- Dell Command | Update
 - Install Dell Command | Update
 - Modify Dell Command | Update
 - Run Dell Command | Update
 - Restart Computer
- Software
 - Install Tier | Applications - Acrobat
 - Install Tier | Applications - Office
 - Install Tier | Mobile Applications
 - Restart Computer
- Apply Post-OS Dept Setting
 - TBHC
 - CDL
 - CHPS
 - CAH
 - CBA
 - CCIE
 - CEDHP
 - COHPA
 - COS
 - FND
 - HR
 - Library
 - OIR
 - SDES
 - TrailBlazers
 - IT
 - UGS
- Cleanup
 - Install Software Updates
 - Enable BitLocker
 - Set Power Scheme - Balanced

- User State Migration Restore
 - USMT Restore User Files and Settings
 - Final Restart
- On Error
 - Remember Original Error Code
 - Support Zone
 - Connect to Log Repository
 - Erase Pre-Existing Logs
 - Create Log Folder
 - Copy Logs
 - Connect to Log Repository
 - Erase Pre-Existing Logs
 - Create Log Folder
 - Copy Logs
 - Return Original Error Code

Round 1

1. Unified Task Sequence (SDP) (R1)

- Establish and Standardize all of the endpoint operating system deployment with a single task sequence to be adopted by all of Cohort 1 and 2 within UCF IT. All of the deskside zones will need to participate in it's creation, provide input on future improvement as well as work together to adopt the standard process, procedure and technology.

2. DHCP Reservations / Dynamic Areas (SDP) (R1)

- **Per the Service Design Package (SDP) Document, All of the Cohort 1 and Cohort 2 areas should have clearly defined VLAN and DHCP Scopes, with a focus on locking down and securing the Faculty and Workstation areas with reservation-only IPs. Adoption is expected of all UCF IT Supported endpoint areas**

3. Microsoft Office Click-to-Run (C2R) (R1)

- As part of the Streamline Client Experience Project (SCEP), It is important that all of the UCF IT Supported Endpoints are using the latest version of Office (Office 365 Pro Plus) before Fall of 2019. The Skype 2019 voice services will only function properly with the latest build of Office on the endpoint. This project is designed to assist the Cohort 1 and 2 deskside zones with migrating from previous builds of office (2016 MSI and Previous) to the latest Office 365 version using Click-to-Run installation technology

4. Jamf Management for macOS (R1)

- JAMF is up for renewal and renegotiation with the vendor, in which moving the platform to the cloud is currently a possibility. Aside from moving the JAMF management platform to the cloud, it will be important to provide parity of services and settings to JAMF devices the same as we are providing currently with SCCM or will provide with Intune in the future. JAMF is the primary management platform for macOS and Apple devices.

DHCP Reservations / Dynamic Areas (SDP) (R1)

SDP Alignment

- Section IX, File, Print and Network Access (p.35)
- Network Access (p.42)

DHCP Reservations / Dynamic Areas (SDP) (R1)

Data Collection

- List of scopes?
- Is the area already reservation only? Why?
- Do you have any exception areas or areas with static IP addressing?
- Are you fully migrated to NET DHCP (No local DHCP servers)?
- What information is in the description field of your reservations? Why?

DHCP Reservations / Dynamic Areas (SDP) (R1)

Migration Process

- Reserve all existing IPs (Convert leases to reservations)
- Provide tools/access for deskside zones to create reservations
- Reconfigure identified areas to dynamic-only VLAN
- Determine standard convention for reservation descriptions

DHCP Reservations / Dynamic Areas (SDP) (R1)

IPAM Tool

- Granular, role-based access to individual scopes
- Logging/Auditing/Reporting
- Extendable, can add data fields
- Current DHCPMgr access group copied to IPAM

DHCP Reservations / Dynamic Areas (SDP) (R1)

Clean Up

- How long should a reservation be unused before deletion?
- Can/should we automate that process?
- Can we leverage IPAM reporting for automation?

Considerations

- Should we wait for IPAM?
- What data would be helpful in description field?
- Special considerations for BYOD?

Round 1

1. Unified Task Sequence (SDP) (R1)

- Establish and Standardize all of the endpoint operating system deployment with a single task sequence to be adopted by all of Cohort 1 and 2 within UCF IT. All of the deskside zones will need to participate in it's creation, provide input on future improvement as well as work together to adopt the standard process, procedure and technology.

2. DHCP Reservations / Dynamic Areas (SDP) (R1)

- Per the Service Design Package (SDP) Document, All of the Cohort 1 and Cohort 2 areas should have clearly defined VLAN and DHCP Scopes, with a focus on locking down and securing the Faculty and Workstation areas with reservation-only IPs. Adoption is expected of all UCF IT Supported endpoint areas

3. Microsoft Office Click-to-Run (C2R) (R1)

- **As part of the Streamline Client Experience Project (SCEP), It is important that all of the UCF IT Supported Endpoints are using the latest version of Office (Office 365 Pro Plus) before Fall of 2019. The Skype 2019 voice services will only function properly with the latest build of Office on the endpoint. This project is designed to assist the Cohort 1 and 2 deskside zones with migrating from previous builds of office (2016 MSI and Previous) to the latest Office 365 version using Click-to-Run installation technology**

4. Jamf Management for macOS (R1)

- JAMF is up for renewal and renegotiation with the vendor, in which moving the platform to the cloud is currently a possibility. Aside from moving the JAMF management platform to the cloud, it will be important to provide parity of services and settings to JAMF devices the same as we are providing currently with SCCM or will provide with Intune in the future. JAMF is the primary management platform for macOS and Apple devices.

Microsoft Office Click-to-Run (SDP) (R1)

SDP Alignment

- Software Lifecycle (p.17)

Microsoft Office Click-to-Run (SDP) (R1)

Data Collection

- Prerequisites
- Onboarding unit provides a brief description of their Office application needs.
- Will help identify any part of the process that is beyond the scope of the “base” installation.

Participating Units

- Burnett Honors College
- College of Sciences
- College of Health and Public Affairs
- College of Nursing
- CREOL
- Foundation
- Human Resources
- International Affairs and Global Strategies
- International Services Center
- Library
- Rosen College of Hospitality Management
- Student Development and Enrollment Services
- UCF Global
- UCF IT –IT Zone / Tech Commons

Microsoft Office Click-to-Run (SDP) (R1)

ProPlus vs Professional Plus

Office 365 ProPlus

Click-to-Run

Streaming installation

Product Updates

Online Activation

Extensibility

Group Policy

Local Install

Telemetry

Office Professional Plus 2016

MSI

Traditional Installation

Service Packs

Product Key



Microsoft Office Click-to-Run (SDP) (R1)

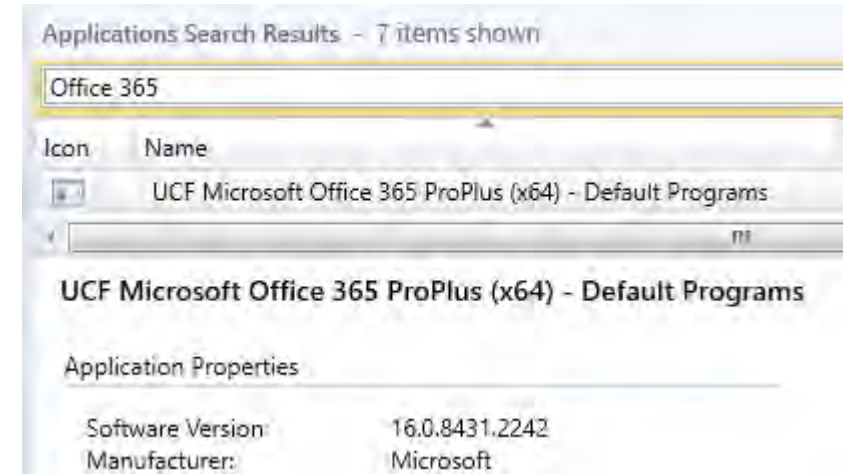
Which version is right for us ?

• Office 2016 ProPlus (MSI)

- Require stable feature set (classic track).
- Require Offline Use > 30 Days.
- Run older Office MSI or C2R side-by-side.
- Windows 7/8.1 legacy support until January 14, 2020.
- Require à la carte transform (MST) pre/post-installation options.*
- Require granular control of quality updates.*

• Office 365 ProPlus (C2R)

- *Nothing from first column.*
- Desire latest features.
- Require future cloud connectivity.
- Modern servicing “Set it and forget it” (Continuous track).



- **Results May Vary!**
- **Not Compatible with specific installs of Office**
- **Will Automatically Uninstall all previous versions**

Microsoft Office Click-to-Run (SDP) (R1)

Additional Recommendations

- Monthly Channel Updates

Update channel	Primary purpose	How often updated with new features	Default update channel for the following products
Monthly Channel	Provide users with the newest features of Office as soon as they're available.	Monthly	Visio Pro for Office 365 Project Online Desktop Client Office 365 Business, which is the version of Office that comes with some Office 365 plans, such as Business Premium.
Semi-Annual Channel	Provide users with new features of Office only a few times a year.	Every six months, in January and July	Office 365 ProPlus
Semi-Annual Channel (Targeted)	Provide pilot users and application compatibility testers the opportunity to test the next Semi-Annual Channel.	Every six months, in March and September	None

Microsoft Office 2019 & 365 Pro Plus

Is Microsoft Office 2019 Right for us?

- Will not operate on Windows 7.
- Will only come in “Click-to-Run” installation method
 - No offline install media
 - This also applies to Visio and Project
- Will receive security patches but **no feature updates**
- Will support MAK and KMS Activation
- Will **not** require an active internet connection post activation.
- Will be supported on LTSC / LTSB Windows Releases

Microsoft Office 365 Pro Plus is still our **Recommended** version for both Windows 10 and *(Now Available)* Windows 7 in the Majority of use-cases.



Round 1

1. Unified Task Sequence (SDP) (R1)

- Establish and Standardize all of the endpoint operating system deployment with a single task sequence to be adopted by all of Cohort 1 and 2 within UCF IT. All of the deskside zones will need to participate in it's creation, provide input on future improvement as well as work together to adopt the standard process, procedure and technology.

2. DHCP Reservations / Dynamic Areas (SDP) (R1)

- Per the Service Design Package (SDP) Document, All of the Cohort 1 and Cohort 2 areas should have clearly defined VLAN and DHCP Scopes, with a focus on locking down and securing the Faculty and Workstation areas with reservation-only IPs. Adoption is expected of all UCF IT Supported endpoint areas

3. Microsoft Office Click-to-Run (C2R) (R1)

- As part of the Streamline Client Experience Project (SCEP), It is important that all of the UCF IT Supported Endpoints are using the latest version of Office (Office 365 Pro Plus) before Fall of 2019. The Skype 2019 voice services will only function properly with the latest build of Office on the endpoint. This project is designed to assist the Cohort 1 and 2 deskside zones with migrating from previous builds of office (2016 MSI and Previous) to the latest Office 365 version using Click-to-Run installation technology

4. Jamf Management for macOS (R1)

- **JAMF is up for renewal and renegotiation with the vendor, in which moving the platform to the cloud is currently a possibility. Aside from moving the JAMF management platform to the cloud, it will be important to provide parity of services and settings to JAMF devices the same as we are providing currently with SCCM or will provide with Intune in the future. JAMF is the primary management platform for macOS and Apple devices.**

JAMF Management for macOS

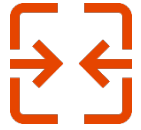
SDP Alignment

- Section III. Methods of Support
- Section IV. Desktop and Mobile Devices
- Section VI. Supported Operating Systems (P.19)

JAMF Management for macOS

Current State

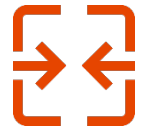
- 1 On-Prem Production JAMF Pro Instance
- 1 On-Prem Development JAMF Pro Instance
- 618 Enrolled Mac Devices
- 6 Colleges/Departments
- 55 Active Policies
- 161 Packaged Applications
- First attempt to streamline with UCF branded packages and scripts available to everyone 12 UCF scripts, 24 UCF packages



JAMF Management for macOS

Data Gathering

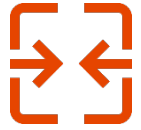
- Are they on the NET domain?
 - If not what domain are they on?
- Are their macs currently domain bound?
 - If their macs are domain bound, in what OUs are their macs bound?
- Do they have a service account for binding computers into those OUs?
 - What is the username and password to those accounts?
- Do they use security groups to allow their technicians admin access to their mac or PC computers?
 - What are the names of those security groups?
- What buildings fall within their area?
- What departments fall within their area?
- What VLANs (Starting + Ending IPs) are within their area?
- Do they have any areas with metered or limited internet connections?
 - Where are these areas?
 - Are there any opportunities where large amounts of data can be pushed such as overnight or on the weekends?
- What Applications do they push to their macs?
 - Are any of those applications licensed?
 - Do any of those applications have restrictions on when they can be updated?
 - Are any of those applications purchased through the Mac App Store with a VPP or Personal Apple Account?
- On what VLANs does Netboot need to be available?



JAMF Management for macOS

Windows Environment Parity

- Folder redirection – Possible/ Needs Testing
- Shortcuts for shared folders - Possible
- Device encryption with centrally managed keys - Possible
- Access to sign in restricted to department/unit level – Needs Testing
- Limited access to guest accounts – Needs Testing
- Remote access permissions by user - Possible
- Block installation of cloud storage clients. - Possible



JAMF Management for macOS

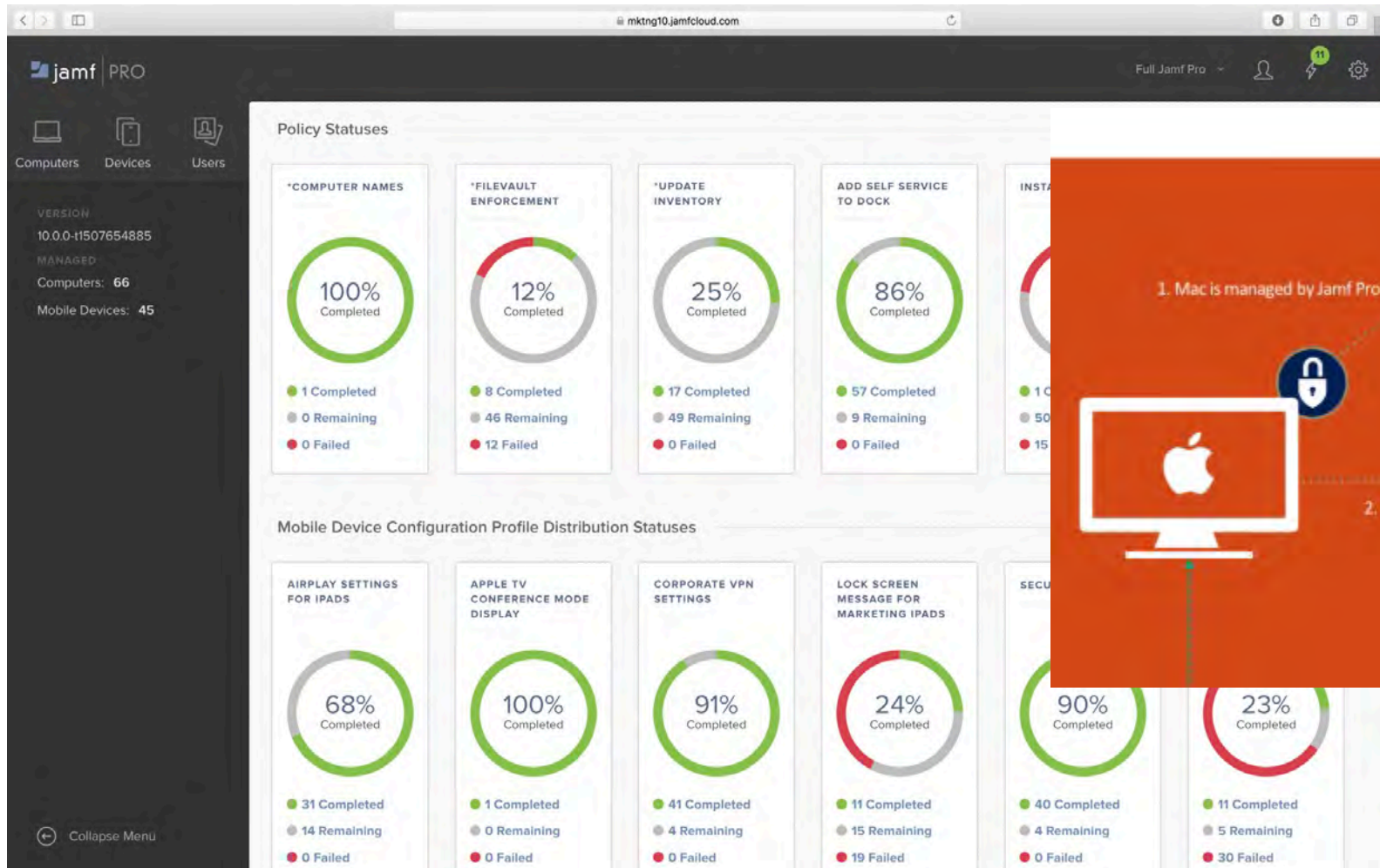
In Progress Projects

- JAMF Cloud
 - 24/7 support
 - AWS cloud instance with all updates handled by JAMF
 - 99.9% uptime
 - DP with unlimited storage
 - Daily backups
 - Live service monitoring
 - Fully scalable
 - Out of band management
- DEP
 - Faster imaging using Apple internet recovery
 - Streamlined first time setup
 - Auto enroll to JAMF



JAMF Management for macOS

Future State



Round 2

5. **Print Server Naming Standards & Papercut (SDP) (R2)**

- As services continue to merge, Endpoint Print Services will need to have a standard naming convention and configuration when being run via a Windows Managed Print Server. Additionally, the creation of centralized print servers that will be DDS managed has to be established to eliminate redundancy currently located at each of the deskside area and Cohort 1 and 2 units. Papercut deployment standards and eventually the Papercut Printing Service would be co-managed by its current service owners and DDS

6. **Hardware and Software Refresh Plan or Implementation (SDP) (R2)**

- Per the SDP, establishing healthy software and hardware lifecycles will be very important in keeping out endpoint fleet current, healthy and productive. As a result, it will be important that we propose a customized hardware and software plan that will suit the needs of each of the Cohort 1 and Cohort 2 units. Adopting and implementing a plan would be ideal, but simply being able to identify what would be needed both logistically and financially should be sufficient at this stage of the UCF IT and IT 2020 initiative.

7. **Remote Support Tool Implementation (SDP) (R2)**

- As it relates to the geographic centralization of the different support zones, each deskside area is responsible for a larger geographic footprint than many of the individual colleges and units were prior to the formation of UCF IT. As a result, a standardized tool with expected behaviors, features and ease-of-use for both the technician and the client are required to achieve efficiency and effectiveness with what will eventually become our primary method of support.

8. **“Mobile First” User Experience when possible (R2)**

- As part of the UCF Downtown Trailblazers POC and the Service Design Package, this project will help us coordinate the architecture, engineering, testing and deployment of a single, generic-use mobile experience that will help maximize use ability while decreasing complexity. This is a result of the “mobile-first” initiative being advertised for the UCF Downtown campus and if successful, can service as our standardized method of deploying and configuring our windows and macOS based mobile devices.

Print Server Naming Standards

SDP Alignment

- Supported OS (p.19)
- Data Encryption (p.38)
- Software Delivery Methods (p.20)

Print Server Naming Standards

Current State

- Management
 - PaperCut, PRTG, No Management
- Printer Models
 - Toshiba, Dell, Brother, HP, Lexmark
- Quotas
 - Quota and Non-Quota Printing
- Naming Standards
 - Various
- Printer Settings
 - No setting standardization
- Network Printer Setup
 - Direct IP + Manual, Print Server + GPO

Print Server Naming Standards

Data Gathering

- What printers are in your environment
 - Location
 - IP
 - Name
 - Model
 - Use Case (Standard Printing, Pay for Print, Large Format Printing, Prescriptions)
 - Restrictions (FERPA, HIPPA, PCI, CJIS, Research)
 - Friendly Name for Each Printer
 - Services Used (scan to file server, Scan to email, wireless printing)
 - Password to Printer Admin Pages
 - Userbase for Printer
 - Release Procedures
- What is the name of the print server used in your area
- What VLAN are printers added to
- Is this a non NATed VLAN
- Is this a VLAN specifically for printers
- What management tools are in use for managing printers?
 - i.e. Papercut, SCOM, PRTG
- How are consumables like ink and paper being funded
- Do you have any printer agreements with business services
- Who purchases supplies
- What security groups are in use for delegating printer access

Print Server Naming Standards

Recommendations

- Naming Scheme : Building_Room_Friendly_Type
 - Ex. TC2_117_StudentLab_BW, CNH_202_HPLaserJet_CL
- All Networked printers get added to centralized print server
- All Networked printers are added to non-NATed VLAN
 - Noted exception may be public printing such as KIC scanners in library
- All unused services turned off
- UCF time server
- SNMPv3 enabled if managed
- Scan to email using UCF SMTP with TLS and SSL
- Local hard drive saving disabled or set to delete after completion
- Windows and AD sharing disabled
- Networked printers with >5 users are added via GPO with role-based access
- Fault tolerant centralized print server
 - Azure or Clustered
- Papercut is standard for managed printing. Strongly recommended but not required.
- Quotas are handled by departments through onboard quota management (Toshiba) or through Papercut (delegated access)
- All printers will use a non-default password for any admin functions/web portals

Print Server Naming Standards

Future State

- Papercut
 - Where does PaperCut live
 - Split PaperCut Server
 - Student, SGA, and Staff/Faculty management servers
- Build Central Print Server
 - Determine best structure
 - Redundant Local, Azure
 - 1 Centralized, 1 for Each Zone
 - WPA2 Availability

Round 2

5. Print Server Naming Standards & Papercut (SDP) (R2)

- As services continue to merge, Endpoint Print Services will need to have a standard naming convention and configuration when being run via a Windows Managed Print Server. Additionally, the creation of centralized print servers that will be DDS managed has to be established to eliminate redundancy currently located at each of the deskside area and Cohort 1 and 2 units. Papercut deployment standards and eventually the Papercut Printing Service would be co-managed by its current service owners and DDS

6. Hardware and Software Refresh Plan or Implementation (SDP) (R2)

- Per the SDP, establishing healthy software and hardware lifecycles will be very important in keeping out endpoint fleet current, healthy and productive. As a result, it will be important that we propose a customized hardware and software plan that will suit the needs of each of the Cohort 1 and Cohort 2 units. Adopting and implementing a plan would be ideal, but simply being able to identify what would be needed both logistically and financially should be sufficient at this stage of the UCF IT and IT 2020 initiative.

7. Remote Support Tool Implementation (SDP) (R2)

- As it relates to the geographic centralization of the different support zones, each deskside area is responsible for a larger geographic footprint than many of the individual colleges and units were prior to the formation of UCF IT. As a result, a standardized tool with expected behaviors, features and ease-of-use for both the technician and the client are required to achieve efficiency and effectiveness with what will eventually become our primary method of support.

8. “Mobile First” User Experience when possible (R2)

- As part of the UCF Downtown Trailblazers POC and the Service Design Package, this project will help us coordinate the architecture, engineering, testing and deployment of a single, generic-use mobile experience that will help maximize use ability while decreasing complexity. This is a result of the “mobile-first” initiative being advertised for the UCF Downtown campus and if successful, can service as our standardized method of deploying and configuring our windows and macOS based mobile devices.

Hardware and Software Refresh Plan

SDP Alignment

- Section IV Desktop and Mobile Devices Lifecycle (p.8)
- Section VI Client Desktop Software Lifecycle (p.17)
- Section VIII Technical Consultation (p.28)

Hardware and Software Refresh Plan

Onboarding Process

- **Initial Information regarding Hardware and Software Refresh (HSR) Guidelines**
 - 5 Year / Warranty Aligned
 - UCF IT Product Catalog
- **Unit Discovery**
- **Deliverables**
 - Hardware Report
 - Software Report
 - Software Updates Schedule

Hardware and Software Refresh Plan

Data Gathering

- **Qualtrics Survey**
- **Automated Information Gathering**
 - SCCM Reports
 - AD Reports via Powershell
 - Telemetry
- **Access to existing software license storage**
 - Usage
 - Basic Compliance
 - Version Analysis

Hardware and Software Refresh Plan

Data Gathering Cont.

- How is refresh done today (Qualtrics?)
- How long? (Years, Until Dead)
- Funding? (Dept/IT/Grant/Tech fee)
- Replacement like for like?
- Peripherals?(Monitor,printer,etc)
- Current budget?
- Non-standard devices?
- Secondary, tertiary?
- Tablets?
- Loaners?
- Hot swap?
- Where is it from?
- Dominos replacements?

Hardware and Software Refresh Plan

Data Gathering Cont.

- Work with the Enterprise Application Support Team (Terry Wheeler)
 - Utilize already gathered information
- Examine possible consolidation of similar products
- Coordinate with departmental liaison and Business Relationship Manager for accuracy
- Identify cycle categories
- ServiceNow Software management import*
- Environment Compatibility

Hardware and Software Refresh Plan

Recommendations

- Develop 5-year plan and present
- Create average cost per year
- Possible ramp up strategy
- Move to Monthly/Yearly plan
- Limitations
- Funding
- Staff Consideration to do the replacements
- Space for storage/set-up

Hardware and Software Refresh Plan

Future State

Hardware as a Service (HaaS)

- Possible Leasing Model
- 5 year or newer machine
- Like-for-like based on need
- On demand refresh each year
- Only pay for what you need
- Hot swap or loaner during repairs
- Long term plan to wrap overhead into cost per unit

Round 2

5. **Print Server Naming Standards & Papercut (SDP) (R2)**

- As services continue to merge, Endpoint Print Services will need to have a standard naming convention and configuration when being run via a Windows Managed Print Server. Additionally, the creation of centralized print servers that will be DDS managed has to be established to eliminate redundancy currently located at each of the deskside area and Cohort 1 and 2 units. Papercut deployment standards and eventually the Papercut Printing Service would be co-managed by its current service owners and DDS

6. **Hardware and Software Refresh Plan or Implementation (SDP) (R2)**

- Per the SDP, establishing healthy software and hardware lifecycles will be very important in keeping out endpoint fleet current, healthy and productive. As a result, it will be important that we propose a customized hardware and software plan that will suit the needs of each of the Cohort 1 and Cohort 2 units. Adopting and implementing a plan would be ideal, but simply being able to identify what would be needed both logistically and financially should be sufficient at this stage of the UCF IT and IT 2020 initiative.

7. **Remote Support Tool Implementation (SDP) (R2)**

- As it relates to the geographic centralization of the different support zones, each deskside area is responsible for a larger geographic footprint than many of the individual colleges and units were prior to the formation of UCF IT. As a result, a standardized tool with expected behaviors, features and ease-of-use for both the technician and the client are required to achieve efficiency and effectiveness with what will eventually become our primary method of support.

8. **“Mobile First” User Experience when possible (R2)**

- As part of the UCF Downtown Trailblazers POC and the Service Design Package, this project will help us coordinate the architecture, engineering, testing and deployment of a single, generic-use mobile experience that will help maximize use ability while decreasing complexity. This is a result of the “mobile-first” initiative being advertised for the UCF Downtown campus and if successful, can service as our standardized method of deploying and configuring our windows and macOS based mobile devices.

Remote Support Tool

SDP Alignment

- Section IV Desktop and Mobile Devices Methods of Support (p.9)

Remote Support Tool



Remote Support Tool

Feature Overview

- Cross-Platform Access (Windows, macOS, Linux, iOS, Android)
- Video Auditing (Session Recording)
- Comprehensive Reporting
- Host Pass (Vendor Access)
- Screen Annotation
- Two-Factor Authentication (IdP - SAML 2.0)
- Unlimited Chat Support
- End-to-End Encryption / Security (HIPAA)
- Custom Branding
- Firewall-Friendly
- Granular Access Controls
- Inactive Session Timeout
- Lock Keyboard & Mouse
- Command Shell, Scripts, and SSH Integration
- Exit Surveys
- Team Chat
- Session Sharing & Transfer
- Reverse Screen Sharing & Presentations
- Wake Up, Restart, and Install

Remote Support Tool

Security

- AES-256 bit end-to-end (*FIPS 140-2 Level 2 – NIST*)
- Session Recording (*Can be disabled by tech in CW*)
- Application Sharing
- Privacy Screen (Blank Guest Monitor)
- Two-Factor Authentication
- Team Chat
- Granular Permissions
- Inject Credentials (Vault)

Remote Support Tool

Integrations

- Pre-Built Service/System Management/CRM (ServiceNow)
- We must purchase this integration separately from both Bomgar software and your ServiceNow solution.
- Customization & Branding
- Security Information and Event Management (SIEM)

Remote Support Tool

Web-Enabled

- Firewall-Friendly
- Supports Closed Networks
- vPro Integration (Bomgar)
- Wake on LAN
- One-Click Customer Client
- Click-to-Chat
- Unattended Access
- Supports Native Protocols (RDP & SSH)

Remote Support Tool

Collaboration

- Team Chat
- Session Sharing & Transfer
- Vendor Access (Bomgar)
- Reverse Screen Sharing
- Screen Annotation
- Remote Camera Access

Remote Support Tool

Management

- Client Policies
- Identity Management (LDAP, Kerberos, SAML, AD)
- Session Reports
- Session Queuing
- Automatic Routing
- Canned Scripts
- Mass Deployment (MSI)

Remote Support Tool

In-Session Tools

- File Transfer
- Multi-Monitor Support
- System & Registry Actions
- Command Shell

Licensing

- TeamViewer based on concurrent support sessions (channels).
- Bomgar Remote Support licensed per concurrent representatives.
- ConnectWise Control Premium limited to 1 “attended” connection per technician (Unlimited “Unattended” sessions).

Round 2

5. **Print Server Naming Standards & Papercut (SDP) (R2)**

- As services continue to merge, Endpoint Print Services will need to have a standard naming convention and configuration when being run via a Windows Managed Print Server. Additionally, the creation of centralized print servers that will be DDS managed has to be established to eliminate redundancy currently located at each of the deskside area and Cohort 1 and 2 units. Papercut deployment standards and eventually the Papercut Printing Service would be co-managed by its current service owners and DDS

6. **Hardware and Software Refresh Plan or Implementation (SDP) (R2)**

- Per the SDP, establishing healthy software and hardware lifecycles will be very important in keeping out endpoint fleet current, healthy and productive. As a result, it will be important that we propose a customized hardware and software plan that will suit the needs of each of the Cohort 1 and Cohort 2 units. Adopting and implementing a plan would be ideal, but simply being able to identify what would be needed both logistically and financially should be sufficient at this stage of the UCF IT and IT 2020 initiative.

7. **Remote Support Tool Implementation (SDP) (R2)**

- As it relates to the geographic centralization of the different support zones, each deskside area is responsible for a larger geographic footprint than many of the individual colleges and units were prior to the formation of UCF IT. As a result, a standardized tool with expected behaviors, features and ease-of-use for both the technician and the client are required to achieve efficiency and effectiveness with what will eventually become our primary method of support.

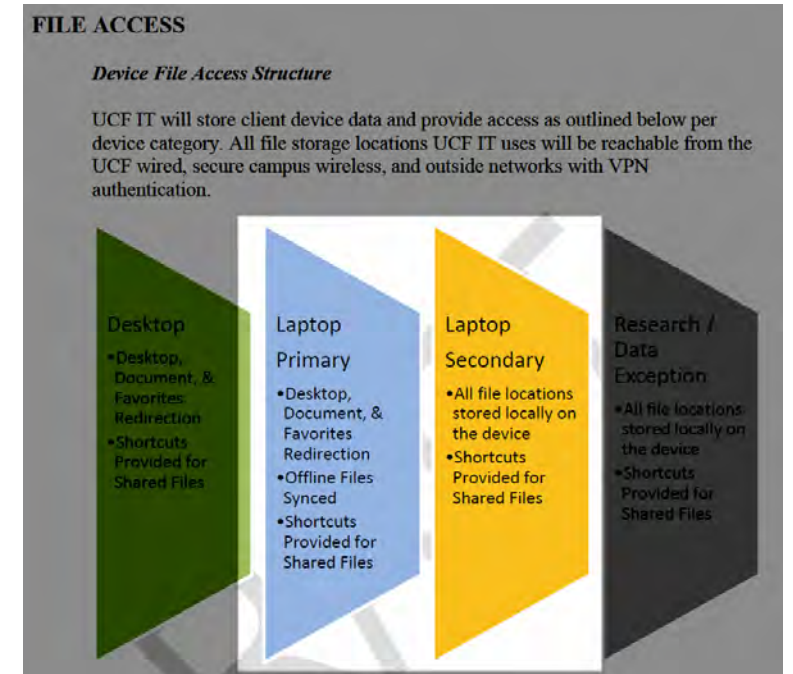
8. **“Mobile First” User Experience when possible (R2)**

- As part of the UCF Downtown Trailblazers POC and the Service Design Package, this project will help us coordinate the architecture, engineering, testing and deployment of a single, generic-use mobile experience that will help maximize use ability while decreasing complexity. This is a result of the “mobile-first” initiative being advertised for the UCF Downtown campus and if successful, can service as our standardized method of deploying and configuring our windows and macOS based mobile devices.

Mobile Device Experience

SDP Alignment

- III. Methods of Support
 - All Available Methods when Managed / University Owned
- IV. Desktop and Devices
 - Subject to 5 year lifecycle and Warranty Length Dependent levels of support
- VI. Client Desktop Software
 - Subject to the same Software Evaluation Criteria / Lifecycle (N-2 Stable/Supported Versions of Applications.)
- VII. Elevated Access
 - Subject to same approval process for administrative access. (This will be a radical shift for some deskside zones)
- IX. File, Print, Scan and Network Access
 - Subject to specifically the Laptop Primary, Laptop Secondary access guidelines.



Mobile Device Experience

Data Gathering

- How many Mobile Devices Total?
- Of those how many are PC?
- How many of the PC are still under warranty?
- of those how many are macOS?
- How many of the macOS are still under warranty?
- Do you have Mobile Devices not Dell / Apple or Consumer Model Line?
- Do the clients have Privileged Access to their mobile device?
- Are the devices Domain Joined?
- Are the devices Managed via SCCM?
- Are the devices accessible via Remote Support Tool?
- How many of the devices are Primary Users Devices (Single Device)?
- Do you have Offline / Out of the Country Mobile Devices?
- Do you have Special Case or Research Mobile Devices?
- Have your mobile users migrated to OneDrive?
- Besides File and Print Resources, are there any other network based resources that mobile users would need access to?

Mobile Device Experience

Recommendations

Operating System & Management

- **Microsoft Windows 10 1709 – Required**
 - Bitlocker Enabled by Default
 - .NET Framework 3.5 Installed by Default
- **MDM Platform Managed**
- **Domain Joined**
 - AzureAD or NET Domain
- **SCCM Managed**
 - Co-Management with MDM if Possible
- **Windows Updates via Microsoft CDN**

Network & Virtualization Resources

- **VPN Client**
 - Pre-configured via XML
 - Desktop Shortcut by Default
- **Remote Support**
 - Default Tool Pre-installed
 - Configured for Unattended Support / Prompt for Permission when in use
- **Citrix / UCF Apps**
 - Citrix Receiver installed by Default with SSO Enabled

Wireless Profiles

- WPA2 and WPA2 Backup Profiles Installed by Default
- SSO Enabled for WPA2 Primary

File, Data & Print

- **OneDrive for Business**
 - Personal User Data primary location
 - On-Demand Feature – **Required**
 - Default Storage Location – **Required**
 - Disable use of Personal MS Accounts
 - Enable Folder Redirection
 - Default Environment Variable (%onedrivesync%)
 - Desktop , Documents, Pictures, Videos, Music, Favorites Folders

Shared Folder Access

- No Change to Current Storage Location (Shared Service VM)
- VPN Connected to Access Resource - **Required**
- Default DFS Path (\\net.ucf.edu\Shares) – **Required**
 - New Shares and Targets will be added and filtered via Access Based Enumeration (ABE)

Printing

- VPN Connected to Access Resource - **Required**
- GPO Deployed

Customization & Settings

- Branded Lock screen with IT Support contact information
- Support Center Icon on Desktop to Self Service Portal
- Software Center Icon on Desktop for application catalog
- Cortana will be Disabled by Default
- Microsoft Store will be enabled only for Free Purchases
 - Ability to Add Personal Accounts Disabled

Round 3

9. AD Reorg or Move (Moran) (R3)

- Work with Infrastructure / Brian Blum on some initial design input as well as provide some initial proof of concept environments / VMs in DEV or QA. Work with Chris and the Enterprise Directory Governance, as well as Roll Based Access POC

10. File and Data Migration (SDP) (R3)

- Work to Define settings for SharePoint Migration Tool, POC overriding OneDrive Security Temporarily (Ideally Script) to allow for Mass Import of Data from File Servers as well as Standardize OneDrive Adoption / Implementation.

11. Baseline DDS Managed GPOs and SCCM Client Settings(SDP) (R3)

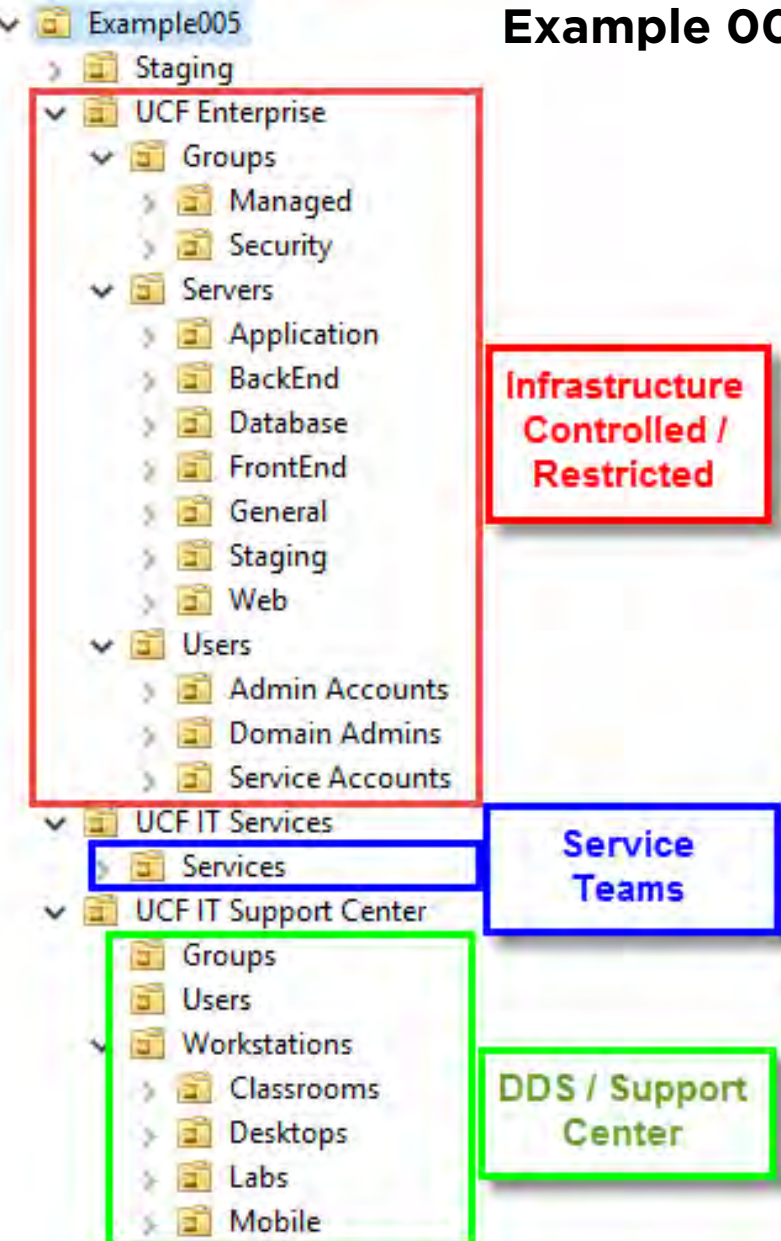
- Work to create baseline Policy in GPO and Intune (if Possible) to be least intrusive but still secure. ISO will need to be involved to determine policy minimums as well as SCCM Client or Intune Baselines. Intune related items if available.



Round 3 - Active Directory

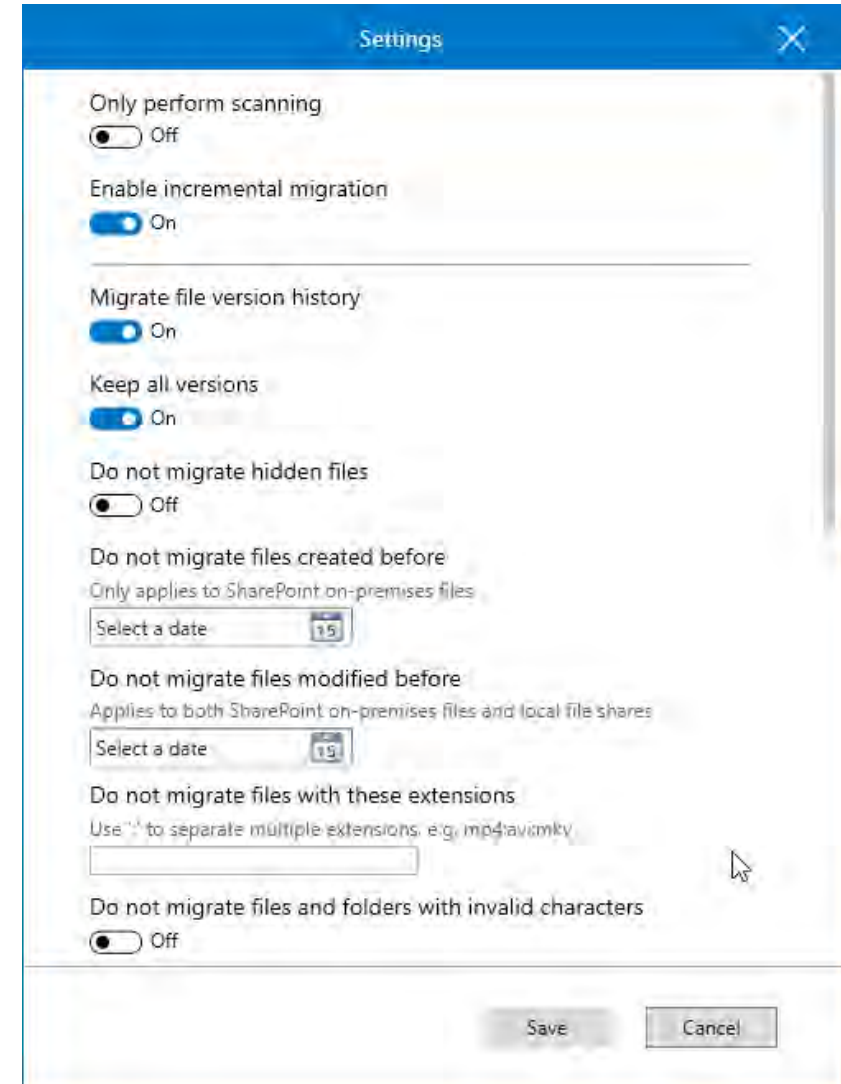
- Create Proof of Concept for RBAC in DEV or QA
- Work with Infrastructure Team and Working Group to determine Viability of Example 005 (vetting)
- Work with the Enterprise Directory Governance to provide feedback and show research already performed
- Suggest any missing roles that our team may need over time, as well as deskside zone specific roles that support staff would need (Zones)
- Suggest Naming Standards for Groups, Devices and any additional SubOU classifications or guidelines

Example 005



Round 3 – File and Data

- Default SMT Settings for all use cases
- Create POC for script that would allow us temporary co-management of individual's OneDrive locations for as-scale deployments of files into the cloud from File Servers
 - Present findings to ISO for approval
 - Work with UC Team with ISO Approval on working on a procedure for getting it completed
- Create POC for at-scale upload of Department Shares to SharePoint / Teams from File Servers
- Manual One Drive Adoption Requirements and SOP
- Manual SharePoint Adoption Requirements and SOP



Round 3 - Baseline Endpoint Configuration



Min Req (High-Level)

- BIOS / UEFI
- Secure Boot
- PXE Stack
- Auto-on Timer
- Passwords
- TPM
- Raid Config
- Legacy Boot
- USB Boot
- Access to the Domain "UCF Domain Policy" Object
- Baseline GPOs →



Baseline Categories

- Power Config
- AppLocker
- Firewall
 - SCCM / RC
 - Azure / Intune
- RDP / Remote Assist / Bomgar
- PSEXEC
- Ping
- NESSUS
- Application Specific Settings
 - MS Store
 - MS Office / S4B
 - Trusted Sites / Site Zones
 - IE Ent. Mode
 - Default Apps
 - Browser Settings



Baseline Categories Cont.

- Branding (Logon Screen \ Wallpaper)
- Resources (File/DFS/Print)
- "IT" Items
 - Powershell
 - Exclusion for IT Admins
 - BG Info
- Windows Update
- OS Specific Settings
 - MS Win 10 Security
 - Star Menu Layout
 - Cortana/Modern Features
 - Telemetry
 - "@ Work Accounts"
 - Local Admin Groups (LAPS)
- Mobile Specific Policy
 - WPA2 SSO
 - VPN XML
- Windows Defender
- SCCM Client Settings



ISO Required / Policy

- Logon Banner
- Lockout Times
- Display Last User
- Encryption
- Ctrl+Alt+Del
- Policy or Already documented Guideline
- Other ISO Recommendations