****

2018-2019

**ACTIVE DIRECTORY- <<APP\_NAME>> MIGRATION READINESS**

[1 Introduction 2](#_Toc528188350)

[2 Objective 3](#_Toc528188351)

[3 Definition & Acronyms 3](#_Toc528188352)

[3.1 Recommended Best Practices 3](#_Toc528188353)

[4 Application components and their Migration strategy 3](#_Toc528188354)

[4.1 Application Name 3](#_Toc528188355)

[4.1.1 Different Application Names 3](#_Toc528188356)

[4.2 Application Authentication Type 3](#_Toc528188357)

[4.2.1 <<$Service\_Accounts>> 3](#_Toc528188358)

[4.2.2 <<$Virtual\_Directory\_Service (VDS+)>> 5](#_Toc528188359)

[4.2.3 <<$CA\_SiteMinder>> 6](#_Toc528188360)

[4.2.4 <<$Enterprise\_Sec>> 7](#_Toc528188361)

[4.2.5 <<$Gateway (ESG)>> 8](#_Toc528188362)

[4.2.6 <<$Ping\_SSO>> 9](#_Toc528188363)

[4.2.7 <<$Centrify>> 10](#_Toc528188364)

[4.2.8 <<$ADFS>> 11](#_Toc528188365)

[4.2.9 <<$Essso>> 12](#_Toc528188366)

[4.2.10 <<$Other>> 13](#_Toc528188367)

[4.2.11 <<$Does not use AD for any authentication>> 14](#_Toc528188368)

[4.3 Authentication Mechanism 14](#_Toc528188369)

[4.3.1 <<$Kerberos>> 14](#_Toc528188370)

[4.3.2 <<$NTLM>> 15](#_Toc528188371)

[4.3.3 <<$Oauth>> 16](#_Toc528188372)

[4.3.4 <<$OpenID>> 17](#_Toc528188373)

[4.3.5 <<$SAML>> 17](#_Toc528188374)

[4.3.6 <<$Other>> 18](#_Toc528188375)

[4.3.7 <<$None>> 19](#_Toc528188376)

[4.4 Application Cross Domain 19](#_Toc528188377)

[4.4.1 <<$Yes\_Access\_Across\_Other\_Domains>> 19](#_Toc528188378)

[4.4.2 <<$No\_Access\_Across\_Other\_Domains>> 20](#_Toc528188379)

[4.5 Application SSL Certificate 20](#_Toc528188380)

[4.5.1 <<$Yes\_SSL\_Certificate>> 20](#_Toc528188381)

[4.5.2 <<$No\_SSL\_Certificate>> 21](#_Toc528188382)

[4.6 Local Accounts Creation 21](#_Toc528188383)

[4.6.1 <<$Yes\_Local\_Accounts>> 22](#_Toc528188384)

[4.6.2 <<$No\_Local\_Accounts>> 22](#_Toc528188385)

[4.7 Application Forest Domain Name 23](#_Toc528188386)

[4.7.1 <<$DMN1>> 23](#_Toc528188387)

[4.7.2 <<$FMRCO>> 24](#_Toc528188388)

[4.7.3 <<$DSDOM1>> 25](#_Toc528188389)

[4.7.4 <<$INTL>> 26](#_Toc528188390)

[4.7.5 <<$Other>> 27](#_Toc528188391)

[4.8 Application Service Account 28](#_Toc528188392)

[4.8.1 <<$List out the name of service accounts>> 28](#_Toc528188393)

[4.8.2 <<$Not using any service accounts>> 29](#_Toc528188394)

[4.9 File and Registry Permissions 29](#_Toc528188395)

[4.9.1 <<$None>> 29](#_Toc528188396)

[4.9.2 <<$Dynamic File Structure>> 29](#_Toc528188397)

[4.9.3 <<$Registry Permission>> 30](#_Toc528188398)

[4.9.4 <<$NAS>> 31](#_Toc528188399)

[4.9.5 <<$SAN>> 32](#_Toc528188400)

[4.10 Application Access Method 33](#_Toc528188401)

[4.10.1 <<$Direct Application Access>> 33](#_Toc528188402)

[4.10.2 <<$Based on Group membership>> 34](#_Toc528188403)

[4.10.3 <<$Based on Rule/Policy>> 35](#_Toc528188404)

[4.10.4 <<$Other>> 35](#_Toc528188405)

[4.11 Application Dependency 36](#_Toc528188406)

[4.11.1 <<$Yes\_Application\_Dependency>> 36](#_Toc528188407)

[4.11.2 <<$No\_Application\_Dependency>> 37](#_Toc528188408)

[4.12 Application Host Model 38](#_Toc528188409)

[4.12.1 <<$Web-Based>> 38](#_Toc528188410)

[4.12.2 <<$On-Premise>> 39](#_Toc528188411)

[4.12.3 <<$Cloud>> 40](#_Toc528188412)

[4.12.4 <<$Mainframe>> 40](#_Toc528188413)

[4.12.5 <<$Standalone (Devices)>> 41](#_Toc528188414)

[4.12.6 <<$Other>> 42](#_Toc528188415)

[4.13 Application Server Domain 43](#_Toc528188416)

[4.13.1 <<$Yes\_App\_Server\_Connected\_AD>> 43](#_Toc528188417)

[4.13.2 <<$No\_App\_Server\_Connected\_AD>> 44](#_Toc528188418)

[4.14 Client Type 44](#_Toc528188419)

[4.14.1 <<$Thin Client>> 44](#_Toc528188420)

[4.14.2 <<$Thick Client>> 45](#_Toc528188421)

[4.14.3 <<$Thin and Thick Client>> 46](#_Toc528188422)

[4.14.4 <<$Citrix (HVD)>> 47](#_Toc528188423)

[4.14.5 <<$Web Browser/Service>> 48](#_Toc528188424)

[4.15 Application Distribution List Mailbox 49](#_Toc528188425)

[4.15.1 <<$Distribution List>> 49](#_Toc528188426)

[4.15.2 <<$Shared Mailbox>> 49](#_Toc528188427)

[4.15.3 <<$Distribution List and Shared Mailbox>> 50](#_Toc528188428)

[4.15.4 <<$None>> 51](#_Toc528188429)

[4.16 Application Share Point 51](#_Toc528188430)

[4.16.1 <<$Yes\_Data\_Repository\_Utilization>> 51](#_Toc528188431)

[4.16.2 <<$No\_Data\_Repository\_Utilization>> 52](#_Toc528188432)

[5 Migration Wave/s 52](#_Toc528188433)

# Introduction

Active directory migration program aims to simplify the complex Active Directory environment in Fidelity. As part of the program, three domains (DMN1, FMRCO and DSDOM1) are transformed into one domain (WINROOT). The applications and infrastructures residing on these legacy domains will be impacted due to the transformation and they need to be migrated to the WINROOT domain.

# Objective

The objective of this document is to provide a comprehensive guide for the application migration. It includes all the AD dependent components that the application uses, and the steps that you need to follow in order to migrate each component to the new domain.

# Definition & Acronyms

|  |  |
| --- | --- |
| **Acronym** | **Definition** |
| AD | Active Directory |
| DN | Domain Name |
| FQDN | Fully qualified domain name |
| DB | Database |
| DFS | Dynamic File Structure |
| GPOs | Group Policy Object |
| BCP | Business Continuity Plan |

## Recommended Best Practices

Identify all places (property file, config file, etc.) where an IP address of an AD domain controller is used and, if possible, replace it with FQDN of AD domain.

# Application components and their Migration strategy

## Application Name

Name of this Application is **<<$Application\_Name>>** and below are the migration considerations and strategies for the application.

#### Different Application Names

* DNS should be checked to find (and change if necessary) any static naming records.

## Application Authentication Type

This application uses **<<$Authetication\_Type>>** as Authentication Type, below are some considerations and migration strategies.

#### <<$Service\_Accounts>>

**Considerations**

As part of Active Directory One Domain Consolidation, all current AD Domains and Forests will be migrated to a Single Forest and one AD domain. Currently there are 135 domain controllers and 3 AD Domains within scope of this project.

Phase 2 of the One Domain project will not begin until after the Assessment has been completed. No AD migrations will occur during the Assessment phase. To help with the planning and creating a Migration plan for your application, reference the below considerations:

* Your Application technical teams are aware of the programme for AD One Domain Consolidation
* Identify all Service Accounts and Domain Security Groups (Permission Groups ) which are used for
  + Service to Service seamless authentication
  + SQL Server Service Accounts for Service start/stop and access permissions
  + Kerberos Sign on using SPNs (service principal name) and Service Accounts
  + IIS Web Server Application Pool configurations using Groups and Service Accounts
  + Service Accounts for running HTTPS(web) on Server which requires Service Account seamless access
  + Service accounts which are member of Folder Permission Group, File Permission Group, Server Share Permission Group, DFS Folder Permission Group, and the Registry Permission Group
  + Service Accounts used for Firewall Connectivity to Legacy AD Domain
  + Service Accounts used for SFTP Gateway Connectivity to Legacy AD Domain
* Identify all places where hardcoded AD details (Service Accounts, host and port) or hardcoded IP addresses are used in your Application server

**Migration strategy**

Where Service Accounts are used to connect legacy AD domain environment, they will need to be replaced with similar Service Accounts in the new AD domain. To achieve this, the application's technical team needs to

* Consult AD Application Remediation team before making changes
* Consult AD Migration team for all changes required for Service Accounts, Permission Groups, and Role Groups
* Once New Service Accounts and DNs of the Service Accounts are available from the new AD Domain, unit test the connectivity along with the credentials
* Make changes to all the places in your Application Server Machine where Service Accounts were re-configured, then test
* Make changes to all the places in your Application source code and configuration files where Service Accounts need to be replaced to connect to the new AD Domain
* Update all Domain Security Groups, Permission Groups, and other Admin Groups where Service Account is a member
* Perform the necessary testing and BCP testing

#### <<$Virtual\_Directory\_Service (VDS+)>>

**Considerations**

As part of Active Directory One Domain Consolidation, all current AD Domains and Forests will be migrated to a Single Forest and one AD domain. Currently there are 135 domain controllers and 3 AD Domains within scope of this project.

Phase 2 of the One Domain project will not begin until after the Assessment has been completed. No AD migrations will occur during the Assessment phase. To help with the planning and creating a Migration plan for your application, reference the below considerations:

* Your Application technical teams are aware of the programme for AD One Domain Consolidation
* Identify if Virtual Directory Server is installed on a windows operating system and if so, whether the Windows Server belongs to any existing AD Forest and AD Domain
* Identify if VDS is connected to any of the Legacy AD Domains and those domain’s AD Objects such as Users, Groups, Admin Accounts. Verify if there is synchronization between the VDS and the Legacy AD Domains
* Identify if VDS is used as a Meta Directory between multiple AD Domains and with any other target platforms
* Identify if VDS only reads or if it has read/write permissions within the Legacy AD domains
* Identify if One or More Applications Reads and Writes to VDS which in turn reads and writes to the Legacy AD
* Identify if Authentication and Authorization with VDS are controlled by Legacy AD Domain Objects

**Migration strategy**

Where Virtual\_Directory\_Service (VDS+) is used to connect to the legacy AD domain environment, it will need to be pointed to the new AD domain. To achieve this, the application's technical team needs to

* Consult AD Application Remediation team before making changes
* Consult AD Migration team for all changes required for VDS such as Re-Hosting VDS to new Windows Server connecting to the new AD Forest and Domain
* Update Synchronization to point to the new AD Domain for AD Objects (Users, Groups, and Admin Accounts)
* If VDS acts as a Meta Directory with multiple legacy AD Domains, will need to ensure needed Users and Groups are synchronized to the new AD Domain
* Update VDS to query the new AD Domain for Authentication and Authorization
* Perform the necessary testing and BCP testing

#### <<$CA\_SiteMinder>>

**Considerations**

As part of Active Directory One Domain Consolidation, all current AD Domains and Forests will be migrated to a Single Forest and one AD domain. Currently there are 135 domain controllers and 3 AD Domains within scope of this project.

Phase 2 of the One Domain project will not begin until after the Assessment has been completed. No AD migrations will occur during the Assessment phase. To help with the planning and creating a Migration plan for your application, reference the below considerations:

* Your Application technical teams are aware of the programme for AD One Domain Consolidation
* Review SiteMinder Integration architecture for legacy AD integrations for Authentication, Single Sign on, and Policy/Group based Authorization
* Review SiteMinder Configurations for Legacy AD Domain Integrations
* Identify if SiteMinder is installed on a windows operating system and if so, whether the Windows Server belongs to any existing AD Forest and AD Domain
* Review SiteMinder’s other Components, such as Proxy Server, Federation Server, Policy Server, have any Legacy AD Integrations
* Review SiteMinder Configurations, such as Policy Domain, Realm, Request, Response headers, to find out if these configurations use Legacy AD Objects such as Users and Groups
* Identify if One or More Applications integrate with CA SiteMinder for Authentication, Course Grained Authorization and Single Sign to allow communications with other Web Based Applications
* Identify all places where hardcoded AD details (host and port) or hardcoded IP addresses are used in your CA SiteMinder server

**Migration strategy**

Where CA SiteMinder is used to connect to the legacy AD domain environment, it will need to be pointed to the new AD domain. To achieve this, the application's technical team needs to

* Consult AD Application Remediation team before making changes
* Consult AD Migration team for all changes required for CA SiteMinder such as Re-Hosting SiteMinder to new Windows Servers that are connected to the new AD Forest and Domain
* Consult AD team if CA SiteMinder infrastructure needs updates to connect to the new AD Domain or if it can work with Legacy AD Domain till some time when Legacy AD Domain will sunset/retire/decommission completely
* Plan to make necessary changes for SiteMinder AD connectivity and SiteMinder Configurations
* Plan to coordinate with multiple Applications team for general testing, validating Authentication, Authorization Use cases, after SiteMinder is migrated to new AD Doman
* Perform the necessary testing and BCP testing

#### <<$Enterprise\_Sec>>

**Considerations**

As part of Active Directory One Domain Consolidation, all current AD Domains and Forests will be migrated to a Single Forest and one AD domain. Currently there are 135 domain controllers and 3 AD Domains within scope of this project.

Phase 2 of the One Domain project will not begin until after the Assessment has been completed. No AD migrations will occur during the Assessment phase. To help with the planning and creating a Migration plan for your application, reference the below considerations:

* Your Application technical teams are aware of the programme for AD One Domain Consolidation
* Identify if Enterprise Security Tool is installed on windows operating system and if so, does the Windows Server belong to any existing AD Forest and Domain
* Identify all places where hardcoded Legacy AD details (host and port) or hardcoded IP addresses are used in your Enterprise Security server
* Identify all Service and Admin Accounts used from Legacy AD Domain
* Identify Authentication Methods used to connect to the Legacy AD Domain
* Identify if Enterprise Security Tool uses desktop security’s seamless sign on solution using Kerberos and/or NTLM

**Migration strategy**

Where Enterprise Security Tools are used to connect to the legacy AD domain environment, they will need to be pointed to the new AD domain. To achieve this, the application's technical team needs to

* Consult AD Application Remediation team before making changes
* Consult AD Migration team for all changes required by Enterprise Security Tools such as Re-Hosting to a Windows Server which is a member of the new AD Forest and Domain
* Plan to connect/query the new AD Domain
* Plan to make changes for hardcoded new AD details (host and port) or hardcoded IP addresses are used in your Enterprise Security server
* Plan to make changes to all Service Accounts, AD Groups, and AD User DNs
* Perform the necessary testing and BCP testing

#### <<$Gateway (ESG)>>

**Considerations**

As part of Active Directory One Domain Consolidation, all current AD Domains and Forests will be migrated to a Single Forest and one AD domain. Currently there are 135 domain controllers and 3 AD Domains within scope of this project.

Phase 2 of the One Domain project will not begin until after the Assessment has been completed. No AD migrations will occur during the Assessment phase. To help with the planning and creating a Migration plan for your application, reference the below considerations:

* Your Application technical teams are aware of the programme for AD One Domain Consolidation
* Identify if ESG Gateway Server is installed on windows operating system and if so, verify if the Windows Server belongs to any existing AD Forests and Domains
* Identify all places where hardcoded Legacy AD details (host and port) or hardcoded IP addresses are used in your ESG Gateway server
* Identify all Service and Admin Accounts used from Legacy AD Domain
* Identify Authentication Methods used to connect to the Legacy AD Domain
* Identify if ESG Gateway Server uses desktop security’s seamless sign on solution using Kerberos and/or NTLM

**Migration strategy**

Where ESG Gateway is used to connect to the legacy AD domain environment, it will need to be pointed to the new AD domain. To achieve this, the application's technical team needs to

* Consult AD Application Remediation team before making changes
* Consult AD Migration team for all changes required for ESG Gateway Server such as Re-Hosting to new Windows Server connecting new AD Forest, Domain
* Plan to connect/query the new AD Domain
* Plan to make changes for hardcoded new AD details (host and port) or hardcoded IP addresses are used in your Enterprise Security server
* Plan to make changes to all Service Accounts, AD Groups, and AD User DNs
* Perform the necessary testing and BCP testing

#### <<$Ping\_SSO>>

**Considerations**

As part of Active Directory One Domain Consolidation, all current AD Domains and Forests will be migrated to a Single Forest and one AD domain. Currently there are 135 domain controllers and 3 AD Domains within scope of this project.

Phase 2 of the One Domain project will not begin until after the Assessment has been completed. No AD migrations will occur during the Assessment phase. To help with the planning and creating a Migration plan for your application, reference the below considerations:

* Your Application technical teams are aware of the programme for AD One Domain Consolidation
* Identify if Ping Federation SSO Server is installed on windows operating system and if so, identify if the Windows Server belongs to any existing AD Forests and Domains
* Identify all places where hardcoded Legacy AD detaisl (host and port) or hardcoded IP addresses are used in your Ping Federation SSO server
* Identify if Ping Federation SSO Server issues SAML, WS-Fed, OAUTH, or OpenID token and whether the Federation server queries the Legacy AD Domain
* Validate if SAML, WS-Fed, OAUTH, or OpenID token contains attributes from the Legacy AD Domain
* Identify all possible Legacy AD domain objects such as AD containers, AD Groups, and Service Accounts used by Ping Federation SSO Server
* Identify if One or More Applications use Ping Federation SSO Server for Authentication or Federation Single Sign on with other internal or external partner Applications

**Migration strategy**

Where Ping Federate SSO is used to connect to the legacy AD domain environment, it will need to be pointed to the new AD domain. To achieve this, the application's technical team needs to

* Consult AD Application Remediation team before making changes
* Consult AD Migration team for all changes required for Ping Federate SSO Server such as Re-Hosting to new Windows Server when querying the new AD Forest and Domain
* Consult AD team if changes to Ping Federate SSO Server re-hosting will be required before the Legacy AD Domain is completely retired/decommissioned or whether Ping Federate SSO can operate in parallel
* Plan to make changes for SAML, WS-Fed, OAUTH, and OpenID configurations if Ping Federate SSO Server leverages attributes (User and Groups)
* Perform the necessary testing and BCP testing.

#### <<$Centrify>>

**Considerations**

As part of Active Directory One Domain Consolidation, all current AD Domains and Forests will be migrated to a Single Forest and one AD domain. Currently there are 135 domain controllers and 3 AD Domains within scope of this project.

Phase 2 of the One Domain project will not begin until after the Assessment has been completed. No AD migrations will occur during the Assessment phase. To help with the planning and creating a Migration plan for your application, reference the below considerations:

* Your Application technical teams are aware of the programme for AD One Domain Consolidation
* Identify if Centrify Server is installed on windows operating system and if so, verify if the Windows Server belongs to any existing AD Forest and Domain
* Identify all places where hardcoded Legacy AD details (host and port) or hardcoded IP addresses are used in your Centrify server
* Identify all Service Accounts, Permission Groups, and Security Groups from Legacy AD domain used to run Centrify Services
* Review Centrify Architecture related to legacy AD Integrations to verify if Centrify requires:
  + Legacy AD User/Password to Login to Centrify
  + Does Centrify protect privileged accounts from legacy AD such as Service, Server Admin, and Local Windows Server Accounts
  + Does Centrify provide one time access to Server Accounts based on Password Rotation Policy
  + Identify how many Windows Server’s Admin Accounts are managed by Centrify.

**Migration strategy**

Where Centrify is used to connect to the legacy AD domain environment, it will need to be pointed to the new AD domain. To achieve this, the application's technical team needs to

* Consult AD Application Remediation team before making changes
* Consult AD Migration team for all changes required for Centrify Server such as Re-Hosting to new Windows Servers or migrating existing servers to the new AD Forest and Domain
* Consult AD team if changes to Centrify Server re-hosting is required until the Legacy AD Domain is completely retired/decommissioned or if it can operate in parallel
* Consult AD team to obtain List of Service Accounts and Permission Groups from new AD Domain and plan to update the configurations to use the new Service Accounts and Permission Groups
* Will need to update the Privileged Account Management process related to managing all in scope Winders Server Service and Admin Accounts
* Perform the necessary testing and BCP testing

#### <<$ADFS>>

**Considerations**

As part of Active Directory One Domain Consolidation, all current AD Domains and Forests will be migrated to a Single Forest and one AD domain. Currently there are 135 domain controllers and 3 AD Domains within scope of this project.

Phase 2 of the One Domain project will not begin until after the Assessment has been completed. No AD migrations will occur during the Assessment phase. To help with the planning and creating a Migration plan for your application, reference the below considerations:

* Your Application technical teams are aware of the programme for AD One Domain Consolidation
* Review Windows Servers versions and ADFS versions such ADFS 2.0, ADFS 3.0, ADFS 4.0
* Identify all Domain Security/Permission Groups and Service Accounts required to run ADFS Services
* Identify if ADFS provides all or any Federation protocol such as SAML, WS-Fed, OAuth, or OpenID
* Identify if Application Authentication and/or Single Sign on is implemented using Windows Identity Foundation (WIF) which consumes and validates federation protocol from the ADFS Server. Also validate if the Windows Identity Federation Utility is used by the Application’s source code and configurations
* Identify Legacy AD Domain OU container for Users and Groups against which ADFS validates Users Credentials
* Validate if the ADFS server is connected to all Legacy AD Domains or specific AD Domains. Also check if AD one-Way Cross Domain Trusts or Two-way Cross Domain Trusts are established

**Migration strategy**

Where ADFS (Active Directory Federation Service) is used to connect to the legacy AD domain environment, it will need to be pointed to the new AD domain. To achieve this, the application's technical team needs to

* Consult AD Application Remediation team before making changes
* Consult AD Migration team for all changes required for ADFS Server such as Re-Hosting to new Windows Server or if migrating the existing server to the new AD Forest and Domain are required
* Plan to make changes for Domain Security/Permission Groups and Service Accounts needed to run ADFS Services when they are migrated to the new AD Forest and Domain
* Work with the Application team for changes, validation and testing needed by Windows Identity Foundation (WIF) and Windows Identity Federation Utility
* Plan to make changes for Federation configurations such as attributes, authentication, and assertion statements for SAML, WS-Fed, OAuth, and OpenID
* Plan to make changes for New AD Domain OU container for Users and Groups against which ADFS validates Users Credentials
* Will need to update the DN (Distinguished Name) to reference the new AD Forest and Domain for user logins and Applications using ADFS
* Perform the necessary testing and BCP testing

#### <<$Essso>>

**Considerations**

As part of Active Directory One Domain Consolidation, all current AD Domains and Forests will be migrated to a Single Forest and one AD domain. Currently there are 135 domain controllers and 3 AD Domains within scope of this project.

Phase 2 of the One Domain project will not begin until after the Assessment has been completed. No AD migrations will occur during the Assessment phase. To help with the planning and creating a Migration plan for your application, reference the below considerations:

* Your Application technical teams are aware of the programme for AD One Domain Consolidation
* Identify all Domain Security/Permission Groups and Service Accounts needed to run ESSO (Enterprise Single Sign on) Services
* Identify how many Platforms, Applications uses Enterprise Single Sign on Services
* Identify which are the Legacy AD Domains ESSO server is connected
* Identify Legacy AD Domain OU Containers for Users, Groups against which Users login to Platforms, Applications using ESSO Server Agents
* Identify if for enterprise, desktop SSO solution any Kerberos, NTLM authentication used and any SPNs (Service Principal Name) are configured

**Migration strategy**

Where ESSO (Enterprise Single Sign On) is used to connect to the legacy AD domain environment, it will need to be pointed to the new AD domain. To achieve this, the application's technical team needs to

* Consult AD Application Remediation team before making changes
* Consult AD Migration team for all changes required for ESSO Server such as migration to the new AD Forest and Domain or Re-Hosting to a new Windows Server connecting new AD Forest and Domain
* Will need to update the DN (Distinguished Name) to reference the new AD Forest and Domain for user logins and Applications using the ESSO Server.
* Update the ESSO server to use the new migrated Service and Domain Security Groups
* Update all SPN settings for Kerberos constrained delegated authentication
* Perform the necessary testing and BCP testing

#### <<$Other>>

**Considerations**

As part of Active Directory One Domain Consolidation, all current AD Domains and Forests will be migrated to a Single Forest and one AD domain. Currently there are 135 domain controllers and 3 AD Domains within scope of this project.

Phase 2 of the One Domain project will not begin until after the Assessment has been completed. No AD migrations will occur during the Assessment phase. To help with the planning and creating a Migration plan for your application, reference the below considerations:

* Your Application technical teams are aware of the programme for AD One Domain Consolidation
* Identify where this Other Authentication Type queries/uses the Legacy AD Domains, such as any centralized Authentication Framework, centralized Single Sign on Framework or any Custom Development Authentication Framework
* Identify if Other Authentication Server/Framework requires any Service Accounts, Admin Accounts, and/or Domain Security Groups from Legacy AD Domain
* Identify Other Authentication Server/Framework use cases related to Legacy AD Domain such as AD OU DNs, User DNs, or Group DNs
* Identify if Custom Authentication Framework supports Kerberos and/or NTLM Authentication for which SPNs are set up

**Migration strategy**

Where Other Authentication Services are used to connect to the legacy AD domain environment, they will need to be pointed to the new AD domain. To achieve this, the application's technical team needs to

* Consult AD Application Remediation team before making changes
* Consult AD Migration team for all changes required for the Other Auth Server such as migration to the new AD Forest and Domain or Re-Hosting to a new Windows Server connecting new AD Forest and Domain
* Plan to make changes for New AD Domain OU Containers for Users, Groups against which Users login to Platforms and Applications using Other Auth Server
* Will need to update the DN (Distinguished Name) to reference the new AD Forest and Domain for user logins and Applications using the Other Auth Server.
* Plan to make changes in Other Auth server for Service Accounts and Domain Security Groups
* Plan to change all SPN settings for Kerberos constrained delegated authentication
* Perform the necessary testing and BCP testing

#### <<$Does not use AD for any authentication>>

This application doesn’t use AD based authentication, so no changes are required.

## Authentication Mechanism

This application uses **<<$Authetication\_Mechanism>>** as an Authentication protocol mechanism, below are some considerations and migration strategies for this selected Authentication mechanism.

#### <<$Kerberos>>

**Considerations**

As part of Active Directory One Domain Consolidation, all current AD Domains and Forests will be migrated to a Single Forest and one AD domain. Currently there are 135 domain controllers and 3 AD Domains within scope of this project.

Phase 2 of the One Domain project will not begin until after the Assessment has been completed. No AD migrations will occur during the Assessment phase. To help with the planning and creating a Migration plan for your application, reference the below considerations:

* Your Application technical teams are aware of the programme for AD One Domain Consolidation
* Identify all places where hardcoded AD details (host and port) or hardcoded IP addresses are used by your authentication server.
* If Kerberos is installed on a non-windows operating system then continue with the existing operating system.
* Identify and list all SPNs, if SPNs and associated service/technical accounts are used for Kerberos authentication
* Identify all SPNs used for Service to Service Authentication across different Application Servers
* Identity all SPNs used for HTTPS(web) on Server where Service is running

**Migration strategy**

Kerberos Authentication using the legacy AD domain environment needs to be updated to authenticate through the new AD domain. To achieve this, the application's technical team needs to

* Consult AD Application Remediation team before making changes
* Update SPNs to reference the new AD Domain and with new lists of Service Accounts
* Change SPNs for Kerberos Authentication for Service to Service Communication
* Change SPNs used for HTTPS(web) on Server where Service is running
* Register the new host in the new AD domain and setup Kerberos authentication.
* Perform the necessary testing and BCP testing.

#### <<$NTLM>>

**Considerations**

As part of Active Directory One Domain Consolidation, all current AD Domains and Forests will be migrated to a Single Forest and one AD domain. Currently there are 135 domain controllers and 3 AD Domains within scope of this project.

Phase 2 of the One Domain project will not begin until after the Assessment has been completed. No AD migrations will occur during the Assessment phase. To help with the planning and creating a Migration plan for your application, reference the below considerations:

* Your Application technical teams are aware of the programme for AD One Domain Consolidation
* Identify all Service/technical accounts are used for authentication
* Identity your Application Server configurations for NTLM related settings
* Identify Applications which uses desktop single sign on using NTLM authentication
* Identify all places where hardcoded AD details (host and port) or hardcoded IP addresses are used on your authentication server
* If authentication components are installed on a non-windows operating system then continue with the existing operating system

**Migration strategy**

NTLM Authentication using the legacy AD domain environment needs to be updated to authenticate through the new AD domain. To achieve this, the application's technical team needs to

* Consult AD Application Remediation team before making changes
* Register the new host in new AD domain and setup Desktop SSO-NTLM authentication.
* Perform the necessary testing and BCP testing

#### <<$Oauth>>

**Considerations**

As part of Active Directory One Domain Consolidation, all current AD Domains and Forests will be migrated to a Single Forest and one AD domain. Currently there are 135 domain controllers and 3 AD Domains within scope of this project.

Phase 2 of the One Domain project will not begin until after the Assessment has been completed. No AD migrations will occur during the Assessment phase. To help with the planning and creating a Migration plan for your application, reference the below considerations:

* Your Application technical teams are aware of the programme for AD One Domain Consolidation
* Identify the Federation Server which issues OAUTH token for the Identity Server and whether and how the Federation server connects to the Legacy Domain (e.g. ADFS 3.0, ADFS 4.0)
* Validate if OAUTH token contains attributes from Legacy AD Domain

Identity all possible Legacy AD domain objects such as AD container, AD Groups, and Service Accounts

**Migration strategy**

OAUTH Authentication using the legacy AD domain environment needs to be updated to authenticate to the new AD domain. To achieve this, the application's technical team needs to

* Consult AD Application Remediation team before making changes
* Update your Application’s Identity Management Federation Service for OAUTH configuration to use the new AD domain
* Register the new host in new AD domain and setup OAUTH authentication
* Perform the necessary testing and BCP testing.

#### <<$OpenID>>

**Considerations**

As part of Active Directory One Domain Consolidation, all current AD Domains and Forests will be migrated to a Single Forest and one AD domain. Currently there are 135 domain controllers and 3 AD Domains within scope of this project.

Phase 2 of the One Domain project will not begin until after the Assessment has been completed. No AD migrations will occur during the Assessment phase. To help with the planning and creating a Migration plan for your application, reference the below considerations:

* Your Application technical teams are aware of the programme for AD One Domain Consolidation
* Validate if the Identity Federation Server which issues OpenID tokens for Identity Server uses a Federation server that connects to the Legacy Domain (e.g. ADFS 3.0, ADFS 4.0)
* Validate if OpenID token contains attributes from Legacy AD Domain
* Identify all possible Legacy AD domain objects such as AD container, AD Groups, and Service Accounts

**Migration strategy**

OpenID Authentication using the legacy AD domain environment needs to be updated to authenticate through the new AD domain. To achieve this, the application's technical team needs to

* Consult AD Application Remediation team before making changes
* Validate if the Identity Management Federation Service for OpenID related configurations are needed in your Application
* Register the new host in new AD domain and setup OpenID authentication
* Perform the necessary testing and BCP testing.

#### <<$SAML>>

**Considerations**

As part of Active Directory One Domain Consolidation, all current AD Domains and Forests will be migrated to a Single Forest and one AD domain. Currently there are 135 domain controllers and 3 AD Domains within scope of this project.

Phase 2 of the One Domain project will not begin until after the Assessment has been completed. No AD migrations will occur during the Assessment phase. To help with the planning and creating a Migration plan for your application, reference the below considerations:

* Your Application technical teams are aware of the programme for AD One Domain Consolidation
* Validate if the Identity Federation Server which issues SAML tokens for Identity Server uses a Federation server that connects to the Legacy Domain (e.g. ADFS 3.0, ADFS 4.0)
* Validate if SAML tokens contain attributes from Legacy AD Domain
* Identity all possible Legacy AD domain objects such as AD container, AD Groups, and Service Accounts

**Migration strategy**

SAML Authentication using the legacy AD domain environment needs to be updated to authenticate through the new AD domain. To achieve this, the application's technical team needs to

* Consult AD Application Remediation team before making changes
* Validate if the Identity Management Federation Service for SAML related configurations are needed in your Application
* Register the new host in new AD domain and setup SAML authentication
* Perform the necessary testing and BCP testing.

#### <<$Other>>

**Considerations**

As part of Active Directory One Domain Consolidation, all current AD Domains and Forests will be migrated to a Single Forest and one AD domain. Currently there are 135 domain controllers and 3 AD Domains within scope of this project.

Phase 2 of the One Domain project will not begin until after the Assessment has been completed. No AD migrations will occur during the Assessment phase. To help with the planning and creating a Migration plan for your application, reference the below considerations:

* Your Application technical teams are aware of the programme for AD One Domain Consolidation
* Identify what are other Authentication Protocols might be used such as HTTPS (SSL Certificate), BASIC Authentication, FORM based Authentication used where Legacy AD Domain is queried for Authentication
* Identify if application uses AD authentication through headers or custom tokens
* Identify all places where hardcoded AD details (host and port) or hardcoded IP addresses are used in your authentication server
* Identity all Legacy AD Domain Service Accounts and AD Domain Security Groups used by your Application

**Migration strategy**

Any Other Authentication services using the legacy AD domain environment need to be updated to authenticate through the new AD domain. To achieve this, the application's technical team needs to

* Consult AD Application Remediation team before making changes
* Make changes for HTTPS, BASIC AUTH, FORM Based Authentication
* Replace Legacy AD Domain Service Accounts and Domain Security groups with the same objects in the New AD Domain
* Perform the necessary testing and BCP testing.

#### <<$None\_Authetication\_Mechanism>>

Application doesn’t use any authentication mechanism which are Legacy AD dependent so no changes are required.

## Application Cross Domain

**Assessment Response**

Based on the Application Assessment details we collected from your Application Team Owner this application is configured to use multiple AD domains.

If an application is hosted/deployed on servers connected to any of the following active directory Domains, DMN1, FMRCO and DSDOM1, please validate the domain names are correct.

**Considerations**

As part of Active Directory One Domain Consolidation, all current AD Domains and Forests will be migrated to a Single Forest and one AD domain. Currently there are 135 domain controllers and 3 AD Domains within scope of this project.

Phase 2 of the One Domain project will not begin until after the Assessment has been completed. No AD migrations will occur during the Assessment phase. To help with the planning and creating a Migration plan for your application, reference the below considerations:

* Your Application technical teams are aware of the programme for AD One Domain Consolidation.
* Identity all Places in the application (e.g. source code, configurations) where AD cross domain authentication, AD groups and group membership is used.
* Identify all places where *host details* (FQDN, DN, host, port, etc.)are used in your application configuration.
* Identity all Places in the application (e.g. Servers) where an *AD cross domain trust* is used.
* Verify if there is any authentication dependency on a local login script being executed.

**Migration strategy**

Where legacy AD domain values are used in application configurations they will need to be replaced with the new domain information. To achieve this, the application's technical owner needs to:

* Consult the AD Application Remediation team before making changes in terms of re-hosting your server connecting to new AD Domain
* Consult the AD Application Remediation team and share your timeline and migration plan
* Change Application Server connectivity details for new AD cross domain trust (e.g. One-way trust, cross domain trust).
* **If Application hosted/deployed servers is not connected to any of these active directory Domains (DMN1, FMRCO and DSDOM1), no changes are required.**

## Application SSL Certificate

**Assessment Response**

Based on Application Assessment, details we collected from your Application Owner, validate all Certificates, which are registered against active directory domains.

**Considerations**

As part of Active Directory One Domain Consolidation, all current AD Domains and Forests will be migrated to a Single Forest and one AD domain. Currently there are 135 domain controllers and 3 AD Domains within scope of this project.

Phase 2 of the One Domain project will not begin until after the Assessment has been completed. No AD migrations will occur during the Assessment phase. To help with the planning and creating a Migration plan for your application, reference the below considerations:

* Your Application technical teams are aware of the programme for AD One Domain Consolidation
* Validate all SSL Certificates Issue Date, Expiry Date, Root CA, Intermediate CA details
* Validate if SSL Certificate is issued from Internal Active Directory Certificate Service (ADCS) and from to which Legacy AD domain
* Validate if SSL certificate is used from external 3rd Party ADCS such as Verizon and does the external certificate has any internal ADCS dependency
* Identity if SSL certificates are stored at Key Store such as Java Key Store (JKS) and protected by secret encryption keys. Also validate if SSL certificates are managed centrally at HSM (Hardware Security Module)
* Validate if SSL Certificates are used for One way SSL Or Two Way SSL Authentication by Applications before allowing Users access to Applications
* Identify all Client side and Server side SSL certificates
* Identify if WebServices API’s use SSL certificates for signing or authenticating services

**Migration strategy**

Where legacy AD domain values might be used by SSL certificates they will need to be replaced with new SSL certificates from new AD domain. To achieve this, the application's technical team needs to:

* Consult AD Application Remediation team before making changes
* Request new SSL Certificate from new Internal Active Directory Certificate Service (ADCS) and from new AD domain
* Import new SSL Certificate to Key Store such as Java Key Store (JKS) or HSM
* Make changes to Application for One way SSL Or Two Way SSL Authentication
* Change all Client side, server side certificates and new SSL certificates
* Change WebServices API’s for new SSL certificates and for signing, authenticating services
* Perform the necessary testing and BCP testing.
* **If this application does not use SSL certificates so no changes are required.**

## Local Accounts Creation

If this application uses local accounts, below are some considerations and migration strategies.

#### <<$Yes\_Local\_Accounts>>

**Considerations**

As part of Active Directory One Domain Consolidation, all current AD Domains and Forests will be migrated to a Single Forest and one AD domain. Currently there are 135 domain controllers and 3 AD Domains within scope of this project.

Phase 2 of the One Domain project will not begin until after the Assessment has been completed. No AD migrations will occur during the Assessment phase. To help with the planning and creating a Migration plan for your application, reference the below considerations:

* Your Application technical teams are aware of the programme for AD One Domain Consolidation
* Identify if your Application requires Admin or Service Accounts from legacy AD Domain
* Identify if the Application Server uses only Local Computer Accounts and Local Admin Groups
* Validate with legacy Domain AD team if Local Computer Accounts are Synched offline to a Legacy AD Domain
* Validate if Domain Member Servers use Local Accounts and if migration to a new domain will have any impact

**Migration strategy**

Where Local Computer Accounts are used to connect to the legacy AD domain environment, they will need to be pointed to the new AD domain. To achieve this, the application's technical team needs to

* Consult AD Application Remediation team before making changes
* Consult AD Migration team for all changes required for the Application Server such as migration to the new AD Forest and Domain or Re-Hosting to a new Windows Server connecting new AD Forest and Domain
* Plan to update any Local Computer Accounts if these Accounts are synchronized to AD Domain
* Perform the necessary testing and BCP testing

#### <<$No\_Local\_Accounts>>

Application doesn’t use any local computer account, no changes are required

## Application Forest Domain Name

#### <<$DMN1>>

This application is integrated with **<<$Forest\_Domain\_Name>>** Forest, Please find the below Considerations and Migration Strategy.

**Assessment Response**

Based on the Application Assessment for Active Directory Integration, the application is registered in the DMN1 Active Directory domain. Please validate the correct domain names.

**Considerations**

As part of Active Directory One Domain Consolidation, all current AD Domains and Forests will be migrated to a Single Forest and one AD domain. Currently there are 135 domain controllers and 3 AD Domains within scope of this project.

Phase 2 of the One Domain project will not begin until after the Assessment has been completed. No AD migrations will occur during the Assessment phase. To help with the planning and creating a Migration plan for your application, reference the below considerations:

* Your Application technical teams are aware of the programme for AD One Domain Consolidation.
* Identify all Places in the application (e.g. source code, configurations, and servers) where AD Domain DMN1 is used or referenced.
* Plan for changing your Application configurations, servers, and source code to reference the new AD Domain once the AD consolidation begins.

**Migration strategy**

Where legacy AD domain values are used in application configurations they will need to be replaced with the new domain information. To achieve this, the application's technical owner needs to:

* Consult AD Application Remediation team before making changes to receive the new AD domain information
* Change Application source code, configurations related to AD domain authentication, AD groups and group memberships
* Validate with AD team new AD infrastructure in place to allow application to run within the new environment (e.g. Appropriate trusts are in place, necessary objects migrated, any used services are in place and accessible, etc.)
* Arrange for the migration of the host/server to a new domain where needed
* Reconfigure the existing application to access the service in the new domain
* Arrange for testing and BCP testing

#### <<$FMRCO>>

This application is integrated with **<<$Forest\_Domain\_Name>>** Forest. Please find the below Considerations and Migration Strategy.

**Assessment Response**

Based on the Application Assessment for Active Directory Integration, the application is registered in the FMRCO Active Directory domain. Please validate the correct domain names.

**Considerations**

As part of Active Directory One Domain Consolidation, all current AD Domains and Forests will be migrated to a Single Forest and one AD domain. Currently there are 135 domain controllers and 3 AD Domains within scope of this project.

Phase 2 of the One Domain project will not begin until after the Assessment has been completed. No AD migrations will occur during the Assessment phase. To help with the planning and creating a Migration plan for your application, reference the below considerations:

* Your Application technical teams are aware of the programme for AD One Domain Consolidation.
* Identify all Places in the application (e.g. source code, configurations, and servers) where AD Domain FRMCO is used or referenced.
* Plan for changing your Application configurations, servers, and source code to reference the new AD Domain once the AD consolidation begins.

**Migration strategy**

Where legacy AD domain values are used in application configurations they will need to be replaced with the new domain information. To achieve this, the application's technical owner needs to:

* Consult AD Application Remediation team before making changes to receive the new AD domain information
* Change Application source code and configurations related to AD domain authentication, AD groups and group memberships
* Validate with AD team new AD infrastructure in place to allow application to run within the new environment (e.g. Appropriate trusts are in place, necessary objects migrated, any used services are in place and accessible, etc.)
* Arrange for the migration of the host/server to a new domain where needed
* Reconfigure the existing application to access the service in the new domain
* Arrange for testing and BCP testing

#### <<$DSDOM1>>

This application is integrated with **<<$Forest\_Domain\_Name>>** Forest. Please find the below Considerations and Migration Strategies.

**Assessment Response**

Based on the Application Assessment for Active Directory Integration, the application is registered in the DSDOM1 Active Directory domain. Please validate the correct domain names.

**Considerations**

As part of Active Directory One Domain Consolidation, all current AD Domains and Forests will be migrated to a Single Forest and one AD domain. Currently there are 135 domain controllers and 3 AD Domains within scope of this project.

Phase 2 of the One Domain project will not begin until after the Assessment has been completed. No AD migrations will occur during the Assessment phase. To help with the planning and creating a Migration plan for your application, reference the below considerations:

* Your Application technical teams are aware of the programme for AD One Domain Consolidation.
* Identify all Places in the application (e.g. source code, configurations, servers) where AD Domain DSDOM1 is used or referenced.
* Plan for changing your Application configurations, servers, and source code to reference the new AD Domain once the AD consolidation begins.

**Migration strategy**

Where legacy AD domain values are used in application configurations they will need to be replaced with the new domain information. To achieve this, the application's technical owner needs to:

* Consult AD Application Remediation team before making changes to receive the new AD domain information
* Change Application source code, configurations related to AD domain authentication, AD groups, and group memberships
* Validate with AD team new AD infrastructure in place to allow application to run within the new environment (e.g. Appropriate trusts are in place, necessary objects migrated, any used services are in place and accessible, etc.)
* Arrange for the migration of the host/server to a new domain where needed
* Reconfigure the existing application to access the service in the new domain
* Arrange for testing and BCP testing.

#### <<$INTL>>

**Assessment Response**

Based on Application Assessment for Active Directory Integrations, Active Directory domain name where application is registered are INTL. Details are collected from your Application Team, Owner at DTM SAM survey. Please validate the correct domain names.

**Considerations**

As part of Active Directory One Domain Consolidation, all current AD Domains and Forests will be migrated to a Single Forest and one AD domain. Currently there are 135 domain controllers and 3 AD Domains within scope of this project.

Phase 2 of the One Domain project will not begin until after the Assessment has been completed. No AD migrations will occur during the Assessment phase. To help with the planning and creating a Migration plan for your application, reference the below considerations:

* Your Application technical teams are aware of the programme for AD One Domain Consolidation.
* Identify all Places in the application (e.g. source code, configurations, servers) where AD Domain INTL is used or referenced.
* Plan for changing your Application configurations, servers, and source code to reference the new AD Domain once the AD consolidation begins.

**Migration strategy**

Where legacy AD domain values are used in application configurations they will need to be replaced with the new domain information. To achieve this, the application's technical owner needs to:

* Consult AD Application Remediation team before making changes to receive the new AD domain information
* Change Application source code, configurations related to AD domain authentication, AD groups and group memberships
* Validate with AD team new AD infrastructure in place to allow application to run within the new environment (e.g. Appropriate trusts are in place, necessary objects migrated, any used services are in place and accessible, etc.)
* Arrange for the migration of the host/server to a new domain where needed
* Reconfigure the existing application to access the service in the new domain
* Arrange for testing and BCP testing.

#### <<$Other>>

**Assessment Response**

Based on Application Assessment, details we collected from your Application Team, Owner at DTM SAM survey Application are below. Please validate Other Domain Details.

**Considerations**

As part of Active Directory One Domain Consolidation, all current AD Domains and Forests will be migrated to a Single Forest and one AD domain. Currently there are 135 domain controllers and 3 AD Domains within scope of this project.

Phase 2 of the One Domain project will not begin until after the Assessment has been completed. No AD migrations will occur during the Assessment phase. To help with the planning and creating a Migration plan for your application, reference the below considerations:

* Your Application technical teams are aware of the programme for AD One Domain Consolidation.
* Identify all Places in the application (e.g. source code, configurations, servers) where the current AD Domain is used or referenced.
* Plan for changing your Application configurations, servers, and source code to reference the new AD Domain once the AD consolidation begins.

**Migration strategy**

Where legacy AD domain values are used in application configurations they will need to be replaced with the new domain information. To achieve this, the application's technical owner needs to:

* Consult AD Application Remediation team before making changes to receive the new AD domain information
* Change Application source code, configurations related to AD domain authentication, AD groups and group memberships
* Validate with AD team new AD infrastructure in place to allow application to run within the new environment (e.g. Appropriate trusts are in place, necessary objects migrated, any used services are in place and accessible, etc.)
* Arrange for the migration of the host/server to a new domain where needed
* Reconfigure the existing application to access the service in the new domain
* Arrange for testing and BCP testing.

## Application Service Account

**Assessment Response**

Based on Application Assessment, details we collected from your Application Team Owner, validate all service/operational accounts created in the legacy Active Directory domain to administrate your application are migrated to the new domain.

**Considerations**

As part of Active Directory One Domain Consolidation, all current AD Domains and Forests will be migrated to a Single Forest and one AD domain. Currently there are 135 domain controllers and 3 AD Domains within scope of this project.

Phase 2 of the One Domain project will not begin until after the Assessment has been completed. No AD migrations will occur during the Assessment phase. To help with the planning and creating a Migration plan for your application, reference the below considerations:

* Your Application technical teams are aware of the programme for AD One Domain Consolidation
* Identify all Service Accounts used by Databases such as Service Accounts used to Authenticate/Start/Stop Databases (e.g. Service Account Name “SA-SQL-P”) and associated SQL Global Permission Group (R-) (e.g. Prefix-SQL Server-Database-Access Level "R-SQL-AllSQLServers-X")
* Identify all Service Accounts used to run Service to Service Level Authentication (e.g. SPN) set for Kerberos Authentication which enables Kerberos to securely communicate with the Service such as setspn –s ABCDAppService/Server Address domain\ SA-Service Account. And associated Service Permission Groups (e.g. Prefix-SERVER-Service Display Name -AccessLevel “P-SMPWEBM05-ComputerBrowser-R”)
* Identify all Service Accounts running HTTPS(web) on server which requires Service Accounts for seamless access (e.g. setspn –s HTTPS/Server Address domain\ SA-Service Account)
* Identify all Domain Security Groups (e.g. SCSM) and associated Service Accounts used on Application Hosted Server
* Identify all Application pools using a service account to run the web service under that SA account (e.g. Role Group, Service Account) configurations in IIS configuration files
* Identify all Service Accounts used by Identity Access Management Tools which require Service Accounts to run or authenticate services against Legacy AD domains such as ADFS, Microsoft Identity Manager, ADAM, Active Role Server and all others.

**Migration strategy**

Where Service Accounts from legacy AD domain might be used they will need to be replaced with new Service Accounts from new AD domain. To achieve this, the application's technical team needs to:

* Consult AD Application Remediation team before making changes
* Change Service Accounts configurations to new AD Domain to run Databases
* Change Service Accounts configurations to new AD Domain to run service to service communications
* Change Service Accounts configurations to new AD Domain for running HTTPS(web) on Server
* Change Service Accounts configurations to utilize Domain Security Groups from the new AD Domain
* Change Service Accounts configurations from new AD Domain to run Application Pool
* Change all Service Accounts configurations to new AD Domain for LDAP services, IAM services
* Perform the necessary testing and BCP testing

**Note # If this application does not use Service Accounts no changes are required.**

## File and Registry Permissions

#### <<$None\_File\_and\_Registry\_Permissions>>

Since the Application doesn’t use any File and Registry Permission no change is required.

#### <<$Dynamic File Structure>>

This Application uses Dynamic Files Structure, below are some considerations and migration strategies.

**Considerations**

As part of Active Directory One Domain Consolidation, all current AD Domains and Forests will be migrated to a Single Forest and one AD domain. Currently there are 135 domain controllers and 3 AD Domains within scope of this project.

Phase 2 of the One Domain project will not begin until after the Assessment has been completed. No AD migrations will occur during the Assessment phase. To help with the planning and creating a Migration plan for your application, reference the below considerations:

* Your Application technical teams are aware of the programme for AD One Domain Consolidation
* Identify full name and path of the file which application uses (e.g. names of DFS Paths or UNC Paths)
* Identify the Service accounts used to access DFS
* Identify system or domain hosting file on the file server which uses Legacy AD Domain
* Identify all File Permission Groups (e.g. Prefix-Server-FolderandFilePath[(#)]-AccessLevel "P-SMPFILEP01-D-Data-Employee Benefits-HR-Documentat-W2.Doc(1)-RW")
* Identify all Folder Permission Groups (e.g. Prefix-Server-Folder Path[(#)]-Access Level "P-SMPWEBM05-D-Apps-Siebel-Rx")
* Identify all Server Share Permission Groups (e.g. Prefix-Server-ShareName-AccessLevel "P-SMPWEBM05-APPS-R")
* Identify all DFS Folder Permission Groups (e.g. Prefix-Domain-DFS Root-DFS Link Name/Folder Path -AccessLevel "P-C-AllLocations-AllDepartments-R")

**Migration strategy**

Where Dynamic files Structure groups and service accounts from legacy AD domain might be used they need to be replaced with DFS service accounts, and groups from new AD domain. To achieve this, the application's technical team needs to:

* Consult AD Application Remediation team before making changes.
* Make changes to system or domain hosting file on the file server connecting to thenew AD Domain.
* Make changes to All Service Accounts, File Permission Groups, Folder Permission Groups, Server Share Permission Groups, and DFS Folder Permission Groups connecting to the new AD Domain.
* Update the full name, DFS Paths, and UNC Paths of the file.
* Arrange for necessary testing and BCP testing.

#### <<$Registry Permission>>

This Application uses Registry Permission, below are some considerations and migration strategies.

**Considerations**

As part of Active Directory One Domain Consolidation, all current AD Domains and Forests will be migrated to a Single Forest and one AD domain. Currently there are 135 domain controllers and 3 AD Domains within scope of this project.

Phase 2 of the One Domain project will not begin until after the Assessment has been completed. No AD migrations will occur during the Assessment phase. To help with the planning and creating a Migration plan for your application, reference the below considerations:

* Your Application technical teams are aware of the programme for AD One Domain Consolidation
* Identify all file/folder/registry permissions and GPOs required for the application
* Identify all Registry Permission Groups in the Legacy AD Domain (e.g. Prefix-Server-Full Name Registry Entry[(#)]-AccessLevel "P-SMPWEBM05-HKLMSYSTEMCurrentControlSetServiceslanmans(1)-R")
* Identify any Registry entries in your Application Server, any hardcoded Legacy AD details (FQDN, host and port) or hardcoded IP addresses used

**Migration strategy**

Where Registry Permission Group, AD entries from legacy AD domain might be used they will need to be replaced with references to the new AD domain. To achieve this, the application's technical team needs to:

* Consult AD Application Remediation team before making changes
* Make changes to registry permissions connecting new AD Domain in your Application hosted Server
* Make changes to Registry Permission Group
* Make changes to hardcoded Legacy AD details (FQDN, host and port) or hardcoded IP addresses in the Registry connecting to the new AD Domain
* Arrange for necessary testing and BCP testing

#### <<$NAS>>

This Application uses NAS, below are some considerations and migration strategies.

**Considerations**

As part of Active Directory One Domain Consolidation, all current AD Domains and Forests will be migrated to a Single Forest and one AD domain. Currently there are 135 domain controllers and 3 AD Domains within scope of this project.

Phase 2 of the One Domain project will not begin until after the Assessment has been completed. No AD migrations will occur during the Assessment phase. To help with the planning and creating a Migration plan for your application, reference the below considerations:

* Your Application technical teams are aware of the programme for AD One Domain Consolidation
* Identify names along with FQDN (Fully qualified domain name) of Network storage server or NAS used by application.
* Identify how Network storage is associated with application

**Migration strategy**

Where Network storage server or NAS from legacy AD domain environment might be used they will need to be replaced from new AD domain. To achieve this, the application's technical team needs to

* Consult AD Application Remediation team before making changes.
* Application uses Network Storage to store data manually or triggered by an event after authenticating against AD. Make sure each of the storage components and servers where this storage is installed are migrated to the new AD domain.
* Perform necessary testing and BCP testing.

**Note** – To request registration of new storage servers on a new AD domain, raise a request.

#### <<$SAN>>

This Application uses SAN, below are some considerations and migration strategies.

**Considerations**

As part of Active Directory One Domain Consolidation, all current AD Domains and Forests will be migrated to a Single Forest and one AD domain. Currently there are 135 domain controllers and 3 AD Domains within scope of this project.

Phase 2 of the One Domain project will not begin until after the Assessment has been completed. No AD migrations will occur during the Assessment phase. To help with the planning and creating a Migration plan for your application, reference the below considerations:

* Your Application technical teams are aware of the programme for AD One Domain Consolidation
* Identify names along with FQDN (Fully qualified domain name) of Network, storage server, or SAN used by application.

**Migration strategy**

Where SAN from legacy AD domain environment might be used they will need to be replaced from new AD domain. To achieve this, the application's technical team needs to

* Consult AD Application Remediation team before making changes
* Application uses Network Storage to store data manually or triggered by an event after authenticating against AD. Make sure each of the storage components and servers where this storage is installed are migrated to the new AD domain.
* Perform necessary testing and BCP testing.

**Note** – To request registration of new storage servers on a new AD domain, raise a request.

## Application Access Method

This application is accessed by users where Legacy AD user IDs are copied directly in the Application Database, below are some considerations and migration strategies.

#### <<$Direct Application Access>>

**Considerations**

As part of Active Directory One Domain Consolidation, all current AD Domains and Forests will be migrated to a Single Forest and one AD domain. Currently there are 135 domain controllers and 3 AD Domains within scope of this project.

Phase 2 of the One Domain project will not begin until after the Assessment has been completed. No AD migrations will occur during the Assessment phase. To help with the planning and creating a Migration plan for your application, reference the below considerations:

* Your Application technical teams are aware of the programme for AD One Domain Consolidation
* Identify if application is accessed directly by users using Legacy AD User Id. List if there are any exceptions.
* Identify how the access to this application is requested by a user.
* Identify if and how any Identity Management Tool provisions Legacy AD User IDs to this Application Database

**Migration strategy**

Legacy AD domain User IDs will need to be replaced with User IDs from new AD domain. To achieve this, the application's technical team needs to

* Consult AD Application Remediation team before making changes
* Consult AD team post AD Migration to find new AD User ID and DN of User ID
* Consult Identity Management team if there will be a change in User Provisioning/De-Provisioning Process to delete/update new AD User IDs in Application Database
* Make changes to your Application source code and configurations connecting to the new AD domain for Authentication and Authorization
* Perform necessary testing and BCP testing.

#### <<$Based on Group membership>>

This application is accessed based on Legacy AD domain group membership. Below are some considerations and migration strategy.

**Considerations**

As part of Active Directory One Domain Consolidation, all current AD Domains and Forests will be migrated to a Single Forest and one AD domain. Currently there are 135 domain controllers and 3 AD Domains within scope of this project.

Phase 2 of the One Domain project will not begin until after the Assessment has been completed. No AD migrations will occur during the Assessment phase. To help with the planning and creating a Migration plan for your application, reference the below considerations:

* Your Application technical teams are aware of the programme for AD One Domain Consolidation
* Identify all Role Groups (R-) (e.g. domain global groups), which are used to group user accounts which are normally used to simplify granting access to Users
* Identify Permission Groups (P-) (e.g. all Application Permission Groups, all SQL Global Permission Groups, all Service Permission Groups, all Folder Permission Groups, all File Permission Groups, and all Server Share Permission Groups) used from Legacy AD Domain
* Identify if Application Portal Server is configured to use the Legacy AD domain for Group Based authorization for Portlets, Pages, and Entitlements
* Identify if your Application Manages AD Groups in Application Database and how the AD groups are synchronized from Legacy AD domain

**Migration strategy**

Where User IDs from the legacy AD domain environment are used they will need to be replaced with User IDs from the new AD domain. To achieve this, the application's technical team needs to

* Consult AD Application Remediation team before making changes
* Consult AD Migration team for all changes required for Permission and Role Groups
* Make changes to your Application Portal Server Configurations related to new AD configuration for Group based authorization of Pages, Portlets, and Entitlements
* Perform necessary testing and BCP testing

#### <<$Based on Rule/Policy>>

This application is accessible based on Rules/Policies. Below are some considerations and migration strategies.

**Considerations**

As part of Active Directory One Domain Consolidation, all current AD Domains and Forests will be migrated to a Single Forest and one AD domain. Currently there are 135 domain controllers and 3 AD Domains within scope of this project.

Phase 2 of the One Domain project will not begin until after the Assessment has been completed. No AD migrations will occur during the Assessment phase. To help with the planning and creating a Migration plan for your application, reference the below considerations:

* Your Application technical teams are aware of the programme for AD One Domain Consolidation
* Identify if your Application is dependent on GPOs (Group Policy Object), defined groups of users, computer accounts from any existing Legacy AD Domain, and/or specific Domain Controllers
* Identify if your Application Server is dependent on Legacy AD Forest’s network, based on defined rules such as Server Access and One-Way trusts established with AD Forest
* Identify the Rules/Policy which are used to segregate functionality and access to the application by any means (e.g. registry based policy, folder redirection, etc.)

**Migration strategy**

Where GPOs, Rules, and Policies from legacy AD domain environment are used, they will need to be replaced with similar GPOs, Rules, and Policies in new AD domain. To achieve this, the application's technical team needs to.

* Consult AD Application Remediation team before making changes
* Consult AD Migration team for all changes required for GPOs, Computer Accounts, and Users/Groups
* Make changes to your Application server configurations by re-hosting to connect to the new AD Domain, to use new GPOs, and Computer Accounts
* Request for Rule/Policy configuration from the new AD domain for the application
* Perform necessary testing and BCP testing.

#### <<$Other>>

This application is accessible based on some other method. Below are some considerations and migration strategies.

**Considerations**

As part of Active Directory One Domain Consolidation, all current AD Domains and Forests will be migrated to a Single Forest and one AD domain. Currently there are 135 domain controllers and 3 AD Domains within scope of this project.

Phase 2 of the One Domain project will not begin until after the Assessment has been completed. No AD migrations will occur during the Assessment phase. To help with the planning and creating a Migration plan for your application, reference the below considerations:

* Your Application technical teams are aware of the programme for AD One Domain Consolidation
* Identify all other access method used to connect to the Legacy AD Domain
* Identify all Service/technical accounts, Local Accounts, Computer Accounts used for authentication from Legacy AD Domain
* Identify your Application Server configurations for Legacy AD related settings
* Identify all places where hardcoded AD details (host and port) or hardcoded IP addresses are used in your authentication server

**Migration strategy**

Where Other Access Methods are used to connect legacy AD domain environment, they will need to be replaced with similar Access Methods to the new AD domain. To achieve this, the application's technical team needs to

* Consult AD Application Remediation team before making changes
* Register the new host in new AD domain and test connectivity for authentication
* Change all places where hardcoded AD details (host and port) or hardcoded IP addresses are used
* Change all Service/technical accounts, Local Accounts, and Computer Accounts
* Perform the necessary testing and BCP testing.

## Application Dependency

This application has dependencies with other applications, below are some considerations and migration strategies.

**Considerations**

As part of Active Directory One Domain Consolidation, all current AD Domains and Forests will be migrated to a Single Forest and one AD domain. Currently there are 135 domain controllers and 3 AD Domains within scope of this project.

Phase 2 of the One Domain project will not begin until after the Assessment has been completed. No AD migrations will occur during the Assessment phase. To help with the planning and creating a Migration plan for your application, reference the below considerations:

* Your Application technical teams are aware of the programme for AD One Domain Consolidation
* Find out which Centralized Authentication Server, Framework has your Application dependent and indirectly uses Legacy AD Domain
* Find out if your Application has any authentication dependency on a login script being executed
* Identify all places where host details (FQDN, DN, host, port, etc.) are used in the Application configuration from Legacy AD Domain

Validate if the Application has a Legacy AD Dependency such as if users of the Application authenticate against Legacy AD

**Migration strategy**

Where Other Applications are dependent on your Application’s querying the legacy AD domain environment, they will need to be pointed to the new AD domain. To achieve this, the application's technical team needs to

* Consult AD Application Remediation team before making changes
* Consult AD Migration team for all changes required for the Application Server such as migration to the new AD Forest and Domain or Re-Hosting to a new Windows Server connecting new AD Forest and Domain
* Validate if there are other Application dependency for authentication against the Legacy AD and plan to make changes in all the places where a specific AD OU, User DN, Group DN, Service Accounts, AD Groups are used
* Perform the necessary testing and BCP testing

**If Application doesn’t have any Dependencies on other applications, then no changes are required.**

## Application Host Model

Based on Application Assessment, details we collected from your Application Team Owner, this application is of type <<$Host\_Model>> Application, please find the below Considerations and migration strategy.

#### <<$Web-Based>>

**Considerations**

As part of Active Directory One Domain Consolidation, all current AD Domains and Forests will be migrated to a Single Forest and one AD domain. Currently there are 135 domain controllers and 3 AD Domains within scope of this project.

Phase 2 of the One Domain project will not begin until after the Assessment has been completed. No AD migrations will occur during the Assessment phase. To help with the planning and creating a Migration plan for your application, reference the below considerations:

* Your Application technical teams are aware of the programme for AD One Domain Consolidation
* If your web server is on non-windows operating system then continue with the existing operating system
* Identify all places where hardcoded AD detail (host and port) or hardcoded IP address is used in the application web server e.g. IIS Web Server App Pool to run the webservice under Service account. Review IIS Webserver, ASP .NET projects configuration files to gather Application Pool (e.g. find out any Service Account, RoleGroup Mapping) configurations like below:

<authorization>

<allow role="domain\R-APP-groupname-M" />

<allow user="\*" />

</authorization>

* Identity all service/technical accounts are used to authenticate against Legacy AD

**Migration strategy**

Where legacy AD domain values are used in application Web server they will need to be replaced with the new domain information. To achieve this, the application's technical team needs to:

* Consult AD Application Remediation team before making changes in terms of re-hosting your server connecting to new AD Domain
* Consult AD Application Remediation team and share your timeline and migration plan
* Change hardcoded AD detail (host and port) or hardcoded IP address to match what is used in the application web server
* Change all service/technical accounts currently configured to authenticate against the Legacy AD to authenticate to the new AD
* Perform the necessary testing and BCP testing

#### <<$On-Premise>>

**Considerations**

As part of Active Directory One Domain Consolidation, all current AD Domains and Forests will be migrated to a Single Forest and one AD domain. Currently there are 135 domain controllers and 3 AD Domains within scope of this project.

Phase 2 of the One Domain project will not begin until after the Assessment has been completed. No AD migrations will occur during the Assessment phase. To help with the planning and creating a Migration plan for your application, reference the below considerations:

* Your Application technical teams are aware of the programme for AD One Domain Consolidation
* If your web server is on non-windows operating system then continue with the existing operating system and server
* Please check if on-premise server is connected to any of AD Domain which require migration to the new AD domain once it is available

Identify all places in your on-premise deployment where Service Accounts, Hardcoded AD details (host and port) or hardcoded IP addresses are used

**Migration strategy**

Where legacy AD domain values are used in application on-premise servers, they will need to be replaced with the new domain information. To achieve this, the application's technical team needs to:

* Consult AD Application Remediation team before making changes in terms of re-hosting your server connecting to new AD Domain
* Consult AD Application Remediation team and share your timeline, migration plan
* Change hardcoded AD detail (host and port) or hardcoded IP address is used in the application web server
* Change all service/technical accounts are used to authenticate against Legacy AD and connect to new AD
* Perform the necessary testing and BCP testing

#### <<$Cloud>>

**Considerations**

As part of Active Directory One Domain Consolidation, all current AD Domains and Forests will be migrated to a Single Forest and one AD domain. Currently there are 135 domain controllers and 3 AD Domains within scope of this project.

Phase 2 of the One Domain project will not begin until after the Assessment has been completed. No AD migrations will occur during the Assessment phase. To help with the planning and creating a Migration plan for your application, reference the below considerations:

* Your Application technical teams are aware of the programme for AD One Domain Consolidation
* Please identify if your Cloud Application is accessed by on-premise Federated Authentication such as Active Directory Federation Service (ADFS)
* Please identify if your cloud hosted server, cloud application uses any on-premise Legacy AD domain objects such as Service Accounts, AD Groups and other objects from AD container

**Migration strategy**

Where legacy AD domain values are used in your Cloud application they will need to be replaced with the new domain information. To achieve this, the application's technical team needs to;

* Consult AD, Application Remediation team before making changes in terms of re-hosting your server connecting to new AD Domain
* Consult AD, Application Remediation team and share your timeline, migration plan
* If on-premise federated authentication is used, plan for changing Authentication, Authorization parameters
* Plan for changing Cloud Application hosted server connecting new AD domain
* Perform the necessary testing and BCP testing

#### <<$Mainframe>>

**Considerations**

As part of Active Directory One Domain Consolidation, all current AD Domains and Forests will be migrated to a Single Forest and one AD domain. Currently there are 135 domain controllers and 3 AD Domains within scope of this project.

Phase 2 of the One Domain project will not begin until after the Assessment has been completed. No AD migrations will occur during the Assessment phase. To help with the planning and creating a Migration plan for your application, reference the below considerations:

* Your Application technical teams are aware of the programme for AD One Domain Consolidation
* Please check Mainframe Application Authentication process such as does the Application uses local mainframe authentication Or Application connects to Legacy AD domain for Authentication/Authorization
* Please check if AD accounts, AD groups are provisioned to Mainframe Application by Identity Management Tool
* Identify places in Mainframe Application where AD objects if used

**Migration strategy**

Where legacy AD domain values are used in your Mainframe application they will need to be replaced with the new domain information. To achieve this, the application's technical team needs to;

* Consult AD Application Remediation team before making changes in terms of re-hosting your server connecting to new AD Domain
* Consult AD Application Remediation team and share your timeline, migration plan
* If Mainframe Application uses Legacy AD authentication/authorization, plan to change configurations connecting to new AD domain
* Consult Identity Management team if changes are made for User Provisioning of the new AD accounts and/or groups from the new AD
* Perform the necessary testing and BCP testing.

#### <<$Standalone (Devices)>>

**Considerations**

As part of Active Directory One Domain Consolidation, all current AD Domains and Forests will be migrated to a Single Forest and one AD domain. Currently there are 135 domain controllers and 3 AD Domains within scope of this project.

Phase 2 of the One Domain project will not begin until after the Assessment has been completed. No AD migrations will occur during the Assessment phase. To help with the planning and creating a Migration plan for your application, reference the below considerations:

* Your Application technical teams are aware of the programme for AD One Domain Consolidation
* Please check your Application Authentication process such as does the Application uses local device authentication Or Application connects to Legacy AD domain for Authentication/Authorization
* Identify all places where hardcoded AD detail (host and port) or hardcoded IP address is used in the application e.g. any webservice, API call

**Migration strategy**

Where legacy AD domain values are used in application Web server they will need to be replaced with the new domain information. To achieve this, the application's technical team needs to:

* Consult AD Application Remediation team before making changes in terms of re-hosting your server connecting to new AD Domain
* Consult AD Application Remediation team and share your timeline and migration plan
* If the application uses Legacy AD authentication/authorization, plan to change Configurations connecting the new AD domain
* Change hardcoded AD detail (host and port) or hardcoded IP address to detail or IP address used in the application web service’s API call
* Perform the necessary testing and BCP testing.

#### <<$Other>>

**Considerations**

As part of Active Directory One Domain Consolidation, all current AD Domains and Forests will be migrated to a Single Forest and one AD domain. Currently there are 135 domain controllers and 3 AD Domains within scope of this project.

Phase 2 of the One Domain project will not begin until after the Assessment has been completed. No AD migrations will occur during the Assessment phase. To help with the planning and creating a Migration plan for your application, reference the below considerations:

* Your Application technical teams are aware of the programme for AD One Domain Consolidation
* Please check your Application Authentication process such as does the Application uses local device authentication Or Application connects to Legacy AD domain for Authentication/Authorization
* Identify all places where hardcoded AD detail (host and port) or hardcoded IP address is used in the application
* Identify all places in your Application deployment where Service Accounts, Hardcode AD details (host and port) or hardcoded IP address is used

**Migration strategy**

Where legacy AD domain values are used in application they will need to be replaced with the new domain information. To achieve this, the application's technical team needs to;

* Consult AD Application Remediation team before making changes in terms of re-hosting your server connecting to new AD Domain
* Consult AD Application Remediation team and share your timeline and migration plan
* Change hardcoded AD detail (host and port) or hardcoded IP address is used in the application web server
* Change all service/technical accounts used to authenticate against Legacy AD to authenticate to the new AD
* Perform the necessary testing and BCP testing

## Application Server Domain

#### <<$Yes\_App\_Server\_Connected\_AD>>

Based on the Application Assessment details we collected from your Application Team Owner this application is configured to use multiple AD domains.

If an application is hosted/deployed on servers connected to any of the following active directory Domains, DMN1, FMRCO and DSDOM1, please validate the domain names are correct.

**Considerations**

As part of Active Directory One Domain Consolidation, all current AD Domains and Forests will be migrated to a Single Forest and one AD domain. Currently there are 135 domain controllers and 3 AD Domains within scope of this project.

Phase 2 of the One Domain project will not begin until after the Assessment has been completed. No AD migrations will occur during the Assessment phase. To help with the planning and creating a Migration plan for your application, reference the below considerations:

* Your Application technical teams are aware of the programme for AD One Domain Consolidation
* Identify all Application Hosted Server Lists, FQDN, IP Address
* Validate Application Server DNS Host Name (e.g. <abcd.im.fmrco.com>) uses the correct Distinguished Name. For example:
  + < CN=abcd,OU=Domain Controllers,DC=im,DC=fmrco,DC=com>
  + <CN=xyz,OU=Servers,OU=FMRCO,OU=US,DC=im,DC=fmrco,DC=com>
  + <CN=mno, OU=Workstations,OU=FIMT,OU=FMRCO,OU=US,DC=im,DC=fmrco,DC=com>
  + < CN=def,OU=Computers,OU=Unix,DC=im,DC=fmrco,DC=com>
* Plan for changing your Application Hosted Server DNSHostName to reference the new AD domain after new AD domain is available

**Migration strategy**

Where legacy AD domain values are used in application hosted servers they will need to be replaced with the new domain information. To achieve this, the application's technical team needs to:

* Consult AD Application Remediation team before making changes in terms of re-hosting your server connecting to new AD Domain
* Consult AD Application Remediation team and share your timeline, migration plan
* Change Application Server connectivity details for new AD cross domain trust (e.g. One way trust, cross domain trust) till the time your Application Server is migrated to new domain (e.g. your new server DNSHostName will change to “cn=abcd,OU=xyz, DC=RootDomain,DC=com”)

#### <<$No\_App\_Server\_Connected\_AD>>

If the Application doesn’t host/deploy servers connected to any of these active directory Domains (DMN1, FMRCO and DSDOM1), no changes are required.

## Client Type

Based on Application Assessment, details we collected from your Application Team Owner, this application is of type <<$Client\_Type>> Application, please find the below Considerations and migration strategy.

#### <<$Thin Client>>

**Considerations**

As part of Active Directory One Domain Consolidation, all current AD Domains and Forests will be migrated to a Single Forest and one AD domain. Currently there are 135 domain controllers and 3 AD Domains within scope of this project.

Phase 2 of the One Domain project will not begin until after the Assessment has been completed. No AD migrations will occur during the Assessment phase. To help with the planning and creating a Migration plan for your application, reference the below considerations:

* Your Application technical teams are aware of the programme for AD One Domain Consolidation
* Identify all places where hardcoded AD detail (FQDN, host and port) or hardcoded IP address is used in the Application Client Configurations e.g. any webservice, API call
* Identify all service/technical accounts, AD Groups are used to authenticate against Legacy AD

**Migration strategy**

Where legacy AD domain values are used by a Thin Client application, they will need to be replaced with the new domain information. To achieve this, the application's technical team needs to:

* Consult AD Application Remediation team before making changes in your thin client application connecting to new AD Domain
* Consult AD Application Remediation team and share your timeline and migration plan
* If Application uses Legacy AD authentication/authorization, plan to change Configurations connecting to the new AD domain (e.g. change Service Account, AD Groups, AD container)
* Change hardcoded AD details (host and port) or hardcoded IP addresses used in the thin client application (e.g. web service or API call)
* Perform the necessary testing and BCP testing

#### <<$Thick Client>>

**Considerations**

As part of Active Directory One Domain Consolidation, all current AD Domains and Forests will be migrated to a Single Forest and one AD domain. Currently there are 135 domain controllers and 3 AD Domains within scope of this project.

Phase 2 of the One Domain project will not begin until after the Assessment has been completed. No AD migrations will occur during the Assessment phase. To help with the planning and creating a Migration plan for your application, reference the below considerations:

* Your Application technical teams are aware of the programme for AD One Domain Consolidation
* Identify all places where hardcoded AD detail (FQDN, host and port) or hardcoded IP address is used in the Application Client Configurations (e.g. any webservice or API call)
* Identify all service/technical accounts and AD Groups used to authenticate against Legacy AD

**Migration strategy**

Where legacy AD domain values are used in application Thick Client they will need to be replaced with the new domain information. To achieve this, the application's technical team needs to:

* Consult AD Application Remediation team before making changes in your thick client application connecting to new AD Domain
* Consult AD Application Remediation team and share your timeline and migration plan
* If Application uses Legacy AD authentication/authorization, plan to change Configurations connecting new AD domain (e.g. change Service Account, AD Groups, AD container)
* Change hardcoded AD detail (host and port) or hardcoded IP address used in the thin client application (e.g. web service or API call)
* Perform the necessary testing and BCP testing

#### <<$Thin and Thick Client>>

**Considerations**

As part of Active Directory One Domain Consolidation, all current AD Domains and Forests will be migrated to a Single Forest and one AD domain. Currently there are 135 domain controllers and 3 AD Domains within scope of this project.

Phase 2 of the One Domain project will not begin until after the Assessment has been completed. No AD migrations will occur during the Assessment phase. To help with the planning and creating a Migration plan for your application, reference the below considerations:

* Your Application technical teams are aware of the programme for AD One Domain Consolidation
* Identify all places where hardcoded AD detail (FQDN, host and port) or hardcoded IP address is used in the Application Client Configurations (e.g. any webservice or API call)
* Identify all service/technical accounts and AD Groups used to authenticate against Legacy AD

**Migration strategy**

Where legacy AD domain values are used in application thin/thick client they will need to be replaced with the new domain information. To achieve this, the application's technical team needs to:

* Consult AD Application Remediation team before making changes in your Application Thin, Thick Client connecting to new AD Domain
* Consult AD, Application Remediation team and share your timeline, migration plan
* If Application uses Legacy AD authentication/authorization, change the Configurations to connect to the new AD domain (e.g. change Service Account, AD Groups, AD container)
* Change hardcoded AD detail (host and port) or hardcoded IP address used in the thin/thick client application (e.g. web service or API call)
* Perform the necessary testing and BCP testing.

#### <<$Citrix (HVD)>>

**Considerations**

As part of Active Directory One Domain Consolidation, all current AD Domains and Forests will be migrated to a Single Forest and one AD domain. Currently there are 135 domain controllers and 3 AD Domains within scope of this project.

Phase 2 of the One Domain project will not begin until after the Assessment has been completed. No AD migrations will occur during the Assessment phase. To help with the planning and creating a Migration plan for your application, reference the below considerations:

* Your Application technical teams are aware of the programme for AD One Domain Consolidation
* Identify current Citrix Authentication process against Legacy AD Domain (e.g. does Citrix uses federated authentication using ADFS (Active Directory Federation Service))
* Identify all places where hardcoded AD details (FQDN, host and port) or hardcoded IP addresses are used in the Citrix Application Configurations
* Please validate if Citrix Application Hosted Server is AD Domain Joined
* Please validate if Citrix Application provide desktop single sign on using Kerberos
* Identify all service/technical accounts and AD Groups used to authenticate against Legacy AD

**Migration strategy**

Where legacy AD domain values are used in Citrix application they will need to be replaced with the new domain information. To achieve this, the application's technical team needs to:

* Consult AD Application Remediation team before making changes in your Citrix Application connecting to the new AD Domain
* Consult AD Application Remediation team and share your timeline and migration plan
* Migrate Citrix Application Hosted Server to connect to the new AD Domain
* Change all service/technical accounts used to authenticate against Legacy AD to authenticate to the new AD
* Change configurations related to desktop single sign on using Kerberos
* Change other AD details (FQDN, host and port) or hardcoded IP addresses to connect to the new AD Domain
* Perform the necessary testing and BCP testing

#### <<$Web Browser/Service>>

**Considerations**

As part of Active Directory One Domain Consolidation, all current AD Domains and Forests will be migrated to a Single Forest and one AD domain. Currently there are 135 domain controllers and 3 AD Domains within scope of this project.

Phase 2 of the One Domain project will not begin until after the Assessment has been completed. No AD migrations will occur during the Assessment phase. To help with the planning and creating a Migration plan for your application, reference the below considerations:

* Your Application technical teams are aware of the programme for AD One Domain Consolidation
* Identify all service/technical accounts and AD Groups used to authenticate against Legacy AD
* Identify all places where hardcoded AD details (FQDN, host and port) or hardcoded IP addresess are used
* Identify if Application requires Integrated Windows Authentication (IWA) to be enabled in Browser connecting to Legacy AD Domain

**Migration strategy**

Where legacy AD domain values are used in application Service they will need to be replaced with the new domain information. To achieve this, the application's technical team needs to:

* Consult AD Application Remediation team before making changes in your Application connecting to new AD Domain
* Consult AD Application Remediation team and share your timeline and migration plan
* Change Integrated Windows Authentication (IWA) configurations to connect to the new AD domain
* Change other AD details (FQDN, host and port) or hardcoded IP addresses to connect to the new AD Domain for the services which used Legacy AD domain
* Perform the necessary testing and BCP testing

## Application Distribution List Mailbox

This application uses Distribution List Mailbox **<<$DL\_MAILBOX>>** for communication, below are some considerations and migration strategies.

#### <<$Distribution List>>

This Application uses Distribution List, below are some considerations and migration strategies.

**Considerations**

As part of Active Directory One Domain Consolidation, all current AD Domains and Forests will be migrated to a Single Forest and one AD domain. Currently there are 135 domain controllers and 3 AD Domains within scope of this project.

Phase 2 of the One Domain project will not begin until after the Assessment has been completed. No AD migrations will occur during the Assessment phase. To help with the planning and creating a Migration plan for your application, reference the below considerations:

* Your Application technical teams are aware of the programme for AD One Domain Consolidation
* Please Identity names of DL's your Application uses, DL's requested, and members of your DL's
* Identify distribution groups used by Application from Legacy AD
* Identify names along with full SMTP address of DL or mail group used by application

**Migration strategy**

Where DL’s from legacy AD domain environment might be used they will need to be replaced from new AD domain. To achieve this, the application's technical team needs to

* Consult AD Application Remediation team before making changes
* Make changes to DL Groups used by Application and repoint to using DL Groups from new AD
* Make changes to SMTP address of DL or mail group used by application
* Perform necessary testing and BCP testing

#### <<$Shared Mailbox>>

This Application uses Shared Mailbox, below are some considerations and migration strategies.

**Considerations**

As part of Active Directory One Domain Consolidation, all current AD Domains and Forests will be migrated to a Single Forest and one AD domain. Currently there are 135 domain controllers and 3 AD Domains within scope of this project.

Phase 2 of the One Domain project will not begin until after the Assessment has been completed. No AD migrations will occur during the Assessment phase. To help with the planning and creating a Migration plan for your application, reference the below considerations:

* Your Application technical teams are aware of the programme for AD One Domain Consolidation
* Identify DS-groups used for sending e-mail communications (mail enabled) and for granting access to shared mailboxes (MB-)
* Identify names along with full SMTP addresses of shared mailbox used by application
* Identify how the access to these shared mailboxes is requested by a user (ex. SNOW or by mai,l etc.)

**Migration strategy**

Where Shared Mailboxes from legacy AD domain environment is used they will need to be replaced from new AD domain. To achieve this, the application's technical team needs to

* Consult AD Application Remediation team before making changes
* Ensure shared mailboxes are migrated to the new AD domain
* Update Application Configurations to use the new Shared Mailboxes
* Perform the necessary testing and BCP testing

#### <<$Distribution List and Shared Mailbox>>

This Application uses both Distribution List and Shared Mailbox, below are some considerations and migration strategies.

**Considerations**

As part of Active Directory One Domain Consolidation, all current AD Domains and Forests will be migrated to a Single Forest and one AD domain. Currently there are 135 domain controllers and 3 AD Domains within scope of this project.

Phase 2 of the One Domain project will not begin until after the Assessment has been completed. No AD migrations will occur during the Assessment phase. To help with the planning and creating a Migration plan for your application, reference the below considerations:

* Identify names along with full SMTP address of DLs or mail groups used by the application.
* Identify names along with full SMTP addresses of shared mailboxes used by application.
* Identify how access to these shared mailboxes is requested by a user (ex. SNOW or by mail etc.).

**Migration strategy**

Where DL’s from legacy AD domain environment might be used they will need to be migrated to the new AD domain. To achieve this, the application's technical team needs to

* Consult AD Application Remediation team before making changes
* Make changes to DL Groups used by the Application and connect to the new AD domain
* Update the SMTP address of DL or mail group used by application
* Ensure the shared mailboxes are migrated to the new AD domain
* Update Application Configurations to use the new Shared Mailboxes
* Perform the necessary testing and BCP testing.

#### <<$None\_DL\_MAILBOX>>

Application doesn’t using any DL or Share mailbox, no changes are required.

## Application Share Point

This application uses Shared Point for Documents Library, content management, below are some considerations and migration strategies.

**Considerations**

As part of Active Directory One Domain Consolidation, all current AD Domains and Forests will be migrated to a Single Forest and one AD domain. Currently there are 135 domain controllers and 3 AD Domains within scope of this project.

Phase 2 of the One Domain project will not begin until after the Assessment has been completed. No AD migrations will occur during the Assessment phase. To help with the planning and creating a Migration plan for your application, reference the below considerations:

* Your Application technical teams are aware of the programme for AD One Domain Consolidation
* Identify how SharePoint access is provided to users of your Application and do all users of your Application get access to SharePoint
* What are the different types of users and how is the access classification done for them
* Identify all legacy AD Domain Groups used for SharePoint access

**Migration strategy**

SharePoint references to the legacy AD domain environment will need to be updated to reference the new AD domain. To achieve this, the application's technical team needs to

* Consult AD Application Remediation team before making changes
* Consult AD team for SharePoint migration plan to the new AD domain
* Update your Application configurations to use the new SharePoint URL and Access
* Update Application specific SharePoint AD Groups and members of the SharePoint AD Group to reference the new AD Domain groups
* Perform necessary testing and BCP testing.

**If the Application doesn’t use any SharePoint or Document library, no changes are required.**

# Migration Wave/s

This application come under **<<$WAVE\_NUMBER>>** for application migration.

* The application **<<$APP\_NAME>>** is considered part of **<<$WAVE\_NUMBER>>** for the migration and planned to migrate into new domain by <**<$DATE>>** tentatively.