****

2018-2019

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

[1 Introduction 3](#_Toc527722072)

[2 Objective 3](#_Toc527722073)

[3 Definition & Acronyms 3](#_Toc527722074)

[3.1 Recommended Best Practices 3](#_Toc527722075)

[4 Application components and their Migration strategy 3](#_Toc527722076)

[4.1 Application Name 3](#_Toc527722077)

[4.2 Application Authentication Type 3](#_Toc527722078)

[4.2.1 <<$Service\_Accounts>> 4](#_Toc527722079)

[4.2.2 <<$Virtual\_Directory\_Service (VDS+)>> 4](#_Toc527722080)

[4.2.3 <<$CA\_SiteMinder>> 5](#_Toc527722081)

[4.2.4 <<$Enterprise\_Sec>> 5](#_Toc527722082)

[4.2.5 <<$Gateway (ESG)>> 6](#_Toc527722083)

[4.2.6 <<$Ping\_SSO>> 6](#_Toc527722084)

[4.2.7 <<$Centrify>> 7](#_Toc527722085)

[4.2.8 <<$ADFS>> 7](#_Toc527722086)

[4.2.9 <<$Essso>> 8](#_Toc527722087)

[4.2.10 <<$Other>> 8](#_Toc527722088)

[4.2.11 <<$Does not use AD for any authentication>> 9](#_Toc527722089)

[4.3 Authentication Mechanism 9](#_Toc527722090)

[4.3.1 <<$Kerberos>> 9](#_Toc527722091)

[4.3.2 <<$NTLM>> 9](#_Toc527722092)

[4.3.3 <<$Oauth>> 10](#_Toc527722093)

[4.3.4 <<$OpenID>> 10](#_Toc527722094)

[4.3.5 <<$SAML>> 11](#_Toc527722095)

[4.3.6 <<$Other>> 11](#_Toc527722096)

[4.3.7 <<$None>> 12](#_Toc527722097)

[4.4 Application Cross Domain 12](#_Toc527722098)

[4.4.1 <<$Yes\_Access\_Across\_Other\_Domains>> 12](#_Toc527722099)

[4.4.2 <<$No\_Access\_Across\_Other\_Domains>> 13](#_Toc527722100)

[4.5 Application SSL Certificate 13](#_Toc527722101)

[4.5.1 <<$Yes\_SSL\_Certificate>> 13](#_Toc527722102)

[4.5.2 <<$No\_SSL\_Certificate>> 13](#_Toc527722103)

[4.6 Local Accounts Creation 14](#_Toc527722104)

[4.6.1 <<$Yes\_Local\_Accounts>> 14](#_Toc527722105)

[4.6.2 <<$No\_Local\_Accounts>> 14](#_Toc527722106)

[4.7 Application Forest Domain Name 14](#_Toc527722107)

[4.7.1 <<$DMN1>> 14](#_Toc527722108)

[4.7.2 <<$FMRCO>> 15](#_Toc527722109)

[4.7.3 <<$DSDOM1>> 15](#_Toc527722110)

[4.7.4 <<$INTL>> 15](#_Toc527722111)

[4.7.5 <<$Other>> 16](#_Toc527722112)

[4.8 Application Service Account 16](#_Toc527722113)

[4.8.1 <<$List out the name of service accounts>> 16](#_Toc527722114)

[4.8.2 <<$Not using any service accounts>> 16](#_Toc527722115)

[4.9 File and Registry Permissions 16](#_Toc527722116)

[4.9.1 <<$None>> 16](#_Toc527722117)

[4.9.2 <<$Dynamic File Structure>> 17](#_Toc527722118)

[4.9.3 <<$Registry Permission>> 17](#_Toc527722119)

[4.9.4 <<$NAS>> 17](#_Toc527722120)

[4.9.5 <<$SAN>> 18](#_Toc527722121)

[4.10 Application Access Method 18](#_Toc527722122)

[4.10.1 <<$Direct Application Access>> 18](#_Toc527722123)

[4.10.2 <<$Based on Group membership>> 19](#_Toc527722124)

[4.10.3 <<$Based on Rule/Policy>> 19](#_Toc527722125)

[4.10.4 <<$Other>> 19](#_Toc527722126)

[4.11 Application Dependency 20](#_Toc527722127)

[4.11.1 <<$Yes\_Application\_Dependency>> 20](#_Toc527722128)

[4.11.2 <<$No\_Application\_Dependency>> 20](#_Toc527722129)

[4.12 Application Host Model 20](#_Toc527722130)

[4.12.1 <<$Web-Based>> 20](#_Toc527722131)

[4.12.2 <<$On-Premise>> 21](#_Toc527722132)

[4.12.3 <<$Cloud>> 22](#_Toc527722133)

[4.12.4 <<$Mainframe>> 22](#_Toc527722134)

[4.12.5 <<$Standalone (Devices)>> 23](#_Toc527722135)

[4.12.6 <<$Other>> 23](#_Toc527722136)

[4.13 Application Server Domain 24](#_Toc527722137)

[4.13.1 <<$Yes\_App\_Server\_Connected\_AD>> 24](#_Toc527722138)

[4.13.2 <<$No\_App\_Server\_Connected\_AD>> 25](#_Toc527722139)

[4.14 Client Type 25](#_Toc527722140)

[4.14.1 <<$Thin Client>> 25](#_Toc527722141)

[4.14.2 <<$Thick Client>> 25](#_Toc527722142)

[4.14.3 <<$Thin and Thick Client>> 25](#_Toc527722143)

[4.14.4 <<$Citrix (HVD)>> 26](#_Toc527722144)

[4.14.5 <<$Web Browser/Service>> 26](#_Toc527722145)

[4.15 Application Distribution List Mailbox 26](#_Toc527722146)

[4.15.1 <<$Distribution List>> 26](#_Toc527722147)

[4.15.2 <<$Shared Mailbox>> 27](#_Toc527722148)

[4.15.3 <<$Distribution List and Shared Mailbox>> 27](#_Toc527722149)

[4.15.4 <<$None>> 27](#_Toc527722150)

[4.16 Application Share Point 28](#_Toc527722151)

[4.16.1 <<$Yes\_Data\_Repository\_Utilization>> 28](#_Toc527722152)

[4.16.2 <<$No\_Data\_Repository\_Utilization>> 28](#_Toc527722153)

[5 Migration Wave/s 28](#_Toc527722154)

[6 References 29](#_Toc527722155)

[6.1 Request for new server 29](#_Toc527722156)

[6.2 Request for new service/technical account 29](#_Toc527722157)

[6.3 Request for local share 29](#_Toc527722158)

[6.4 Request for shared mailbox 29](#_Toc527722159)

[6.5 Request for new DL 29](#_Toc527722160)

[6.6 Request for file/folder/registry permissions 29](#_Toc527722161)

[6.7 Support Information 29](#_Toc527722162)

# 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 IP address of AD domain is used and change it with FQDN of AD domain

# Application components and their Migration strategy

## Application Name

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

## Application Authentication Type

This application uses **<<$Authetication\_Type>>** as Authentication Type. Please find the below Considerations and Migration strategy.

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

**Considerations**

* If the application is hosted in same server then no changes are required with respect to server else If a new server has been provisioned for this application, on the target domain, please identify the server name and IP Address. If not please refer section "**Request for new server**".
* If service/technical accounts are used for authentication, then request for the same service/technical account on the new server. Please refer section " **Request for new service/technical account** " for details.
* Identify all places where hardcoded AD detail (host and port) or hardcoded IP address is used in your authentication server.
* If authentication components are installed on a non-windows operating system then continue with the existing operating system.

**Migration strategy**

* Register the new host in new AD domain and setup service account authentication.
* Perform the necessary testing and BCP testing.

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

**Considerations**

* If the application is hosted in same server then no changes are required with respect to server else If a new server has been provisioned for this application, on the target domain, please identify the server name and IP Address. If not please refer section "**Request for new server**".
* If service/technical accounts are used for authentication, then request for the same service/technical account on the new server. Please refer section " **Request for new service/technical account** " for details.
* Identify all places where hardcoded AD detail (host and port) or hardcoded IP address is used in your authentication server.
* If authentication components are installed on a non-windows operating system then continue with the existing operating system.

**Migration strategy**

* Register the new host in new AD domain and setup Virtual Directory Service authentication.
* Perform the necessary testing and BCP testing.

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

**Considerations**

* If the application is hosted in same server then no changes are required with respect to server else If a new server has been provisioned for this application, on the target domain, please identify the server name and IP Address. If not please refer section "**Request for new server**".
* If service/technical accounts are used for authentication, then request for the same service/technical account on the new server. Please refer section " **Request for new service/technical account** " for details.
* Identify all places where hardcoded AD detail (host and port) or hardcoded IP address is used in your authentication server.
* If authentication components are installed on a non-windows operating system then continue with the existing operating system.

**Migration strategy**

* Register the new host in new AD domain and setup Web SSO solution based on CA Site Minder authentication.
* Perform the necessary testing and BCP testing.

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

**Considerations**

* If the application is hosted in same server then no changes are required with respect to server else If a new server has been provisioned for this application, on the target domain, please identify the server name and IP Address. If not please refer section "**Request for new server**".
* If service/technical accounts are used for authentication, then request for the same service/technical account on the new server. Please refer section " **Request for new service/technical account** " for details.
* Identify all places where hardcoded AD detail (host and port) or hardcoded IP address is used in your authentication server.
* If authentication components are installed on a non-windows operating system then continue with the existing operating system.

**Migration strategy**

* Register the new host in new AD domain and setup Enterprise Sec authentication.
* Perform the necessary testing and BCP testing.

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

**Considerations**

* The application is hosted in same server then no changes are required with If respect to server else If a new server has been provisioned for this application, on the target domain, please identify the server name and IP Address. If not please refer section "**Request for new server**".
* If service/technical accounts are used for authentication, then request for the same service/technical account on the new server. Please refer section " **Request for new service/technical account** " for details.
* Identify all places where hardcoded AD detail (host and port) or hardcoded IP address is used in your authenatioticn server.
* If authentication components are installed on a non-windows operating system then continue with the existing operating system.

**Migration strategy**

* Register the new host in new AD domain and setup ESG authentication.
* Perform the necessary testing and BCP testing.

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

**Considerations**

* If the application is hosted in same server then no changes are required with respect to server else If a new server has been provisioned for this application, on the target domain, please identify the server name and IP Address. If not please refer section "**Request for new server**".
* If SPNs and associated service/technical accounts are used for authentication, then request for the same SPN and service/technical account on the new server. Please refer section " **Request for new service/technical account** " for details.
* Identify all places where hardcoded AD detail (host and port) or hardcoded IP address is used in your authentication server.
* If authentication components are installed on a non-windows operating system then continue with the existing operating system.

**Migration strategy**

* Register the new host in new AD domain and setup Web SSO solution based on Ping Federate SSO authentication.
* Perform the necessary testing and BCP testing.

#### <<$Centrify>>

**Considerations**

* If the application is hosted in same server then no changes are required with respect to server else If a new server has been provisioned for this application, on the target domain, please identify the server name and IP Address. If not please refer section "**Request for new server**".
* If service/technical accounts are used for authentication, then request for the same service/technical account on the new server. Please refer section " **Request for new service/technical account** " for details.
* Identify all places where hardcoded AD detail (host and port) or hardcoded IP address is used in your authentication server.
* If authentication components are installed on a non-windows operating system then continue with the existing operating system.

**Migration strategy**

* Register the new host in new AD domain and setup Centrify authentication.
* Perform the necessary testing and BCP testing.

#### <<$ADFS>>

**Considerations**

* If the application is hosted in same server then no changes are required with respect to server else If a new server has been provisioned for this application, on the target domain, please identify the server name and IP Address. If not please refer section "**Request for new server**".
* If service/technical accounts are used for authentication, then request for the same service/technical account on the new server. Please refer section " **Request for new service/technical account** " for details.
* Identify all places where hardcoded AD detail (host and port) or hardcoded IP address is used in your authentication server.
* If authentication components are installed on a non-windows operating system then continue with the existing operating system.

**Migration strategy**

* Register the new host in new AD domain and setup ADFS authentication.
* Perform the necessary testing and BCP testing.

#### <<$Essso>>

**Considerations**

* If the application is hosted in same server then no changes are required with respect to server else If a new server has been provisioned for this application, on the target domain, please identify the server name and IP Address. If not please refer section "**Request for new server**".
* If SPNs and associated service/technical accounts are used for authentication, then request for the same SPN and service/technical account on the new server. Please refer section " Request for new service/technical account " for details.
* Identify all places where hardcoded AD detail (host and port) or hardcoded IP address is used in your authentication server.
* If authentication components are installed on a non-windows operating system then continue with the existing operating system.

**Migration strategy**

* Register the new host in new AD domain and setup Web SSO solution based on Ping Federate SSO authentication.
* Perform the necessary testing and BCP testing.

#### <<$Other>>

**Considerations**

* Identify if application is accessed only by internal and external users. List if there are any exceptions.
* Identify how the access to this application is requested by a user. (on mail, external portal, partners, ARP, BBS, on mail etc.)

**Migration strategy**

**Scenario 1**

* If access to this application is affirmed from AD authentication through headers/tokens etc., make sure the resource is migrated to the new AD domain.
* Perform necessary testing and BCP testing.

**Scenario 2**

* Application doesn’t use AD based access for users, no change required

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

Application doesn’t use AD based authentication, no change required

## Authentication Mechanism

This application uses **<<$Authetication\_Mechanism>>**as Authentication protocol Mechanism, Please find the below Considerations and Migration Strategy for selected Authentication mechanism.

#### <<$Kerberos>>

**Considerations**

* If the application is hosted in same server then no changes are required with respect to server else If a new server has been provisioned for this application, on the target domain, please identify the server name and IP Address. If not please refer section "**Request for new server**".
* If SPNs and associated service/technical accounts are used for Kerberos authentication, then request for the same SPN and service/technical account on the new server. Please refer section " **Request for new service/technical account** " for details.
* Identify all places where hardcoded AD detail (host and port) or hardcoded IP address is used in your authentication server.
* If Kerberos is installed on a non-windows operating system then continue with the existing operating system.

**Migration strategy**

* Register the new host in new AD domain and setup Kerberos authentication.
* Perform the necessary testing and BCP testing.

#### <<$NTLM>>

**Considerations**

* If the application is hosted in same server then no changes are required with respect to server else If a new server has been provisioned for this application, on the target domain, please identify the server name and IP Address. If not please refer section "**Request for new server**".
* If Service/technical accounts are used for authentication, then request for the same SPN and service/technical account on the new server. Please refer section " **Request for new service/technical account** " for details.
* Identify all places where hardcoded AD detail (host and port) or hardcoded IP address is used in your authentication server.
* If authentication components are installed on a non-windows operating system then continue with the existing operating system.

**Migration strategy**

* Register the new host in new AD domain and setup Desktop SSO-NTLM authentication.
* Perform the necessary testing and BCP testing.

#### <<$Oauth>>

**Considerations**

* If the application is hosted in same server then no changes are required with respect to server else If a new server has been provisioned for this application, on the target domain, please identify the server name and IP Address. If not please refer section "**Request for new server**".
* If SPNs and associated service/technical accounts are used for Kerberos authentication, then request for the same SPN and service/technical account on the new server. Please refer section " **Request for new service/technical account** " for details.
* Identify all places where hardcoded AD detail (host and port) or hardcoded IP address is used in your authentication server.
* If Kerberos is installed on a non-windows operating system then continue with the existing operating system.

**Migration strategy**

* Register the new host in new AD domain and setup Oauth authentication.
* Perform the necessary testing and BCP testing.

#### <<$OpenID>>

**Considerations**

* If the application is hosted in same server then no changes are required with respect to server else If a new server has been provisioned for this application, on the target domain, please identify the server name and IP Address. If not please refer section "**Request for new server**".
* If SPNs and associated service/technical accounts are used for Kerberos authentication, then request for the same SPN and service/technical account on the new server. Please refer section " **Request for new service/technical account** " for details.
* Identify all places where hardcoded AD detail (host and port) or hardcoded IP address is used in your authentication server.
* If Kerberos is installed on a non-windows operating system then continue with the existing operating system.

**Migration strategy**

* Register the new host in new AD domain and setup OpenID authentication.
* Perform the necessary testing and BCP testing.

#### <<$SAML>>

**Considerations**

* If the application is hosted in same server then no changes are required with respect to server else If a new server has been provisioned for this application, on the target domain, please identify the server name and IP Address. If not please refer section " **REF \_Ref462752514 \h \\* MERGEFORMAT Request for new server**".
* If SPNs and associated service/technical accounts are used for Kerberos authentication, then request for the same SPN and service/technical account on the new server. Please refer section " **Request for new service/technical account** " for details.
* Identify all places where hardcoded AD detail (host and port) or hardcoded IP address is used in your authentication server.
* If Kerberos is installed on a non-windows operating system then continue with the existing operating system.

**Migration strategy**

* Register the new host in new AD domain and setup SAML authentication.
* Perform the necessary testing and BCP testing.

#### <<$Other>>

**Considerations**

* If the application is hosted in same server then no changes are required with respect to server else If a new server has been provisioned for this application, on the target domain, please identify the server name and IP Address. If not please refer section " **REF \_Ref462752514 \h \\* MERGEFORMAT Request for new server**".
* If SPNs and associated service/technical accounts are used for Kerberos authentication, then request for the same SPN and service/technical account on the new server. Please refer section " **Request for new service/technical account** " for details.
* Identify all places where hardcoded AD detail (host and port) or hardcoded IP address is used in your authentication server.
* If Kerberos is installed on a non-windows operating system then continue with the existing operating system.

**Migration strategy**

* Based on other type of Authentication , will perform necessary changes and do the testing

#### <<$None>>

**Considerations**

* Identify if application is used any other Authentication mechanism. List if there are any exceptions.
* Identify how the access to this application is requested by a user. (on mail, external portal, partners etc.)

**Migration strategy**

**Scenario 1**

* If access to this application is affirmed from AD authentication through headers/tokens etc., make sure the resource is migrated to the new AD domain.
* Perform necessary testing and BCP testing.

**Scenario 2**

* Application doesn’t use authentication mechanism , no change required

## Application Cross Domain

#### <<$Yes\_Access\_Across\_Other\_Domains>>

This application integrated with cross Domains, Please find the below Considerations and Migration Strategy.

**Considerations**

* Is there are authentication dependency on a local login script being executed at client level?
* Identify all places where host details (FQDN, DN, host, port etc.) are used in your client configuration

**Migration strategy**

* Update the client configuration with AD details of new domain and/or server.
* Perform the necessary testing and BCP testing.

#### <<$No\_Access\_Across\_Other\_Domains>>

This application does not integrate with cross Domains so no changes are required.

## Application SSL Certificate

#### <<$Yes\_SSL\_Certificate>>

This Application is connected to AD by certificate based system to system authentication, Please find the below Considerations and migration Strategy.

**Considerations**

* If the application is hosted in same server then no changes are required with respect to server else If a new server has been provisioned for this application, on the target domain, please identify the server name and IP Address. If not please refer section " **REF \_Ref462752514 \h \\* MERGEFORMAT Request for new server**".
* Identify all places where hardcoded AD detail (host and port) or hardcoded IP address is used in the application server.
* If authentication components are installed on a non-windows operating system then continue with the existing operating system.

**Migration strategy**

* Application or any of its component use certificate (e.g SSL) for system to system authentication with respect to AD, make sure right certificates are imported and trust store is updated with new AD domain details.
* Perform necessary testing and BCP testing.

#### <<$No\_SSL\_Certificate>>

Application doesn’t connect to AD by certificate based system to system authentication, no change required.

## Local Accounts Creation

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

This application use create any local account, Please find the below Considerations and migration Strategy.

**Considerations**

* Identify if application is accessed only by internal users. List if there are any exceptions.
* • Identify how the access to this application is requested by a user. (e.g ARP, BBS, MAC, on mail etc.)

**Migration strategy**

* If access to this application is gained from AD authentication, make sure the resource is migrated to the new AD domain.
* Perform necessary testing and BCP testing.

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

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

## Application Forest Domain Name

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

#### <<$DMN1>>

**Considerations**

* Identify all places where hardcoded AD detail (host and port) or hardcoded IP address or any other configurations related to AD is used in the application.

**Migration strategy**

* Update all configurations where AD details are used with new AD details.
* If application uses a dedicated DB/storage/repository to store full or partial data. Make sure these repositories are pointing to the new AD domain.
* Arrange for testing and BCP testing.

#### <<$FMRCO>>

**Considerations**

* Identify all places where hardcoded AD detail (host and port) or hardcoded IP address or any other configurations related to AD is used in the application.

**Migration strategy**

* Update all configurations where AD details are used with new AD details.
* If application uses a dedicated DB/storage/repository to store full or partial data. Make sure these repositories are pointing to the new AD domain.
* Arrange for testing and BCP testing.

#### <<$DSDOM1>>

**Considerations**

* Identify all places where hardcoded AD detail (host and port) or hardcoded IP address or any other configurations related to AD is used in the application.

**Migration strategy**

* Update all configurations where AD details are used with new AD details.
* If application uses a dedicated DB/storage/repository to store full or partial data. Make sure these repositories are pointing to the new AD domain.
* Arrange for testing and BCP testing.

#### <<$INTL>>

**Considerations**

* Identify all places where hardcoded AD detail (host and port) or hardcoded IP address or any other configurations related to AD is used in the application.

**Migration strategy**

* Update all configurations where AD details are used with new AD details.
* If application uses a dedicated DB/storage/repository to store full or partial data. Make sure these repositories are pointing to the new AD domain.
* Arrange for testing and BCP testing.

#### <<$Other>>

**Considerations**

* Identify all places where hardcoded AD detail (host and port) or hardcoded IP address or any other configurations related to AD is used in the application.

**Migration strategy**

* Update all configurations where AD details are used with new AD details.
* If application uses a dedicated DB/storage/repository to store full or partial data. Make sure these repositories are pointing to the new AD domain.
* Arrange for testing and BCP testing.

## Application Service Account

#### <<$List out the name of service accounts>>

This Application uses Service account for authentication, Please find the below Considerations and Migration Strategy.

**Considerations**

* If service/technical accounts are used for authentication, then request for the same service/technical account on the new server. Please refer section " **Request for new service/technical account** " for details.
* Identify all places where hardcoded AD detail (host and port) or hardcoded IP address is used in your authentication server.
* If authentication components are installed on a non-windows operating system then continue with the existing operating system.

**Migration strategy**

* Setup service account for authentication in new AD domain.
* Perform the necessary testing and BCP testing.

#### <<$Not using any service accounts>>

Application doesn’t using any services accounts, no change required.

## File and Registry Permissions

#### <<$None>>

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

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

This Application uses Dynamic files Structure, Please find the below Considerations and migration Strategy.

**Considerations**

* Identify full name and path of the file which application uses.
* Identify the account used to access the DFS.
* If system or domain hosting the file on file server has changed as part of AD migration, identify the new path of the file.

**Migration strategy**

* Request access to DFS in the target domain.
* Make the necessary change in the application to use the file on new server and/ or domain.
* Arrange for testing and BCP testing.

#### <<$Registry Permission>>

This Application uses Registry Permission, Please find the below Considerations and migration Strategy.

**Considerations**

* Identify all file/folder/registry permissions and GPOs required for the application.

**Migration strategy**

* Request for file/folder/registry permissions and GPOs on the target AD domain. Refer section "Request for file/folder/registry permissions" for details.
* Make the necessary change in the application configuration to make sure the application works properly with new AD domain.
* Arrange for testing and BCP testing.

#### <<$NAS>>

This Application uses NAS, Please find the below Considerations and migration Strategy.

**Considerations**

* 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**

* 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, Please find the below Considerations and migration Strategy.

**Considerations**

* Identify names along with FQDN (Fully qualified domain name) of Network storage server or SAN used by application.
* Identify how Network storage is associated with application

**Migration strategy**

* 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

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

This application is accessible directly by users, Please find the below Considerations and Migration Strategy.

**Considerations**

* Identify if application is accessed directly by users. List if there are any exceptions.
* Identify how the access to this application is requested by a user. (e.g.SNOW, on mail etc.)

**Migration strategy**

* If access to this application is gained from AD authentication, make sure the resource is migrated to the new AD domain.
* Perform necessary testing and BCP testing.

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

This application is accessible based on group membership, Please find the below Considerations and Migration Strategy.

**Considerations**

* Identify all permission groups used by the application.
* Identify the account used for permission group.
* Identify how access to these permissions is requested.

**Migration strategy**

* Request access to permission groups on new domain
* Perform necessary testing and BCP testing.

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

This application is accessible based on Rule/Policy, Please find the below Considerations and Migration Strategy.

**Considerations**

* Identify the Rules/Policy which are used in segregation of functionality and access to application by any means (e.g. registry based policy, folder redirection etc.)

**Migration strategy**

* Request for Rule/Policy configuration on new AD domain for the application.
* Arrange for testing and BCP testing.

#### <<$Other>>

This application is accessible based on other method, Please find the below Considerations and Migration Strategy.

**Considerations**

* Identify the other way which are used in segregation of functionality and access to application by any means.

**Migration strategy**

* Request for configuration on new AD domain for the application.
* Arrange for testing and BCP testing.

## Application Dependency

#### <<$Yes\_Application\_Dependency>>

This application is having dependency with other application, Please find the below Considerations and migration strategy.

**Considerations**

* Is there are authentication dependency on a local login script being executed at client level?
* Identify all places where host details (FQDN, DN, host, port etc.) are used in the client configuration

**Migration strategy**

* Update the client configuration with AD details of new domain and/or server.
* Perform the necessary testing and BCP testing

#### <<$No\_Application\_Dependency>>

* Application doesn’t have any Dependency , no change are required

## Application Host Model

This application is hosted on <<$Host\_Model>>, please find the below Considerations and migration strategy.

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

**Considerations**

* If the application is hosted in same server then no changes are required with respect to server else If a new server has been provisioned for this application, on the target domain, please identify the server name and IP Address. If not please refer section "**Request for new server**".
* If service/technical accounts are used to authenticate against AD then request for the same service/technical account on the new server. Please refer section "**Request for new service/technical account**" for details.
* Identify all places where hardcoded AD detail (host and port) or hardcoded IP address is used in the application server.
* If your web server is on non-windows operating system then continue with the existing operating system.

**Migration strategy**

**Scenario 1**

* If web server is authenticating against AD then make sure it points to the new AD domain details.
* Perform the necessary testing and BCP testing.

**Scenario 2**

* If application server authenticate locally or not against AD then no configuration change is required

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

**Considerations**

* If the application is hosted in same server then no changes are required with respect to server else If a new server has been provisioned for this application, on the target domain, please identify the server name and IP Address. If not please refer section "**Request for new server**".
* If service/technical accounts are used to authenticate against AD then request for the same service/technical account on the new server. Please refer section "**Request for new service/technical account**" for details.
* Identify all places where hardcoded AD detail (host and port) or hardcoded IP address is used in the application server.
* If the application server is on non-windows operating system then continue with the existing operating system.

**Migration strategy**

**Scenario 1**

* If application server is authenticating against AD then make sure it points to the new AD details.
* Perform the necessary testing and BCP testing.

**Scenario 2**

* If application server authenticate locally or not against AD then no configuration change is required.

#### <<$Cloud>>

**Considerations**

* If service/technical accounts are used to authenticate against AD then request for the same service/technical account on the new server. Please refer section "**Request for new service/technical account**" for details.
* Identify all places where hardcoded AD detail (host and port) or hardcoded IP address is used in the application server.
* If the application server is on non-windows operating system then continue with the existing operating system.

**Migration strategy**

**Scenario 1**

* If application server is authenticating against AD then make sure it points to the new AD details.
* Perform the necessary testing and BCP testing.

**Scenario 2**

* If application server authenticate locally or not against AD then no configuration change is required.

#### <<$Mainframe>>

**Considerations**

* If service/technical accounts are used to authenticate against AD then request for the same service/technical account on the new server. Please refer section "**Request for new service/technical account**" for details.
* Identify all places where hardcoded AD detail (host and port) or hardcoded IP address is used in the application server.
* If the application server is on non-windows operating system then continue with the existing operating system.

**Migration strategy**

**Scenario 1**

* If application server is authenticating against AD then make sure it points to the new AD details.
* Perform the necessary testing and BCP testing.

**Scenario 2**

* If application server authenticate locally or not against AD then no configuration change is required.

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

**Considerations**

* If the application is hosted in same server then no changes are required with respect to server else If a new server has been provisioned for this application, on the target domain, please identify the server name and IP Address. If not please refer section "**Request for new server**".
* If service/technical accounts are used to authenticate against AD then request for the same service/technical account on the new server. Please refer section "**Request for new service/technical account**" for details.
* Identify all places where hardcoded AD detail (host and port) or hardcoded IP address is used in the application server.
* If the application server is on non-windows operating system then continue with the existing operating system.

**Migration strategy**

**Scenario 1**

* If application server is authenticating against AD then make sure it points to the new AD details.
* Perform the necessary testing and BCP testing.

**Scenario 2**

* If application server authenticate locally or not against AD then no configuration change is required.

#### <<$Other>>

**Considerations**

* If the application is hosted in same server then no changes are required with respect to server else If a new server has been provisioned for this application, on the target domain, please identify the server name and IP Address. If not please refer section "**Request for new server**".
* If service/technical accounts are used to authenticate against AD then request for the same service/technical account on the new server. Please refer section "**Request for new service/technical account**" for details.
* Identify all places where hardcoded AD detail (host and port) or hardcoded IP address is used in the application server.
* If the application server is on non-windows operating system then continue with the existing operating system.

**Migration strategy**

**Scenario 1**

* If application server is authenticating against AD then make sure it points to the new AD details.
* Perform the necessary testing and BCP testing.

**Scenario 2**

* If application server authenticate locally or not against AD then no configuration change is required.

## Application Server Domain

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

Application is hosted/deployed servers connected to any of these active directory Domains (DMN1, FMRCO and DSDOM1), please find the below Considerations and migration strategy.

**Considerations**

* If there is a data dependency to be migrated after application points to new AD domain, list down the name and type of DB/repositories.
* Identify all places where hardcoded AD detail (host and port) or hardcoded IP address is used in Database server.

**Migration strategy**

* If application uses a dedicated DB/storage/repository to store full or partial data. Make sure these repositories are pointing to the new AD domain.
* Perform necessary testing and BCP testing.

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

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

## Client Type

This application used **<<$Client\_Type>>** as Client type. Please find the below Considerations and migration strategy.

#### <<$Thin Client>>

**Considerations**

* Identify all places where host details (FQDN, DN, host, port etc.) are used in the client configuration.

**Migration strategy**

* Update the client configuration with host details of new domain and/or server.
* Perform the necessary testing and BCP testing.

#### <<$Thick Client>>

**Considerations**

* Identify all places where AD details (host, port, FQDN or DN) are used in your client configuration.

**Migration strategy**

* Update the client configuration with AD details of new domain and/or server.
* Perform the necessary testing and BCP testing.

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

**Considerations**

* Identify all places where host details (FQDN, DN, host, port etc.) are used in your client configuration.

**Migration strategy**

* Update the client configuration with host details of new domain and/or server.
* Perform the necessary testing and BCP testing.

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

**Considerations**

* Identify all places where host details (FQDN, DN, host, port etc.) are used in your client configuration.

**Migration strategy**

* Update the client configuration with host details of new domain and/or server.
* Perform the necessary testing and BCP testing.

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

**Considerations**

* Identify all places where host details (FQDN, DN, host, port etc.) are used in your client configuration.

**Migration strategy**

* No need to make any changes as browser will have necessary settings with the latest patch

## Application Distribution List Mailbox

This application uses <<$DL\_MAILBOX>> for communication, Please find the below Considerations and migration strategy.

#### <<$Distribution List>>

**Considerations**

* Identify names along with full SMTP address of DL or mail group used by application.

**Migration strategy**

* Configure the DL or mail group in the application wherever required.
* Perform the necessary testing and BCP testing.

**Note** – To request creation of new DL or mail group on a new AD domain, refer section **'Request for new DL**'

#### <<$Shared Mailbox>>

**Considerations**

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

**Migration strategy**

* Application uses shared mailbox for communication with users manually or triggered by an event. Make sure all the shared mailboxes are migrated to the new AD domain.
* Perform the necessary testing and BCP testing.

**Note** – To request creation of shared mailbox on new AD domain, Refer section '**Request for shared mailbox'**

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

**Considerations**

* Identify names along with full SMTP address of DL or mail group used by application.
* Identify names along with full SMTP address of shared mailbox used by application.
* Identify how the access to these shared mailboxes is requested by a user. (ex. ARP, BBS, MAC, on mail etc.)

**Migration strategy**

* Request for the DL or mail group on new domain.
* Configure the DL or mail group in the application wherever required.
* Perform the necessary testing and BCP testing.
* Application uses shared mailbox for communication with users manually or triggered by an event. Make sure all the shared mailboxes are migrated to the new AD domain.
* Perform the necessary testing and BCP testing.
* Note – To request creation of shared mailbox on new AD domain, Refer section 'Request for shared mailbox'

#### <<$None>>

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

## Application Share Point

#### <<$Yes\_Data\_Repository\_Utilization>>

This application uses share point to store application data, Please find the below Considerations and migration strategy.

**Considerations**

* If the application is hosted in same server then no changes are required with respect to server else If a new server has been provisioned for this application, on the target domain, please identify the server name and IP Address. If not please refer section "**Request for new server**".
* Identify all places where hardcoded AD detail (host and port) or hardcoded IP address is used in the application server.
* If authentication components are installed on a non-windows operating system then continue with the existing operating system.

**Migration strategy**

* Application uses SharePoint for content management with users manually or triggered by an event. Make sure SharePoint is migrated to the new AD domain.
* Perform necessary testing and BCP testing.

**Note** – To request creation of a new SharePoint site on new AD domain, refer section ‘**this’**

#### <<$No\_Data\_Repository\_Utilization>>

Application doesn’t using any SharePoint, 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.

# References

## Request for new server

* Step1
* Step2

## Request for new service/technical account

* Step1
* Step2

## Request for local share

* Step1
* Step2

## Request for **shared mailbox**

* Step1
* Step2

## Request for new DL

* Step1
* Step2

## Request for file/folder/registry permissions

* Step1
* Step2

## Support Information

|  |  |
| --- | --- |
| **Support Category** | **Contact Information** |
| Application owner | <<App\_OwnerName>> |
|  |  |
|  |  |