/Modernize IAM accelerators for CA SiteMinder

CA SiteMinder Migration - ForgeRock Solution Guide

Table of Contents

/ Author	/ Action	/ Date	/ Version
Daniel Coman	Draft - Template	2020-07-15	0.1

1 Introduction

The purpose of this document is to provide guidance for customers and partners to accelerate migration projects from CA SiteMinder to the ForgeRock Identity Platform.

The target audience for this document is technical staff (enterprise architect, solution architect, integration architect) with a general understanding of identity and access management systems.

1.1 Glossary

The following terms and abbreviations are used in this guide:

Term	Description
AM	ForgeRock Access Management
SSO	Single Sign-On
IG	ForgeRock Identity Gateway
RP	Reverse Proxy
CA	Computer Associate's
API	Application Programmable Interface
OIDC	OpenID Connect
RS	Resource Server
PEP	Policy Enforcement Point
PDP	Policy Definition Point
TLS	Transport Layer Security
REST	Representational State Transfer

1.2 CA SiteMinder Architecture

The following typical legacy solution architecture is a baseline for the Modernize IAM Accelerators:

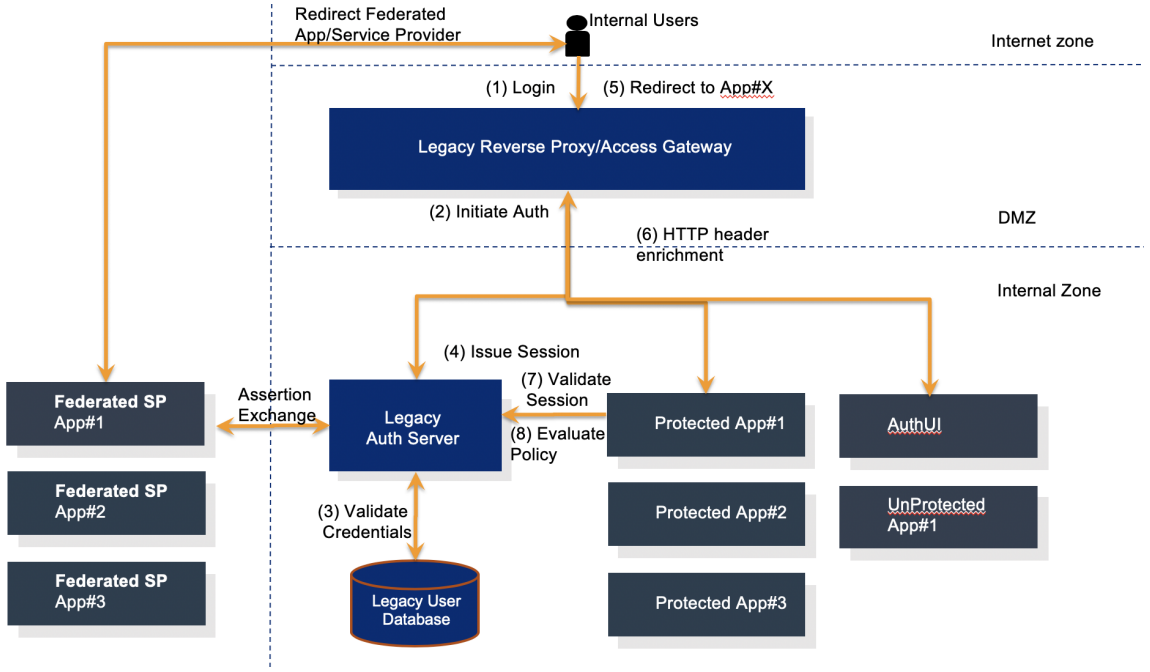

Figure 1 - Legacy CA SiteMinder Deployment

System	Role
CA SiteMinder	Validates authentication and authorization requests
Legacy reverse proxy	Unified point of entry inside the domain
Legacy User Store	User store (eg. Active Directory)
Protected apps	Existing applications integrated with CA SiteMinder
Auth UI	Legacy UI pages for authentication (login, logout)
Unprotected apps	Existing applications not protected by CA SiteMinder

2 ForgeRock AM Based SSO Toolkit for CA SiteMinder

2.1 Target Customer Deployment

The ForgeRock AM-based SSO Toolkit accelerates migration activities in customer scenarios where the following assumptions are met:

- CA SiteMinder deployment with Siteminder Java AgentAPI and the DMS API is available
- A username & password authentication scheme is used in SiteMinder
- The userstore is configured
- The user profile API (/userinfo) is available

The toolkit implementation has been tested against CA SiteMinder 12.8 and Active Directory as the user store.

2.2 High Level Reference Architecture

The reference architecture for the AM-based SSO Toolkit consists of:

- ForgeRock Access Manager
- ForgeRock Directory Server
- ForgeRock Identity Manager
- CA SiteMinder 12.8 Runtime with standard configuration, having Active Directory user store
- CA Siteminder 12.8 Java AgentAPI and the DMS API

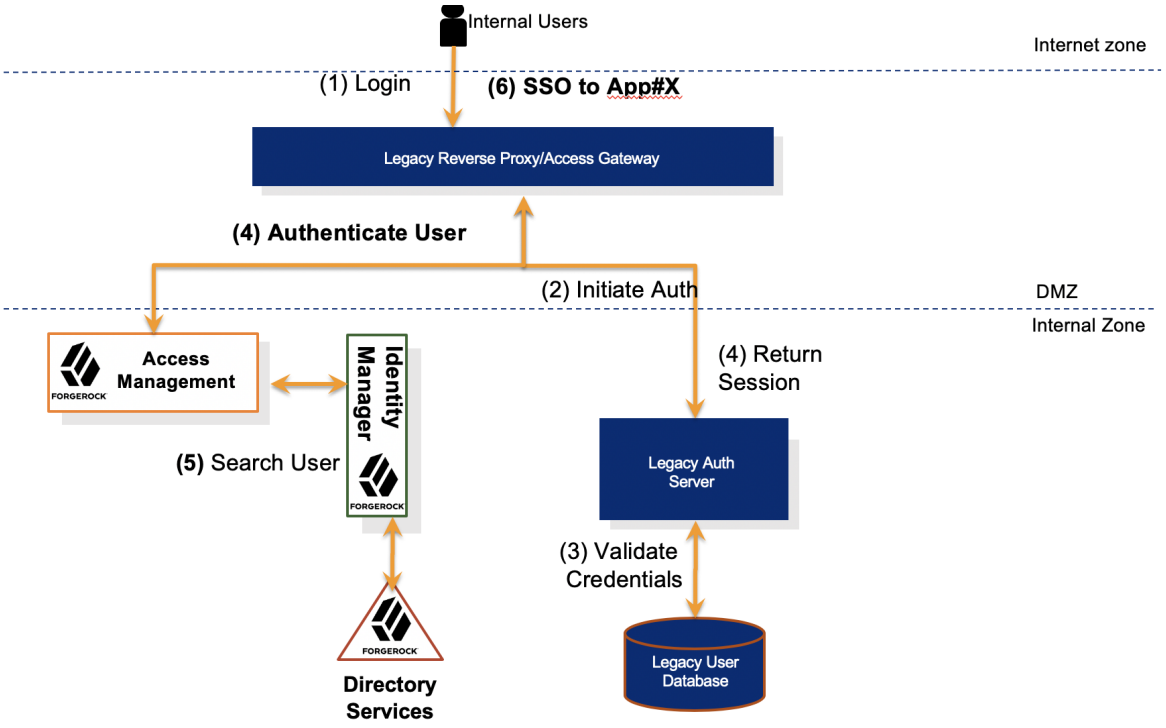

Figure 2 - AM based SSO Framework for CA SiteMinder

2.2.1 Scope Definition

The toolkit provides a collection of custom nodes and a migration tree that can handle very complex migration scenarios, including bidirectional SSO between CA SiteMinder and ForgeRock AM.

The framework can be easily extended to support migration from any CA SiteMinder platform that exposes client SDKs/APIs for operations such as:

- Validating existing CA SiteMinder tokens
- Calling the authentication API, with a username and password as input

2.2.2 Extensible Framework for Bidirectional SSO

Powered by ForgeRock Intelligent Authentication and the powerful capabilities of authentication trees, the framework has built-in capabilities to detect:

- An existing CA SiteMinder session;
- Whether users are provisioned (or partially provisioned) in ForgeRock Directory Server;
- Whether users have already been migrated but are missing passwords.

Validation of a user-entered password in CA SiteMinder is used as a decision point that determines whether the password is ready to be provisioned in ForgeRock IAM.

The Migration authentication tree provides these capabilities. Successful authentication using this tree results in a valid ForgeRock Access Manager SSO token that enables subsequent execution of outbound SSO flows using OIDC or SAMLv2.

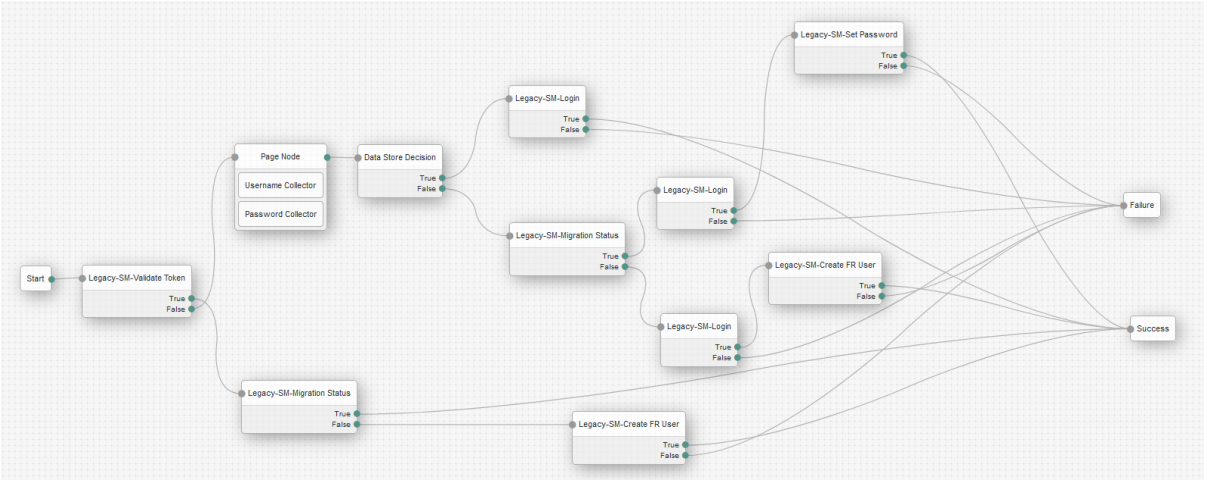

Figure 3 - Migration Authentication Tree

2.2.3 Migration Accelerators Package

The following high-level configuration of modules and extensions are included in this package:

System	Type	Name	Description
AM	Node	Legacy-SM-Validate Token	Detects if an existing legacy token exists in the browser in a specific cookie and validates this as an active token against the legacy IAM system via an SDK/API call. The default node uses a GET API call with the cookie fetched from the incoming http request. The name of the cookie and the target URL is configurable.
AM	Node	Legacy-SM-Migration Status	Searches ForgeRock IDM to obtain the user identity based on the username from the shared state.
AM	Node	Legacy-SM-Create FR User	Calls the ForgeRock IDM API to provision the managed user.
AM	Node	Legacy-SM-Login	Validates the credentials (username and password) entered by the user against the legacy SiteMinder IAM system via an SDK/API call.
AM	Node	Legacy-SM-Set Password	Updates the ForgeRock IDM managed user object with the password captured and stored in the shared state.
AM	Tree Hook	LegacySMSessionTreeHook	Manages cookies if a successful login is performed into CA SiteMinder by the tree.
AM	Authentication Tree	siteminderMigrationSsoTree	Implements migration login and bidirectional SSO.
AM	Custom Nodes	openam-modernize-siteminder-auth-nodes-1.0-SNAPSHOT.jar	Custom AM nodes that are used in the migration authentication tree.

2.2.3.1 External Libraries Needed for Rebuilding the Code

- The migration toolkit uses the CA SiteMinder Java AgentAPI and the DMS API. Download the SDK from your CA SiteMinder support page or get the required jar files from your existing CA SiteMinder installation. The migration toolkit requires the following jar files:
    - smagentapi.jar

- smjavasdk2.jar
- smcrypto.jar
- bc-fips-1.0.1.jar

2.3 Solution Design

2.3.1 Migration Authentication Tree

The execution of the Migration tree depends on the current state of the user profile:

- Existing user profile and password – no provisioning is required
- Existing user profile but no password – authentication to CA SiteMinder and provisioning of the user password is required
- Existing legacy SSO session – only provisioning of the user profile can be executed
- No existing user profile – upon successful authentication to CA SiteMinder, both the user profile and user password are provisioned and SSO is triggered

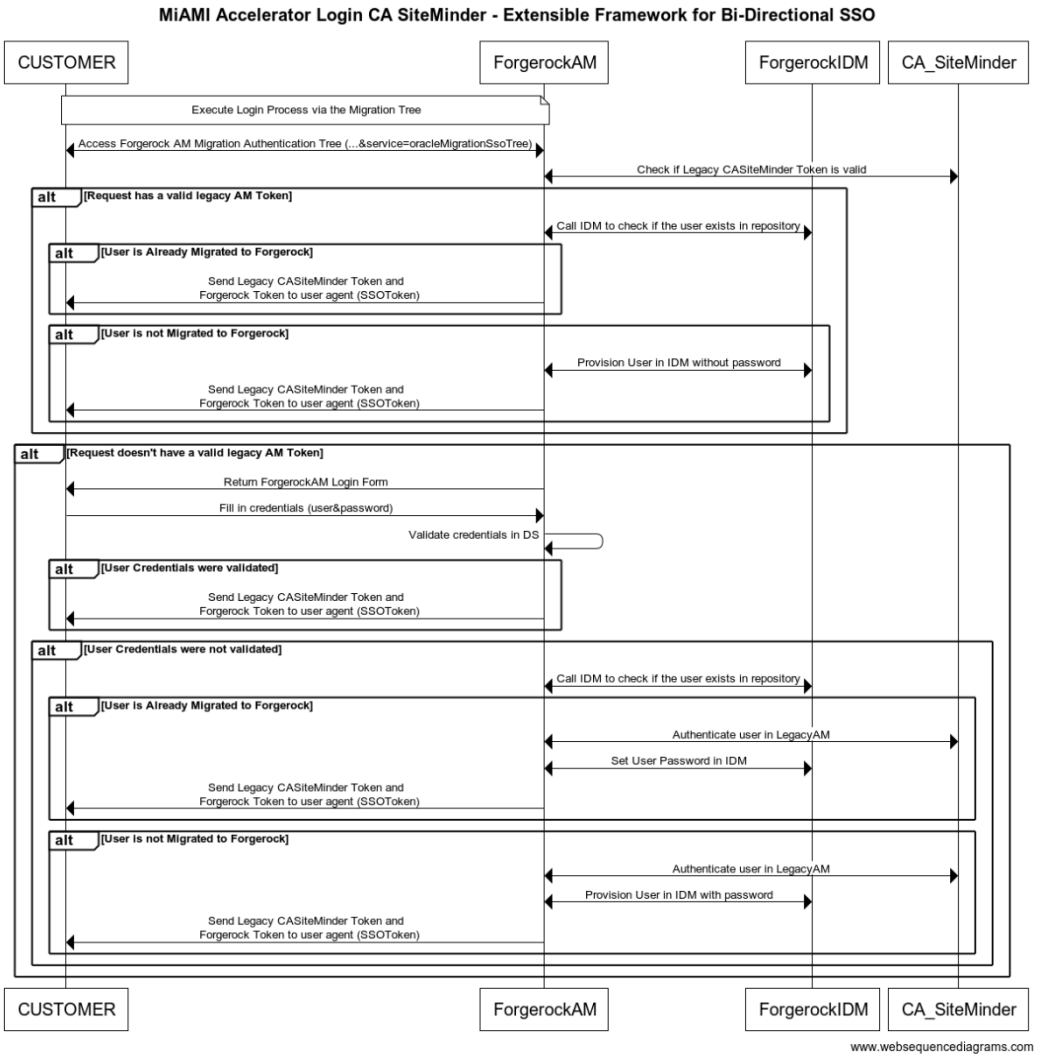

Figure 4 - Extensible Framework for BI-Directional SSO

2.3.2 Scenarios

2.3.2.1 ***Scenario 1*** - The user has a valid legacy CA SiteMinder SSO token in the browser, and accesses the authentication tree

- The user (not previously migrated) authenticates first to the legacy CA SiteMinder instance.
- The user accesses the authentication tree.
- Upon accessing the tree, the user is automatically logged in because a valid legacy CA SiteMinder SSO token is present in the browser. As a result, a user profile is created in ForgeRock IDM and AM, with no password set.

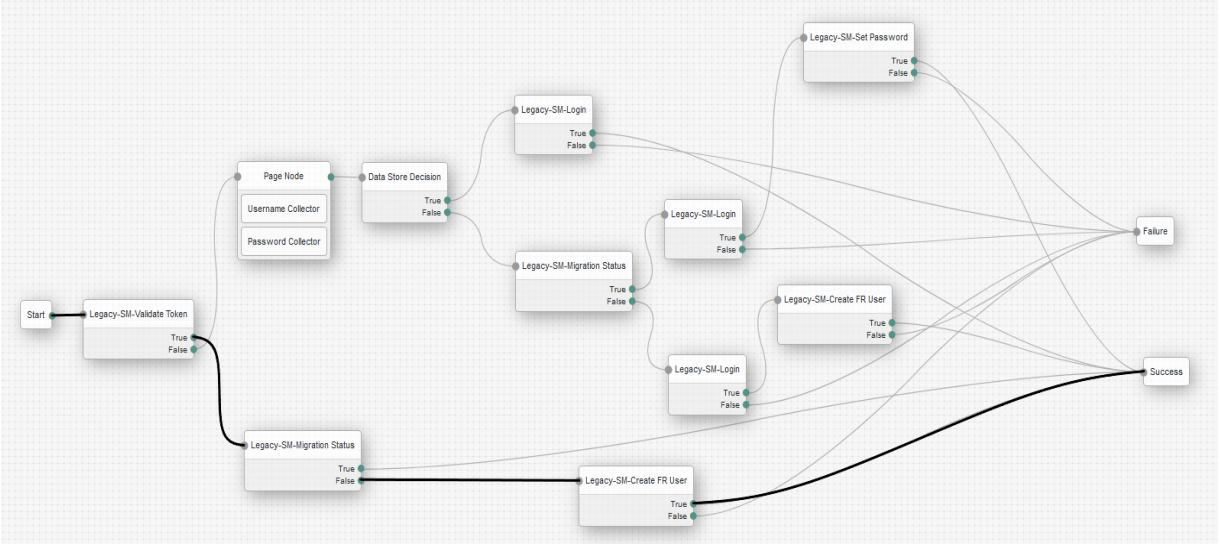

Figure 5 - Scenario 1

2.3.2.2 ***Scenario 2*** - The user accesses the authentication tree, with no legacy CA SiteMinder SSO token in the browser, after previously he accessed Scenario 1 - was created with no password

- The user accesses the authentication tree. The tree is prompting the user for the username and password.
- After providing credentials, the user is successfully authenticated. This happens because the user was successfully logged in to the legacy CA SiteMinder. Since the Data Store Decision node returned false but the user

was already migrated, and the legacy login was successful, the password is also updated in DS.

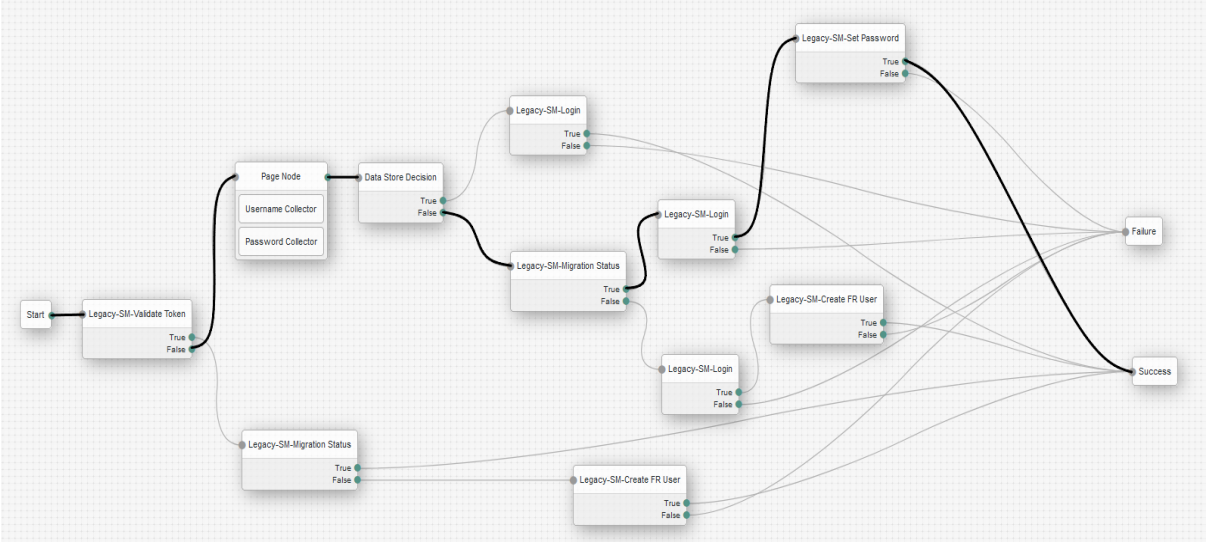

Figure 6 - Scenario 2

2.3.2.3 ***Scenario 3*** - The user is not migrated, does not have a valid legacy CA SiteMinder SSO token, and accesses the authentication tree

- The user accesses the authentication tree. The tree prompts the user for the username and password.
- After providing credentials, the user is successfully authenticated. This happens because the user was successfully logged in to the legacy CA SiteMinder instance, and the user's profile was successfully provisioned in ForgeRock DS, including the password.

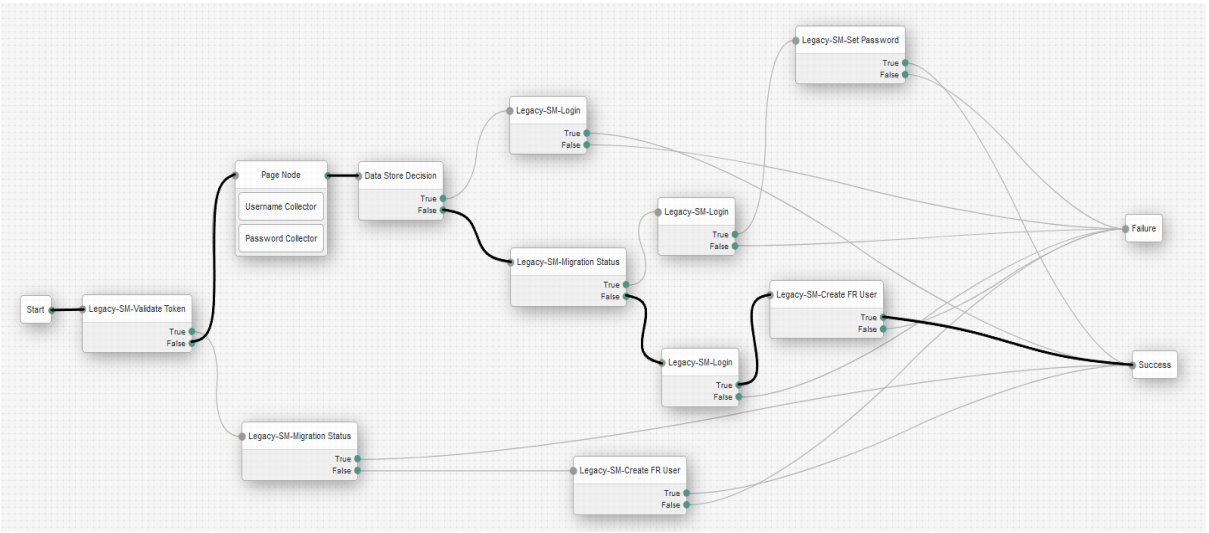

Figure 7 - Scenario 3

2.3.2.4 ***Scenario 4*** - This scenario is triggered when the user has a valid legacy CA SiteMinder SSO token in the browser and is already migrated

- The user (previously migrated) authenticates first to the legacy CA SiteMinder instance.
- The user accesses the authentication tree.
- The outcome of this scenario is that the user is authenticated automatically to both the legacy CA SiteMinder instance and to ForgeRock AM after execution of the tree has completed.

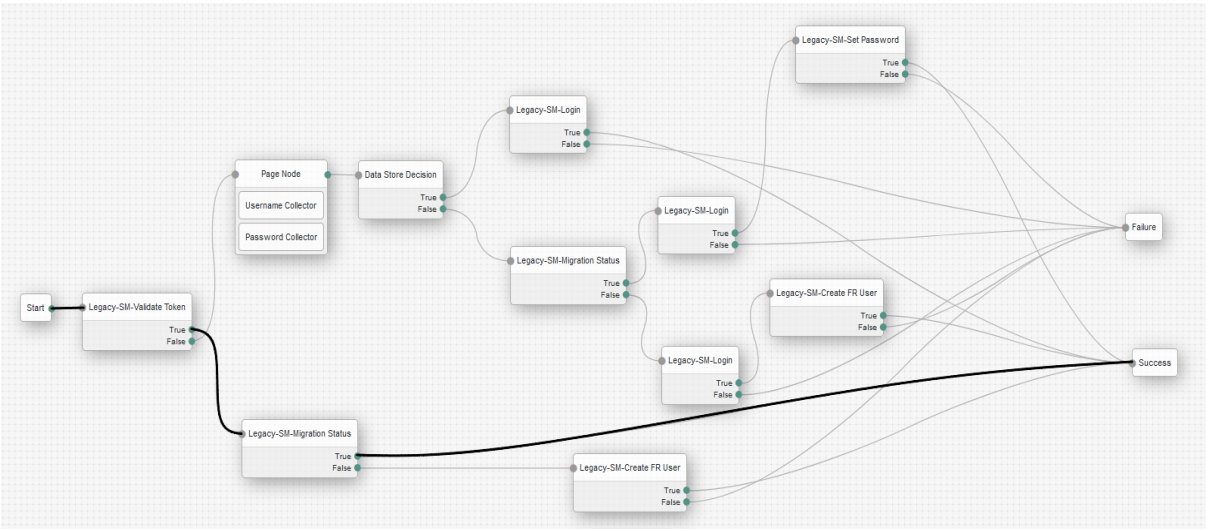

Figure 8 - Scenario 4

2.3.2.5 ***Scenario 5*** - This is the standard scenario triggered when the user is already migrated, and a Data Store Decision node authenticates the user successfully

- The user accesses the authentication tree. The tree prompts the user for the username and password.
- The outcome of this scenario is that the user is authenticated automatically to both the legacy CA SiteMinder instance and to ForgeRock AM after execution of the tree has completed.

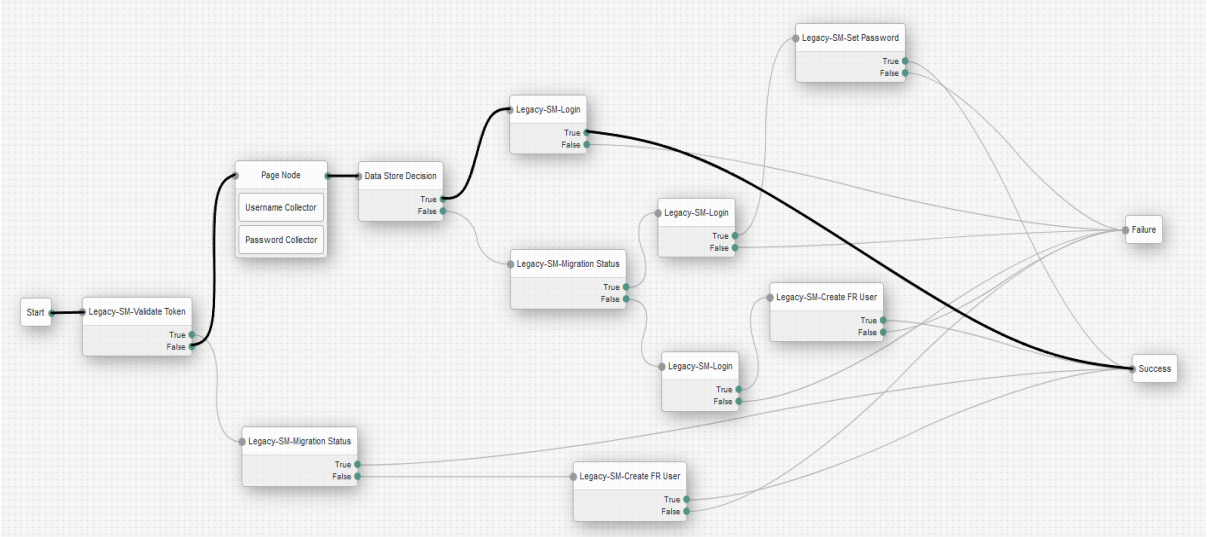

Figure 9 - Scenario 5

2.3.3 Secret Stores

The passwords used in the toolkit authentication tree nodes must be saved in secret stores for security reasons.
The toolkit uses AM secret stores as described in the ForgeRock documentation.