



Migrating applications from Symantec SiteMinder to Azure Active Directory

[Abstract](#)

In this document, we provide the planning for and benefits of migrating your application authentication from Symantec SiteMinder to Azure AD.

For the latest version of this document check: <https://aka.ms/SiteMinderToAzureAD>

Last updated: June 2021

A decorative graphic on the left side of the page, consisting of several thin, curved lines in shades of blue and grey that sweep upwards and to the right.

© 2021 Microsoft Corporation. All rights reserved. This document is provided "as-is." Information and views expressed in this document, including URL and other Internet Web site references, may change without notice. You bear the risk of using it. This document does not provide you with any legal rights to any intellectual property in any Microsoft product. You may copy and use this document for your internal, reference purposes. This document is confidential and proprietary to Microsoft. It is disclosed and can be used only pursuant to a non-disclosure agreement.

Contents

- Introduction..... 2
 - Overview..... 2
 - Key benefits..... 3
 - Architecture overview 4
- Plan your migration phases and project strategy..... 6
 - The phases of migration 6
 - Assemble the project team 7
- Phase 1: Discover and plan..... 8
 - Discover the applications 8
 - Create applications inventory 9
 - Prepare the roadmap 14
- Phase 2: Deploy Azure AD 16
 - Azure AD deployment steps..... 16
 - Communicate updates to user 17
- Phase 3: Migrate and integrate your applications..... 18
 - Types of apps to migrate..... 18
 - Integrate your apps..... 18
 - Address governance and compliance requirements 24
 - Setup access control policies 25
- Remove Symantec SiteMinder 28
- Example: Symantec SiteMinder to Azure AD application migration using F5 BIG-IP APM 28
 - Migration of PeopleSoft..... 28
- Frequently asked questions 35
- Appendix A: Modernize applications..... 36
- Appendix B: Coexistence strategy 37

Introduction

This document is intended for the following audiences:

- Technology executives, for example CIOs, or CISOs evaluating their options for replacing their existing Symantec SiteMinder solution
- Security architects planning their Symantec SiteMinder to Azure AD migration
- Security and Identity and access management (IAM) engineers moving applications from Symantec SiteMinder to Azure AD

Overview

For organizations that currently use Symantec SiteMinder for their Single sign-on (SSO) solution, migrating to [Azure Active Directory \(AD\)](#) offers a frictionless user experience through [Azure AD SSO](#).

The following considerations are important for any SSO solution:

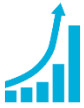
- **High availability:** When fully implemented, SSO is critical to the operation of your organization. If the SSO solution is down, access to all applications that are integrated with it becomes unavailable.
- **Built to handle unexpected loads:** Business needs and application usage changes over time. These changes can be either temporary, for example, a promotion or enrollment period, or permanent in case of a merger or acquisition.
- **Includes updated threat detection and mitigation:** Detecting and mitigating threats requires a solution that not only provides the required capabilities but can also be updated quickly and reliably as new threats are encountered.

In this document, we provide the planning for and benefits of migrating your application authentication from Symantec SiteMinder to Azure AD.

To deploy Azure AD SSO, you require an Azure AD subscription. Microsoft offers a [trial subscription](#).

Key benefits

Moving app authentication to Azure AD will help you manage risk and cost, increase productivity, and address compliance and governance requirements.



INCREASE PRODUCTIVITY

Enabling SSO across enterprise applications and Office 365 provides a superior sign-in experience for existing users. The user's environment feels more cohesive and is less distracting without multiple prompts or the need to manage multiple passwords.



MANAGE RISK

Coupling Azure AD SSO with Conditional Access (CA) policies can significantly improve security. This includes cloud-scale [Identity Protection](#), [risk-based access control](#) capabilities, native [Multi-factor Authentication](#) support, and [CA policies](#), which allow for granular control based on applications, or on groups that need higher levels of security. This improves the overall security of the identity system by ensuring the right people have the right access to applications.



ADDRESS COMPLIANCE AND GOVERNANCE

Azure AD supports native audit logs for every application access request performed. It becomes easier to audit access requests and approvals for the application, as well as understanding overall application usage. Auditing includes requester identity, requested date, business justification, approval status, and approver identity. This data is also available from an API, which will enable importing this data into a [Security Incident and Event Monitoring \(SIEM\) system](#) of choice.



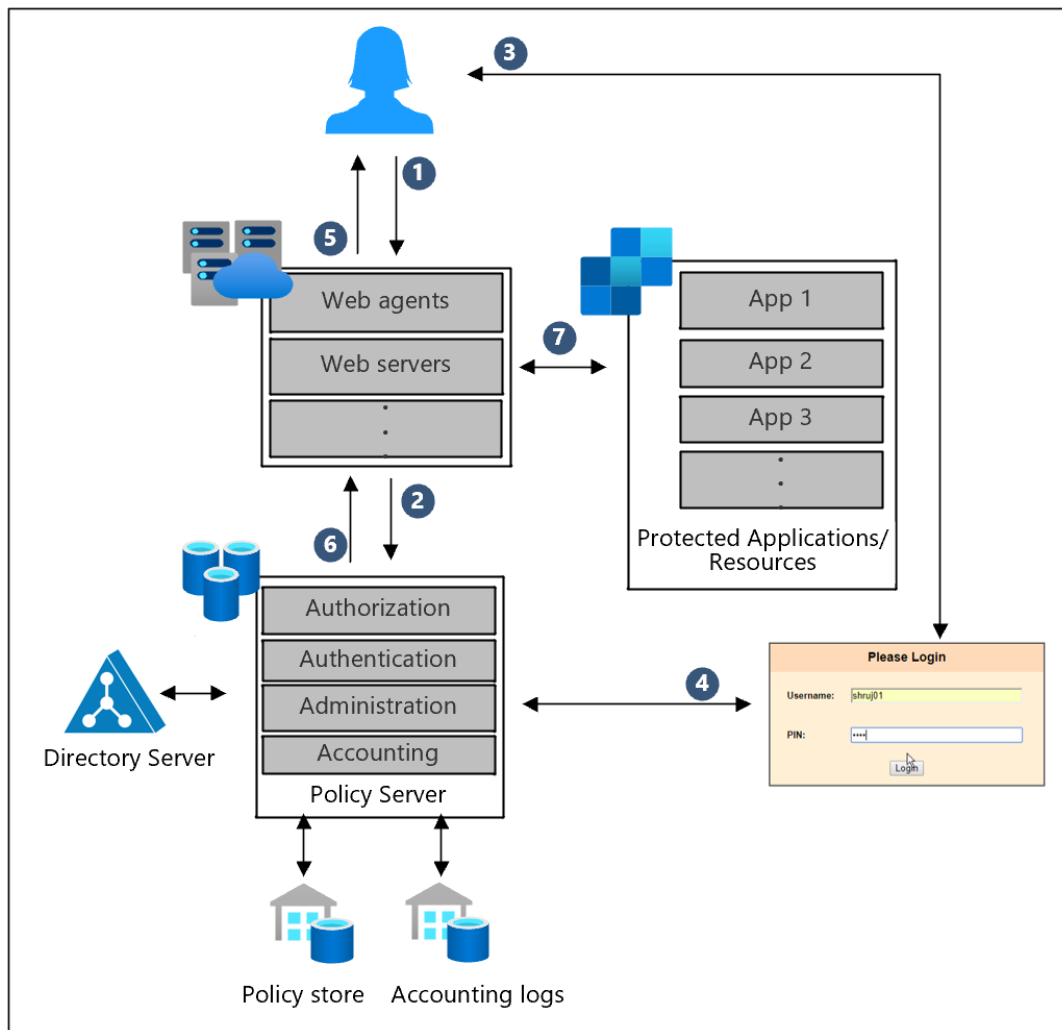
MANAGE COST

Replacing current access management and provisioning processes and migrating to Azure AD provides significant cost reductions related to running, managing, and maintaining on-premises infrastructure. Additionally, removing application specific password requirements eliminate costs related to password reset for that application, and lost productivity while retrieving passwords. Access controls are managed and approved by business groups, saving IT Management cost through [self-service and dynamic membership](#).

Architecture overview

In the following diagram, we discuss the **current high-level Symantec SiteMinder architecture**. It includes the following components:

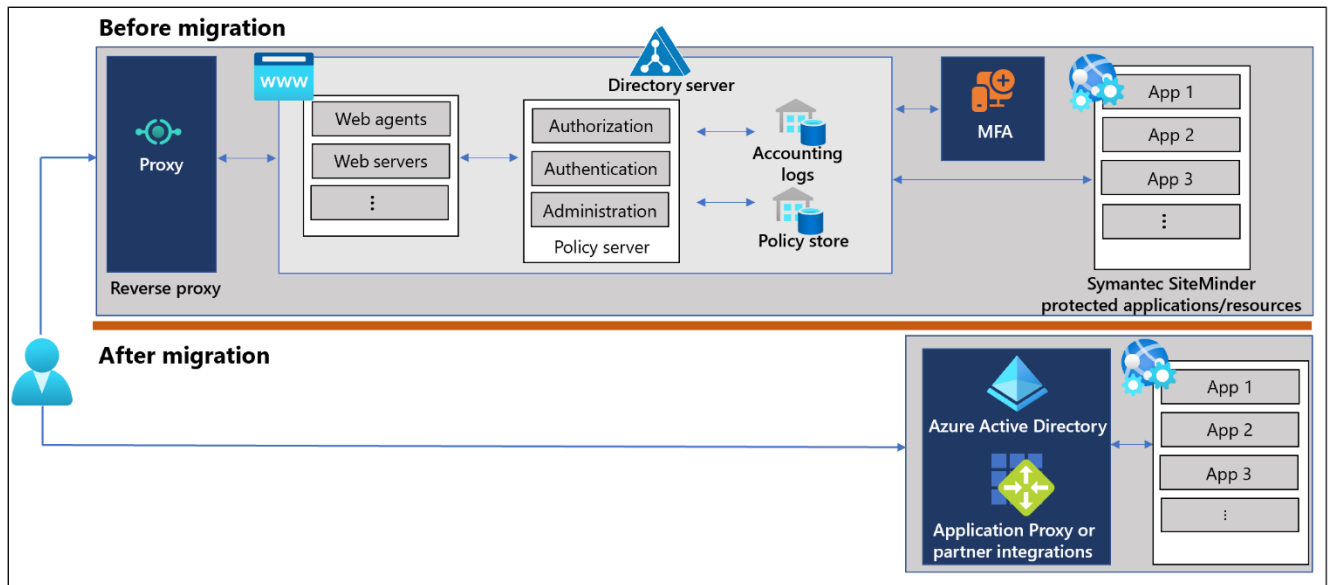
- **Policy server:** The policy server handles configuring and enforcing authentication and authorization policies. The policy configuration is stored in a policy store database. The users, groups and group memberships are stored in an LDAP directory server and audit information is stored in the accounting logs database.
- **Web server/Web agent:** A Symantec SiteMinder Web agent is installed on each of the application web servers. The web agents' interface with the policy server to enforce authentication and authorization policies. There are also application server and Enterprise Resource Planning (ERP) agents that work in a fashion like the web agent but are installed on the Application or ERP servers.
- **Application resources:** The web agents change the incoming request and forwards them to the application being protected. The user identity information is supplied to the application via HTTP headers or other methods as per the application requirement.



Description of workflow:

1. An end-user accesses an application that is protected by Symantec SiteMinder
2. The Symantec SiteMinder web agent or reverse proxy checks for a session
3. If no sessions exist, the end-user is asked to authenticate
4. Symantec SiteMinder validates the end-user credentials
5. The end-user is redirected to the application
6. The web agent or reverse proxy protecting the application checks the authorization with Symantec SiteMinder
7. The web agent or reverse proxy sends the HTTP headers to the application.

Once the application is migrated to Azure AD, **the end-state architecture changes**. See this diagram:



With this migration, Azure AD provides these **key differences and benefits**:

- **Lower Infrastructure costs:** The Azure AD solution resides almost entirely in the cloud. [Application Proxy](#) requires some infrastructure to interface with on-premises applications. Migration to the Azure AD solution can be done with no changes to the application.
- **Built-in security:** The Azure AD solution takes advantage of and implements modern security mechanisms, for example, Multi-Factor Authentication, OAuth, and OpenID Connect (OIDC), to centralize administration and minimize the need for 3rd party solutions.
- **Reduced maintenance and administration:** The burden of upgrades, patching and enforcing security are managed as part of the Azure AD solution which reduces the risk to the organization and allows the IT staff to address organization-specific infrastructure needs.

Plan your migration phases and project strategy

When technology projects fail, it is often due to mismatched expectations, the right stakeholders not being involved, or a lack of communication. Ensure your success by planning the project itself.

The phases of migration

Before we get into the tools, understand how to think through the migration process. Through several direct-to-customer workshops, **we recommend these three phases:**

Phase 1 – Discover and plan

- a. Document the current Symantec SiteMinder architecture and deployment
- b. Create an application inventory. Note the current configuration and integration requirements
- c. Build a roadmap for the migration



Phase 2 – Deployment of Azure AD

Deploying Azure AD is a prerequisite for using Azure AD SSO. Ensure you understand all requirements including attributes that are needed to access the applications, and that are available in Azure AD.



Phase 3 – Application migration

Using the roadmap developed in the first two phases, migrate the applications from Symantec SiteMinder to Azure AD. Migration involves the application, Azure AD and Symantec SiteMinder teams. Symantec SiteMinder will first be integrated with Azure AD so that the two solutions can coexist during the migration timeframe. This allows for a controlled rollout to accommodate the release schedules of the applications being migrated.

Assemble the project team

Application migration is a team effort, and you need to ensure that you have all the vital positions filled. During the migration project, one person may fulfill multiple roles, or multiple people fulfill each role, depending on your organization's size and structure. You may also have a dependency on other teams that play a key role in your security landscape.

The following table includes the key roles and their contributors:

Roles	Responsibilities
End-user	A representative group of users for whom the capabilities will be implemented. They often preview the changes in a pilot program.
IT Support Manager	A representative from the IT support organization who can provide input on the supportability of this change from a helpdesk perspective.
Identity Architect	Identity management team representative responsible to: <ul style="list-style-type: none">• design the solution in cooperation with stakeholders• document the solution design and operational procedures for handoff to the operations team• manage the pre-production and production environments Identity management team representative in-charge of defining how this change is aligned with the core identity management infrastructure in your organization.
Azure Global Administrator	Azure AD administration leads responsible for the configuration and licensing of the Azure AD solution
Symantec SiteMinder Team Manager	Technical resource who understands the current Symantec SiteMinder deployment and making any changes to the Symantec SiteMinder configuration required to support the migration.
Application Business Owner	The overall business owner of the affected application(s), which may include managing access. May also provide input on the user experience and usefulness of this change from an end-user's perspective.
Security Owner	A representative from the security team that can sign off that the plan will meet the security requirements of your organization.
Compliance Manager	The person within your organization responsible for ensuring compliance with corporate, industry, or governmental requirements.

Phase 1: Discover and plan

Application discovery and analysis is a fundamental exercise to give you a good start. The first decision point in migration is to decide which **applications are in-scope** for the migration and **which integration method(s)** will be used to migrate them.

Discover the applications

The **planning table** can help prepare the strategy for various applications as they are discovered. The inventory of the applications in scope, version, number of users and business priorities are some of the first items to be captured.

Refer to the following sample table to capture this information:

Applications		Version	Users	Priority	Migration strategy	Integration strategy	Migration effort	Notes
	PeopleSoft	9.x	45k					
	Oracle EBS	12i	100k					
	Salesforce	SaaS	100k					
	Custom App	1.0	50k					
	AccountsPay	12.1	10k					






Create applications inventory

This phase analyses the discovered applications and develops roadmap for the **migration/integration strategy** based on the technologies used and options available. The migrated solution will need to meet requirements that are either part of the existing Symantec SiteMinder solution or new requirements that will be addressed as part of the migration. Choosing the proper tools to meet the solution requirements requires a high-level understanding of the features and capabilities available in each toolset.

Gather this information:

- [Application control and integration requirements](#)
- [Application integration methods](#)
- [Application configurations](#)

Use this table to update your migration and integration strategy for each application:

Applications	Version	Users	Priority	Migration strategy	Integration strategy	Migration effort	Notes
 PeopleSoft	9.x	45k		Migrate	Azure AD App Proxy		
 Oracle EBS	12i	100k		Migrate	F5 BIG-IP APM		
 Salesforce	SaaS	100k		Migrate	SAML Azure AD Gallery App		
 Custom App	1.0	50k		-	-		
 AccountsPay	12.1	10k		-	-		

Access control and integration requirements

The following table provides a description of the access control and integration requirements, and prevalence satisfied by most Symantec SiteMinder solutions.

Requirement	Type	Prevalence	Description
Federated SSO	Authentication	Common	This is generally implemented using one of the standard SSO protocols, for example, Security Assertion Markup Language (SAML) or OIDC
Header based integration	Integration	Common	An Application Proxy solution performs the SSO integration with the Identity Provider (IDP) and then passes identity or other application data as HTTP headers to the application
Application authorization	Authorization	Common	CA policies can be specified based on the application being accessed, the user's group membership or other policies. This only applies to the initial authentication to the application and does not manage subsequent application requests.
Step-up authentication	Authentication	Occasional	Policies can be defined to force added authentication, for example, to gain access to sensitive resources.
Fine grained authorization	Authorization	Occasional	Provides access control at the URL level. Added policies can be enforced based on the URL being accessed.
Authorization mapping	Integration	Occasional	If not all, information related to an authorization decision is available in the authentication user store. Additional user data can be retrieved from a separate user store to make authorization decisions provided to the application.

Requirement	Type	Prevalence	Description
Immediate access termination	Authorization	Occasional	Provides the capability to terminate a session as soon as a user is terminated rather than waiting for the next login.
Cookie based integration	Integration	Rare	An Application Proxy solution performs the SSO integration with the IDP and then passes identity or other application data as HTTP cookies to the application. Note: This is not a common integration, but it is supported by Symantec SiteMinder.
Time based authorization	Authorization	Rare	Allows access only during certain times of the day.
Impersonation	Authorization	Rare	Allows an administrator to assume the authentication context of a user. This allows Helpdesk administrators to see exactly what the end user sees, for instance.

Note: Some of the requirements in the table may have used features or capabilities in Symantec SiteMinder that are not available in Azure AD. This, however, can be easily resolved **by fulfilling the same requirement with a different design in Azure AD**. For instance, if authorization mapping is required, Azure AD can sync with an external data source to store the additional authorization information rather than retrieving the data when the user is authenticated.

There are options such as **Open-Source web server modules** that customers can use, depending upon their infrastructure and application architecture. These options can also address the above requirements. The Symantec SiteMinder solution will have addressed some governance and compliance requirements as well.

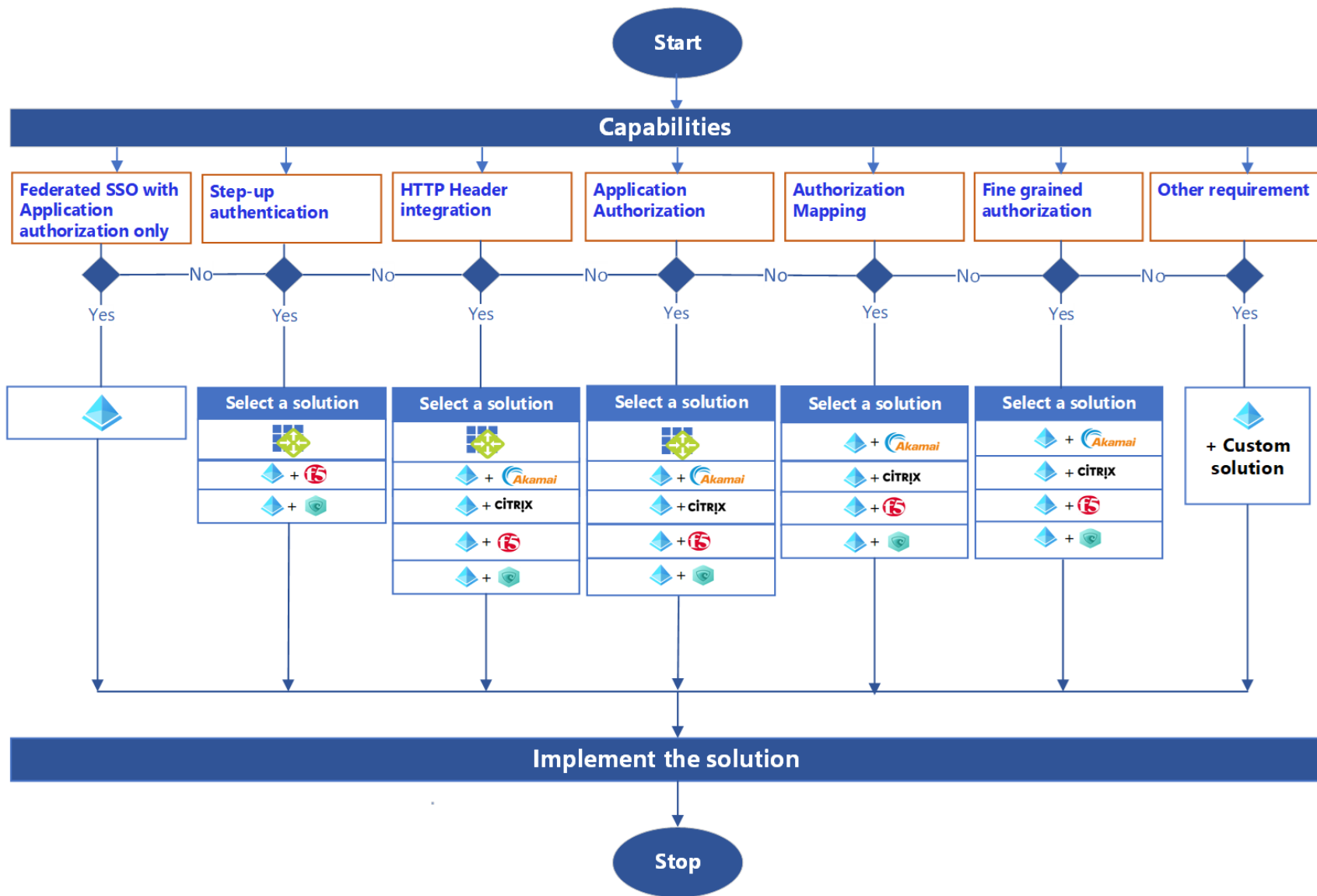
Application integration methods

The migration path for each application is determined by which application integration method is used. There are two ways to integrate the applications.

- **If the application supports, or can be changed to support SAML or OIDC**, then the application should be integrated using one of the protocols. The configuration used will be like the applications that are currently integrated in Symantec SiteMinder.
- **If the application can't be integrated using SAML or OIDC**, then the Azure AD Application Proxy or one of the available Application Delivery Controllers (ADCs) such as Akamai and Citrix NetScaler should be used for integration. These applications will generally replace the Symantec SiteMinder web agent to pass HTTP headers to the application.

The following ADC solutions are available:

- [Azure AD Application Proxy](#)
- [Akamai](#)
- [Citrix NetScaler](#)
- [F5 BIG-IP Access Policy Manager \(APM\)](#)
- [Strata Mavericks Identity Orchestrator](#)



Application configurations in Symantec SiteMinder

You will also need this information from your current applications for a successful migration:

- Agent/Proxy integration details as configured in Symantec SiteMinder
- Authentication and authorization policies as applied in Symantec SiteMinder
- Session management policies and settings as applied in Symantec SiteMinder
- Branding details, whether the application have special corporate branding requirements that are applied or affected by Symantec SiteMinder integration.
- User endpoint information, such as types and versions of browsers, mobile devices and other user-agents that are used to access the applications.

The migration of these Symantec SiteMinder configurations can be scripted using the [Symantec SiteMinder Policy REST API](#) or [CLI](#). Understand if the requirements are already integrated with the existing Symantec SiteMinder solution or need to be addressed with migration.

Prepare the roadmap






Classifying the migration of your apps is an important exercise. Not every app needs to be migrated and transitioned at the same time. Once you have collected information about each of the apps, you can rationalize which apps should be migrated first and which may take added time.

1. Put applications in specific categories based on the decision chart and set priorities.
2. Determine time required to migrate.
3. Coordinate with application release schedules.

We recommend that you prepare the roadmap as per the following criteria:

- **Application criticality:** Applications with large user bases or, the one that has high usability, and are mission critical should not be migrated first.
- **Application migration complexity:** Applications that already are integrated using SAML or OIDC should be migrated first assuming all other criteria are equal. Applications that require customizations or other integration steps should be migrated later since they will take some time to setup and test in non-production environments.
- **Application release schedule:** The migration should be coordinated with planned application release schedules to either coincide with a scheduled upgrade or deploy as a separate release depending on the changes required for the migration and the changes being released in the application.
- **Decide which applications will not be migrated:** Some applications may be retired or replaced within the migration timeframe. If applications are scheduled to be retired within or shortly after the migration timeframe, they may be excluded from the migration.

Once you have classified your applications, update the information in your planning table:

Applications		Version	Users	Priority	Migration strategy	Integration strategy	Migration effort	Notes
	PeopleSoft	9.x	45k	3	Migrate	Azure AD App Proxy	3 days	
	Oracle EBS	12i	100k	1	Migrate	F5 BIG-IP APM	4 days	Requires IE + JDK
	Salesforce	SaaS	100k	2	Migrate	SAML Azure AD Gallery App	1 day	
	Custom app	1.0	50k	4	Upgrade	MSAL library integration	5 days	
	AccountsPay	12.1	10k	5	Retire	Replace with SaaS	1 day	

Phase 2: Deploy Azure AD

A well-planned and executed identity infrastructure paves the way for secure access to your productivity workloads and data by known users and devices only. [Azure AD deployment plans](#) walk you through the business value, planning considerations, and operational procedures needed to successfully deploy common Azure AD capabilities.

Azure AD deployment steps

Here is a high-level overview of the Azure AD deployment steps:

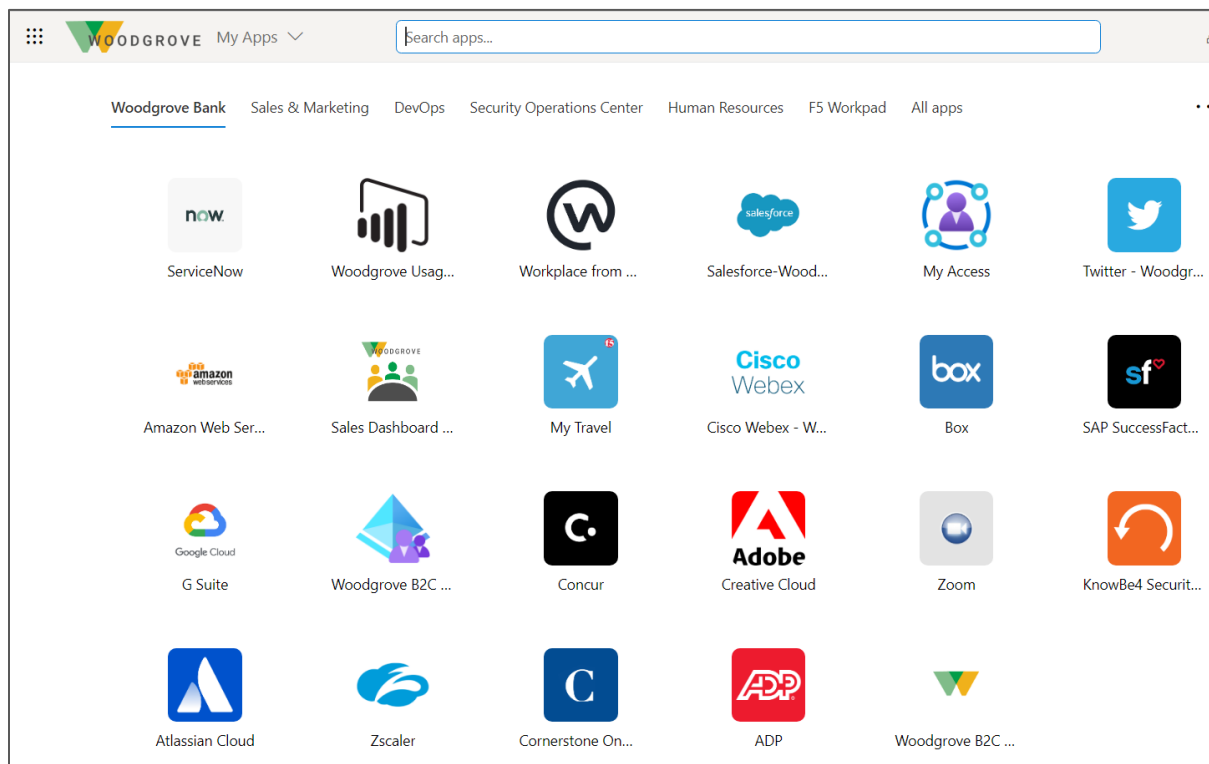
1. **Include the right stakeholders:** When beginning your deployment and planning for a new capability, it is important to include key stakeholders across your organization. We recommend that you identify and document the person or people who fulfill each of the following roles:
 - End-user
 - IT support managers
 - Identity architect or Azure global administrator
 - Application business owner
 - Security owner and Compliance manager
2. **Implement a pilot:** A pilot allows you to test with a small group before turning a capability on for everyone. Ensure that as part of your testing, each use case within your organization is thoroughly tested. It is best to target a specific group of pilot users before rolling this out to your entire organization.
3. **Deploy authentication:** The specific authentication mechanisms for your organization will be determined by your security requirements and use cases. The following authentication methods and capabilities are available:
 - Multi-Factor Authentication
 - CA policy
 - Self-Service Password Reset (SSPR)
 - Passwordless
4. **Deploy application management:** Applications are integrated to the Azure AD SSO solution using the right integration type. An application access panel is provided as a launch pad for the integrated applications and provides a mechanism for requesting and approving access to applications.
5. **Deploy hybrid access scenarios:** Some applications you will not be able to modify to integrate with any of the standard SSO federated solutions. These applications will need to have an Application Proxy or other mechanism to simulate their current integration.
6. **Deploy governance and reporting:** User application access governance needs to be implemented as part of the Azure AD solution. Azure AD provides tools for reporting on user application access that can be utilized to provide access certification to meet security and compliance requirements.

Communicate updates to user

During the coexistence/transition phase, the only difference that the end users will experience is that they will be using the Azure AD login page rather than the Symantec SiteMinder login page. The following notifications should be sent to the end users during this phase:

- When Azure AD is implemented and integrated with Symantec SiteMinder, **notify all users that their login page will change**. In addition, if any other security policy changes, for example, you implement Multi-Factor Authentication, communicate to the user.
- As each application is migrated from Symantec SiteMinder to Azure AD, **notify the application user community**. It is possible that application specific issues may surface when it is completely migrated to Azure AD, so the users need to know how to report and get support for these issues.
- There should be a **final notification to all users when Symantec SiteMinder is removed**. It is possible that some applications are overlooked during the migration and may experience issues that must get resolved.

Azure AD offers a centralized access console for your applications that includes both on-premises and cloud apps. This is where users can discover all applications without trying to call helpdesk or jump through multiple consoles.



Phase 3: Migrate and integrate your applications

When possible, applications should be [modernized](#) rather than migrated.

See the [Appendix A: Modernize applications](#) and [Appendix B: Coexistence strategy](#) for more info.

Types of apps to migrate

There are four main types of applications that you can add to your enterprise applications and manage with Azure AD:

- **[Azure AD Gallery applications](#):** Azure AD has a gallery that holds thousands of applications that have been pre-integrated for SSO with Azure AD. Some of the applications your organization uses are probably in the gallery. Learn about planning your app integration or get detailed integration steps for individual apps in the [SaaS application tutorials](#). These apps already use modern authentication protocols such as [SAML](#) or [OIDC](#), and can be reconfigured to authenticate with Azure AD.
- **[On-premises and legacy applications](#):** With Azure AD, you can integrate your on-premises web apps with Azure AD to support SSO. Then end-users can access your on-premises web apps in the same way they access Office 365 and other SaaS apps. Start by extending these apps into [Azure AD Application Proxy](#) or via our [partner solutions](#) with ADC you might have deployed already.
- **[Custom-developed applications](#):** When building your own Line-of-business (LOB) applications, you can integrate them with Azure AD to support SSO. By registering your application with Azure AD, you have control over the authentication policy for the application. If you have new apps in the pipeline, we recommend using the [Microsoft Identity Platform](#) to implement [OIDC](#).
- **[Non-Gallery applications](#):** These could be apps that already exist in your organization or any third-party apps from a vendor who is not a part of the Azure AD gallery. These apps also use [SAML](#) or [OIDC](#) and can be reconfigured to authenticate with Azure AD.

Integrate your apps

Once you identify the types of apps to migrate to Azure AD, use the tools and guidance in this section to integrate the apps to Azure AD.

SAML integration

The [SSO SAML protocol](#) describes the SSO sequence. The cloud service provider (SP) uses the HTTP redirect binding to pass an [AuthnRequest](#) (authentication request) element to Azure AD IDP. Azure AD then uses the HTTP post binding to post a Response element to the cloud service. If an application supports SAML integration, then it can be integrated for SSO directly with Azure AD.

For applications that do not support SAML or OIDC, you can use [Azure AD Application Proxy](#). This allows HTTP headers to be passed to the application to enable SSO.

OAuth/OIDC integration

[OIDC is an authentication protocol](#) built on OAuth 2.0 that you can use to securely sign in a user to an application. When you use the Microsoft Identity platform endpoint's implementation of OIDC, you can add sign-in and protect API access to your apps.

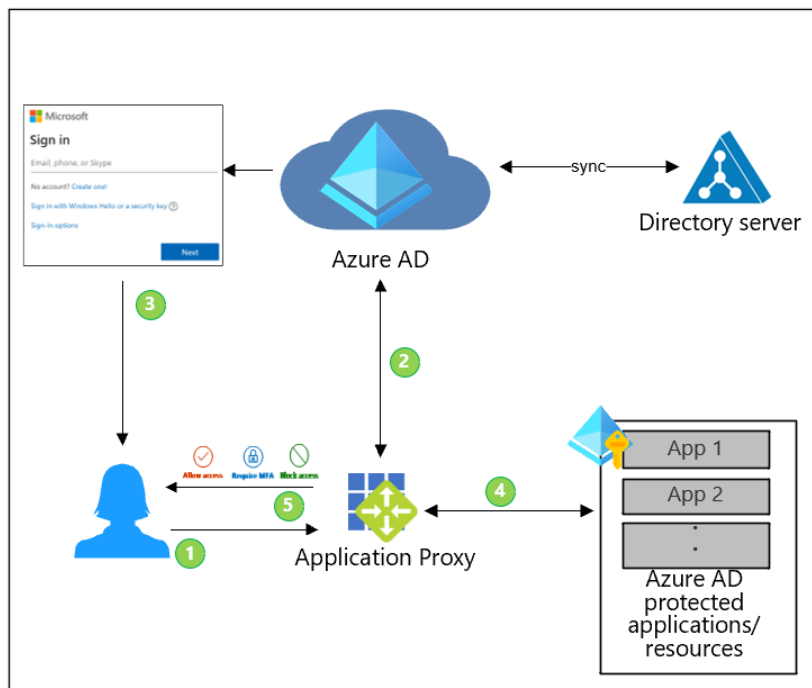
On-premises and legacy app integrations

Application Proxy integration

Azure AD's [Application Proxy](#) provides secure remote access to on-premises web applications.

After a SSO to Azure AD, users can access both cloud and on-premises applications through an external URL or an internal application portal. For example, Application Proxy can provide remote access and SSO to [Remote Desktop](#), [SharePoint](#), [Teams](#), [Tableau](#), [Qlik](#), and [LOB applications](#).

The following diagram shows how Azure AD and Application Proxy work together to provide SSO to on-premises applications.

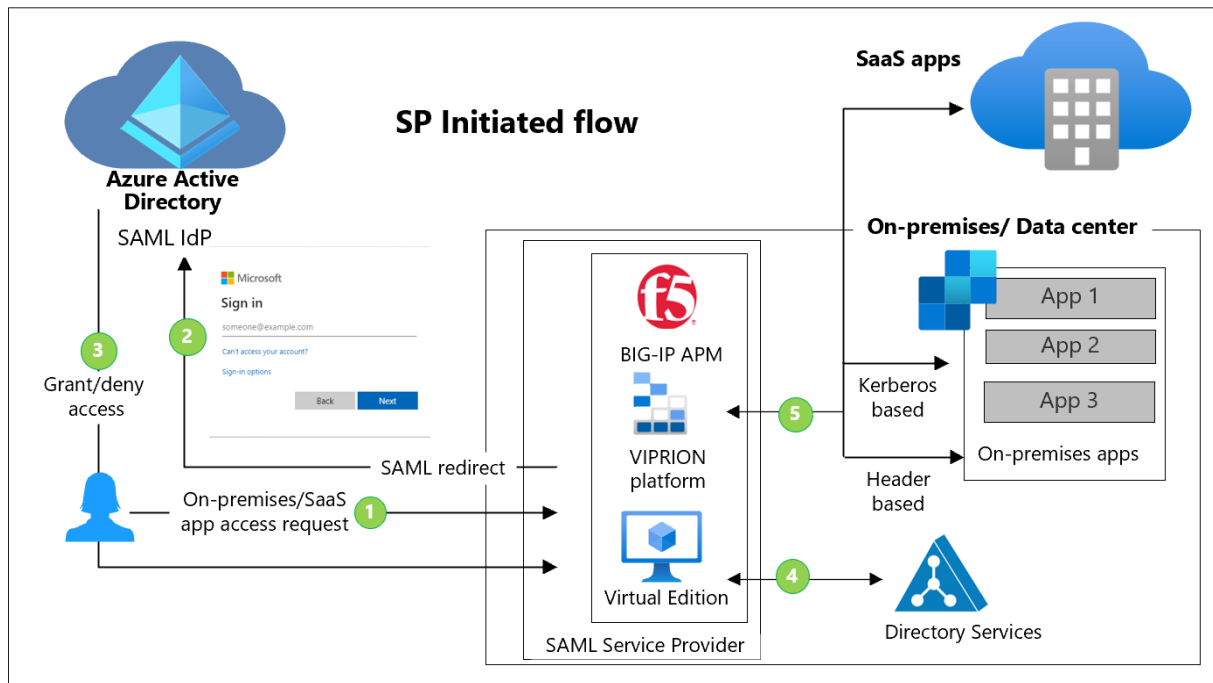


Description of workflow:

1. User requests access to an application protected by Azure AD (with or without a partner solution).
2. Azure AD checks for an existing session.
3. If no session exists, the user is asked to authenticate.
4. Based on the user context, such as location, device health, or group membership, Azure AD Conditional Access authorizes the user to access the content.
5. Azure AD (with or without a partner solution) serves the application data to the user using a secure channel.

F5 BIG-IP APM integration

The following diagram shows the [SSO integration with the F5 BIG-IP \(APM\)](#). This integration allows the F5 BIG-IP APM to act as a reverse-proxy with Kerberos or HTTP header SSO to the app.



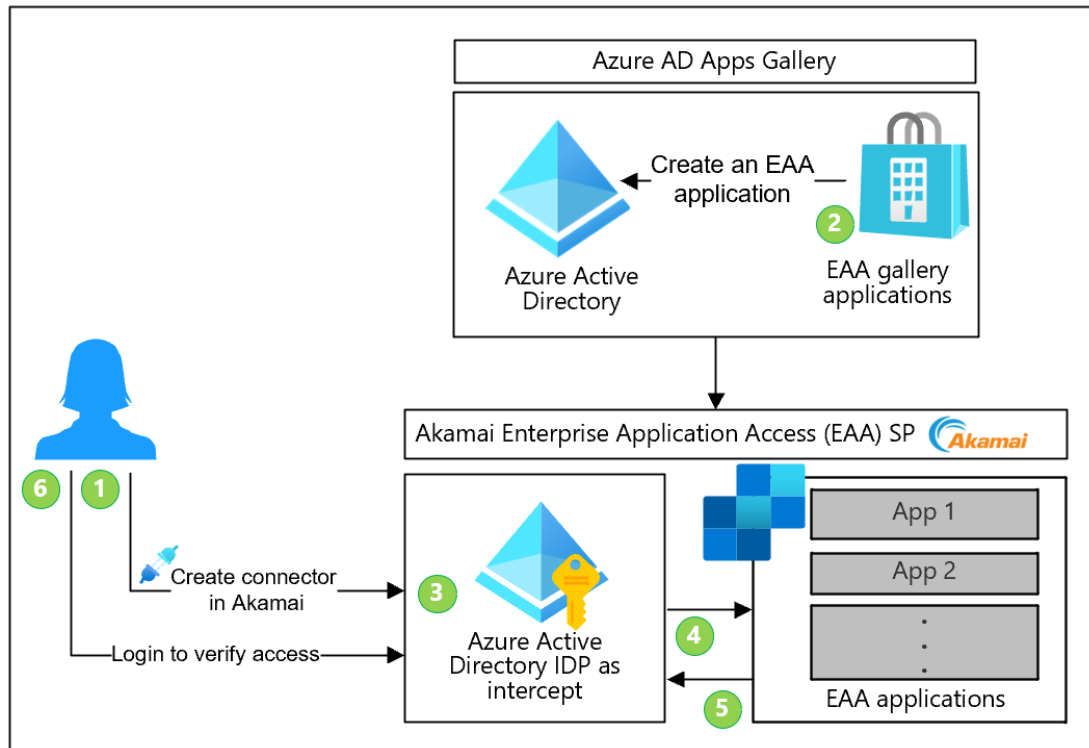
Description of workflow:

1. User sends access request for an on-premises or SaaS application to the F5 BIG-IP SAML SP.
2. F5 BIG-IP SP redirects user to Azure AD for authentication and SSO.
3. User authenticates and is granted or denied SSO.
4. The F5 BIG-IP APM queries the User ID in the on-premises directory services/domain for additional authentication/authorization.
5. User is granted access to on-premises application or SaaS apps based on Kerberos/header-based authentication.

Note: See the [Azure AD and F5 BIG-IP APM example](#) in this document on the F5 BIG-IP APM integration.

Akamai integration

The following diagram depicts the [Akamai SSO integration with Azure AD](#).



Description of workflow:

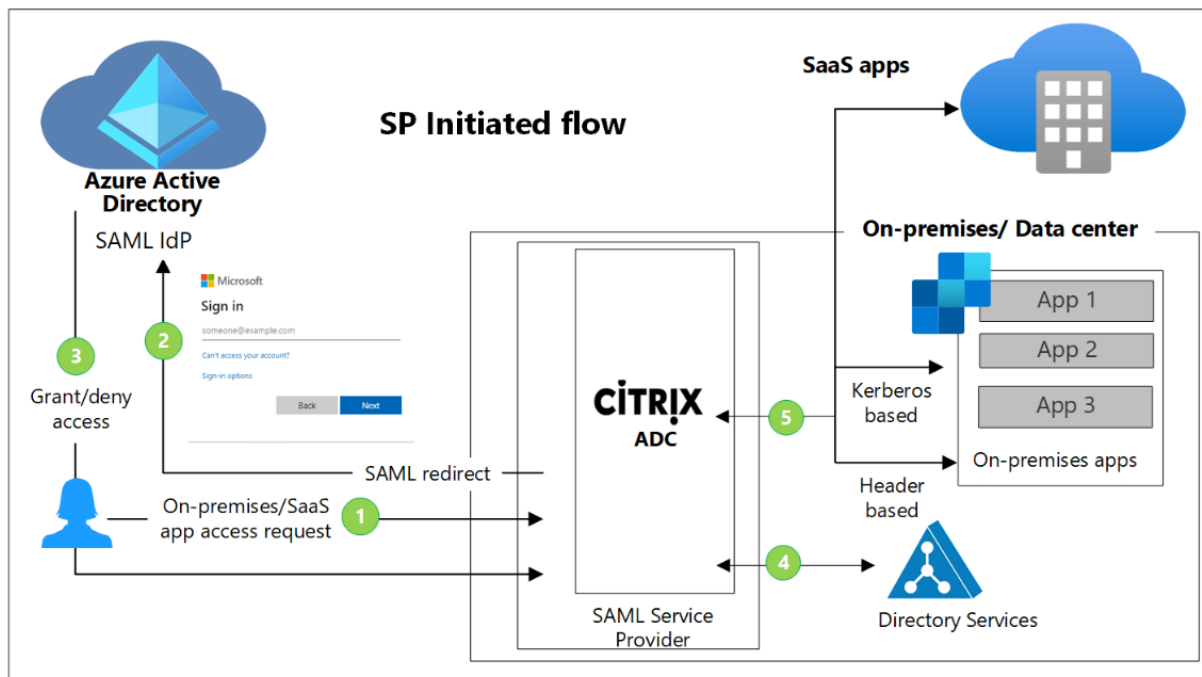
1. Create a [connector](#) in Akamai and [deploy](#) it.
2. Create an Akamai Enterprise Application Access (EAA) gallery application in Azure AD environment and [configure SSO](#).
3. Create an Azure AD IDP in Akamai EAA.
4. [Configure the authentication settings](#) for the Azure AD IDP in EAA.
5. [Assign the Azure AD IDP](#) to an application in EAA.
6. Log into <https://myapplications.microsoft.com/> and verify user access.

Citrix NetScaler integration

The Citrix NetScaler integration offers to:

- Control who has access to Citrix NetScaler using Azure AD.
- Enable users to automatically [SSO into Citrix NetScaler](#) with their Azure AD accounts.
- Manage user accounts in one central location – [the Azure portal](#).

The following diagram shows the Azure AD Citrix NetScaler traffic flow.

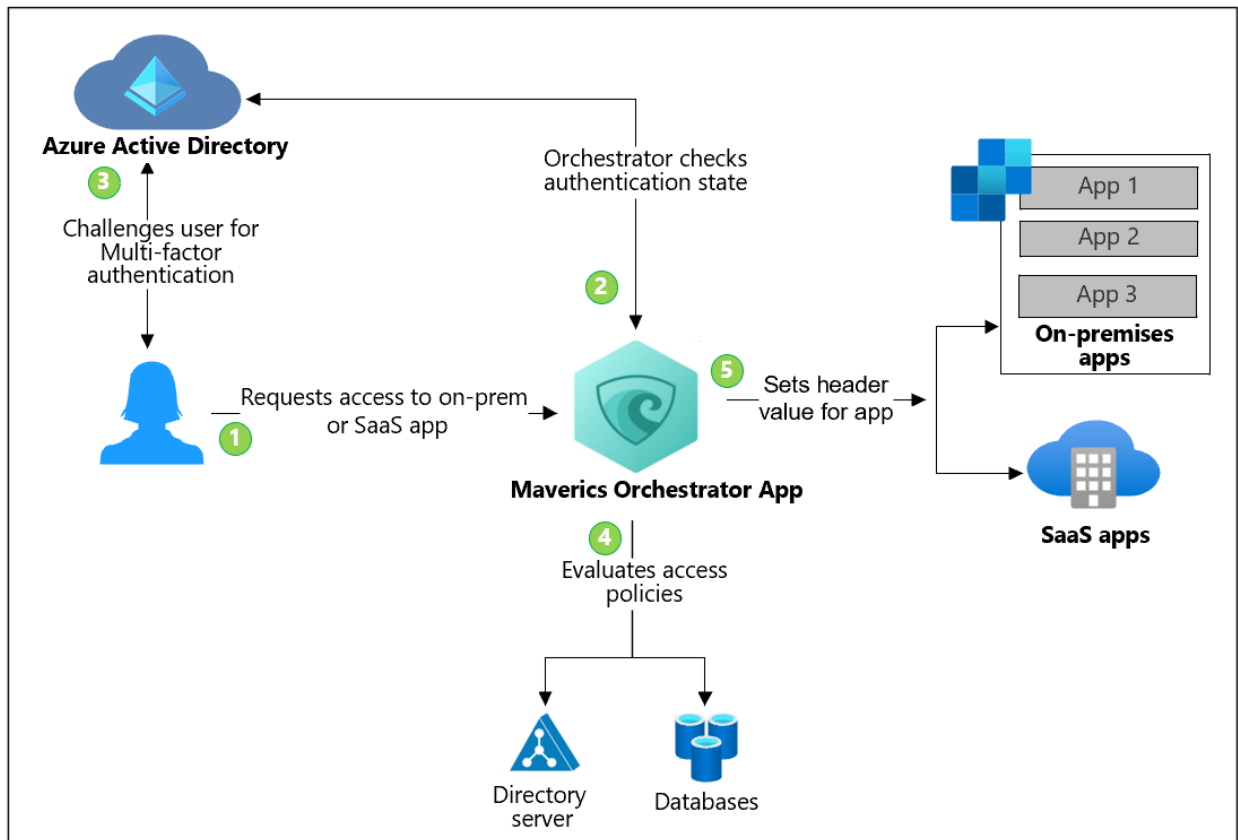


Description of workflow:

1. User sends access request for an on-premises or SaaS application to the Citrix ADC SAML SP.
2. Citrix ADC SP redirects user to Azure AD for authentication and SSO.
3. User authenticates and is granted or denied SSO.
4. The Citrix ADC queries the user ID in the on-premises directory services/domain for additional authentication/authorization.
5. User is granted access to on-premises application or SaaS apps based on Kerberos/header-based authentication.

Strata Mavericks Identity Orchestrator integration

The following diagram shows [Maverics Orchestrator integration with Azure AD](#). In this integration, Mavericks Orchestrator acts as a reverse-proxy and a gateway to the application.



Description of workflow:

1. User makes a request to access the on-premises/SaaS application. The Mavericks Identity Orchestrator intercepts the access request made by the user to the application.
2. The Orchestrator checks the user's session token. If it doesn't have a valid session token, the Orchestrator redirects the user to Azure AD for authentication and SSO.
3. Azure AD challenges the user for credentials and upon authentication, user is granted or denied SSO.
4. The Orchestrator evaluates the access policies and calculates attribute values to be included in HTTP headers sent to the application. During this step, the Orchestrator may call out to additional attribute providers such as directory server and databases to retrieve additional user information needed to set the header values correctly.
5. The Orchestrator sets the header values and sends the request to the application. The user is now authenticated and has access to the application with a valid session token.

Address governance and compliance requirements

Symantec SiteMinder is often deployed with **Symantec Identity Governance and Administration (IGA)** (previously Identity Suite/Identity Manager, Identity Governance Identity Portal, and the Virtual Appliance) to address the governance and compliance requirements.

The migration of the capabilities provided by Symantec IGA are not in scope of this document and would need to be addressed separately.

However, the Symantec SiteMinder solution does provide [auditing and reporting solutions](#) that can support a limited set of governance and compliance requirements. It is also common to integrate Symantec SiteMinder with a SIEM solution such as Splunk.

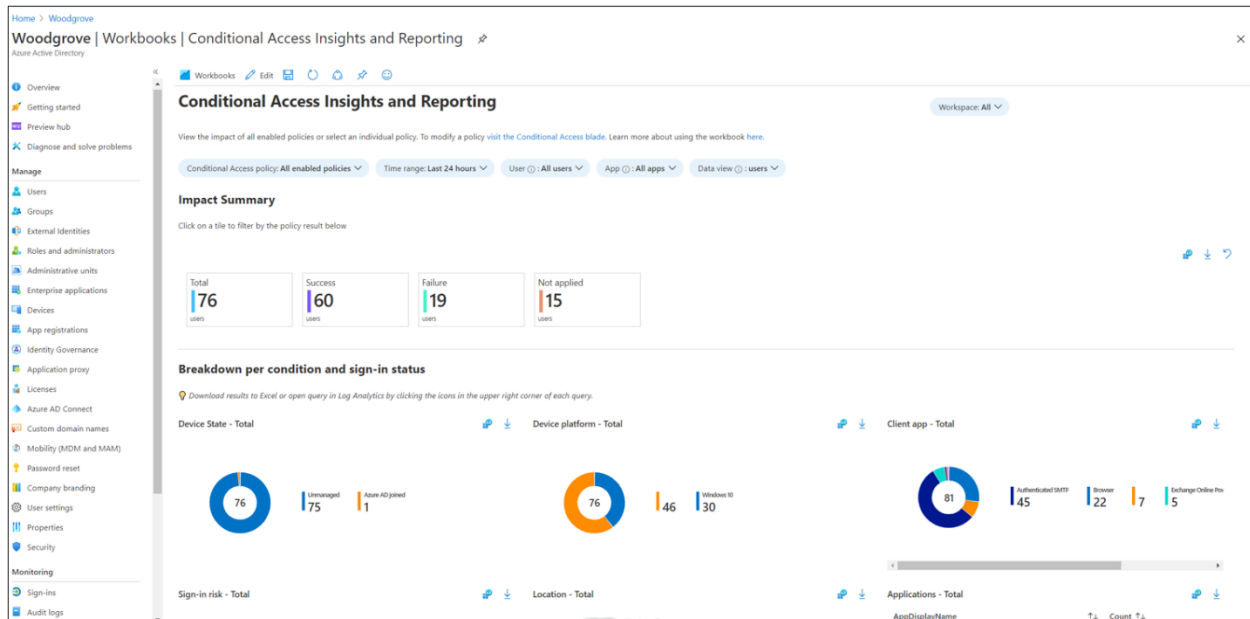
As part of the migration, you can migrate these reporting solutions to the [advanced Azure AD reporting and monitoring solutions](#).



Additionally, Azure AD offers monitoring and reporting capabilities that are not available in Symantec SiteMinder and can be integrated with the SIEM solution used in your organization.

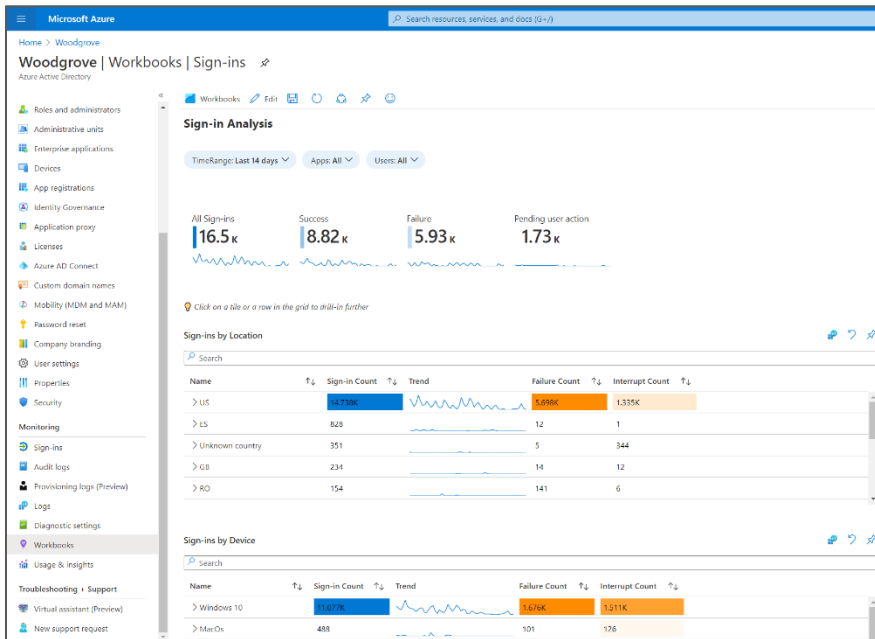
Setup access control policies

Azure AD uses [Conditional Access](#) to bring signals together, to make decisions, and enforce organizational policies. By using CA policies, you can apply the right access controls when needed to control user access to applications.



Azure AD and Symantec SiteMinder both provide mechanisms to apply access policies. A policy is an if-then statement of Assignments and Access Controls.:

- **Assignment:** Controls the conditions in a policy. A policy is enforced only when assignment conditions are met
- **Access Controls:** Controls how a policy is enforced for example, grant or block access when a policy is applied.



Map assignment conditions

The following table **maps the conditions available in Azure AD with the associated rules in Symantec SiteMinder** (if available):

Azure AD Condition	Symantec SiteMinder Rule	Notes
Specific user	Specific user	
Member of user group	Member of user group	
Member of directory role	Member of CA identity manager role	
N/A	LDAP search filter	In Azure AD, this can be implemented using Dynamic Groups where group membership is based on user attributes
Cloud App or condition	Protected resource	In Symantec SiteMinder, the URL of the protected resource is specified. Note: Addition settings can be configured on the Application Proxy or ADC in use.
User location	Not available	In Symantec SiteMinder, the IP addresses associated with the location must be specified.
IP address	IP address	Includes IP address ranges and subnets
Device Platform such as iOS and Android	Not available	

Azure AD Condition	Symantec SiteMinder Rule	Notes
Device State (only allows devices that are compliant)	Not available	
Client App such as Browser	Not available	
Sign-in risk and user risk	Must use third party risk analysis tool and specify confidence level	The Azure AD CA component provides similar risk analysis and policy enforcement capabilities to those provided by Symantec SiteMinder in combination with a third-party risk tool. The organization's sign-in and user risk requirements need to be evaluated to determine if there are requirements that cannot be met by the Azure AD CA capabilities.
N/A	Time restrictions (only allowed access during specified times of day)	This is on the roadmap for Azure AD

Map access control policies

The following table maps Azure AD policies and the equivalent policies in Symantec SiteMinder.

Azure AD Access control	Symantec SiteMinder Access control	Notes
Grant access	Grant access	For Azure AD, additional conditions may need to be met to grant access
Block access	Block access	
Grant - Require MFA (Azure MFA)	Not available	
Grant - Require device to be marked as compliant (Microsoft Intune)	Not available	
Grant - Require hybrid Azure AD joined device	Not available	
Grant - Require approved client application	Not available	
Grant - Require application protection policy	Not available	
Grant - Require password change	Not available	

Remove Symantec SiteMinder

After the migration is complete, the Symantec SiteMinder agents and policy server should be uninstalled.

To remove Symantec SiteMinder Web agents:

1. Remove the Symantec SiteMinder IIS agent using these [instructions](#).
2. Uninstall other agents, as required, based on the agent types installed in your environment.

Next, remove policy server using these [instructions](#).

Example: Symantec SiteMinder to Azure AD application migration using F5 BIG-IP APM

This section provides an example of migrating an on-premises solution from Symantec SiteMinder to Azure AD. As discussed, [earlier in this document](#), there are many options for integrating on-premises applications and the decision on which integration method to use is based on the specific application requirements. The example and the components used here are for illustration purposes only.

Migration of PeopleSoft

PeopleSoft is an enterprise human resources application used by many large businesses. To illustrate the migration of a business-critical application's SSO from Symantec SiteMinder to Azure AD, we have constructed a lab-version of the application migration which includes:

- **Oracle's PeopleSoft HRMS** – the business application
- **Symantec SiteMinder v12** – the legacy on-premises SSO product
- **Microsoft Azure AD** – the target SSO system
- **F5 BIG-IP APM v15** – facilitates Azure AD integration of on-premises apps, for example, PeopleSoft

In the legacy approach using Symantec SiteMinder, PeopleSoft is proxied by IIS and protected by Symantec SiteMinder using web agent. Peoplesoft SSO is achieved using header-based authentication. HTTP_PSUSER is the header that is expected by Symantec SiteMinder for SSO.

Application migration	Resources	Estimated time
Configure Peoplesoft	Application admin	20 mins
Configure F5	Application admin	30 mins
Configure Azure AD	Security + Identity team	30 mins
Checklist and application redirects	Application + Azure AD admin	60 mins

Step 1. Configure Peoplesoft

The following table lists the configuration of the PeopleSoft application:

Component	Description
Operating system	Linux
Version	HRMS 9.20.000
PeopleTools	8.57.07
Port	8000
Public user	PUBUSER
Webprofile	PROD
Virtual address	https://psft.icsdemo.com:443

PeopleSoft customized "PeopleCode"

This is a typical custom code that is used to configure PeopleSoft to leverage an HTTP header for user identification and would be used for both Symantec SiteMinder and Azure AD integrations.

```
Function OAMSSO_AUTHENTICATION()
    &fileLog = GetFile("access.log", "A");
    &fileLog.WriteLine(%Datetime | " Attempting SSO_AUTHENTICATION()");
    &fileLog.WriteLine(%Datetime | " HTTP_PSUSER: " |
%Request.GetHeader("HTTP_PSUSER"));
    If %PSAuthResult = True And
        &authMethod <> "LDAP" And
        &authMethod <> "WWW" And
        &authMethod <> "OSSO" And
        &authMethod <> "SSO" Then
        getWWWAuthConfig();
        If %SignonUserId = &defaultUserId Then
            &userID = %Request.GetHeader("HTTP_PSUSER");
            &fileLog.WriteLine(%Datetime | " HTTP_PSUSER" | &userID);
            If &userID <> "" Then
                If &bConfigRead = False Then
```

```
        getLDAPConfig();
    End-If;
    SetAuthenticationResult( True, Upper(&userID), "", False);
    &authMethod = "OAMSSO";
    &fileLog.WriteLine(%Datetime | " AUTH SUCCESS");
End-If;
End-If;
End-If;
&fileLog.WriteLine(" ");
&fileLog.Close();
End-Function;
```


Symantec SiteMinder configuration (for reference not used)

This section shows the Symantec SiteMinder configuration used in this example.

Symantec SiteMinder directory configuration (Policy store)

The Symantec SiteMinder Policy store configuration is shown in the following table.

Component	Description
Operating system	Windows 2012 R2 64 Bit
Java JDK	JDK 8 u 251
Java installation path	C:\Java
CA directory	12
Installation path	C:\CA\Directory
Port	20389

Symantec SiteMinder policy server configuration – Installation checklist

The Symantec SiteMinder policy server configuration is shown in the following table.

Component	Description
Operating system	Windows 2012 R2 64 Bit
Java JDK	JDK 8 u 251
Java installation path	C:\Java
Policy server	12.7
Policy store	CA Directory
Policy server installation path	C:\CA\Siteminder
Admin UI	C:\CA\Siteminder\Siteminder
Admin UI URL	https://<>:8443/iam/siteminder/adminui
Credentials	SiteMinder \ <>

Symantec SiteMinder policy details for PeopleSoft application

The PeopleSoft application policy details for PeopleSoft app are shown in the following table.

Component	Description
Agent	wsagent
Agent configuration object	iisaco
Host configuration object	DefaultHostSettings
Policy	Pspt
Domain	Access
Rules	/
Response	Custom – Static Header [HTTP_PSUSER:PS]
Target Users	AD

Symantec SiteMinder Web Agent details – IIS

The Symantec SiteMinder Web Agent details for IIS are shown in the following table.

Component	Description
WebAgent	IIS
Version	12.52 64 bits
Enable shared secret	Unchecked

Step 2. Azure AD and F5 BIG-IP APM

You can use [F5 BIG-IP APM integration](#) to act as an extension to Azure AD SSO. Create custom code (iRules) in APM to forward the necessary HTTP header(s) to the application – in this case, PeopleSoft. See [the Azure AD and F5 BIG-IP APM integration and configuration approach details](#).

Configure F5

The F5 configuration details are listed in the following table.

Component	Description
Version	BIG-IP 15.1.0 Build 0.0.31 Final
Modules	Local Traffic (LTM), APM
Configuration	Single NIC

Configure iRule

Insert custom logic into the F5 BIG-IP APM pipeline using code called iRules. Here is a sample iRule that, in this case, uses the Azure AD user identity to create a custom HTTP header suitable for PeopleSoft. In this sample, the HTTP_PSUSER header is mapped to the AZUREAD_USERNAME attribute.

The mapping is dependent on the requirements, but the attribute mapped must match the PeopleSoft UserID.

```
when RULE_INIT {
    set static::debug 0
}

when HTTP_REQUEST_SEND {
    set AZUREAD_USERNAME [ACCESS::session data get
"session.saml.last.attr.name.http://schemas.xmlsoap.org/ws/2005/05/identity/c
laims/name"]

    if { $static::debug } { log local0. "AZUREAD_USERNAME =
$AZUREAD_USERNAME" }

    if { !([HTTP::header exists "HTTP_PSUSER"]) } {
        HTTP::header insert "HTTP_PSUSER" $AZUREAD_USERNAME
    }

    set AZUREAD_DISPLAYNAME [ACCESS::session data get
"session.saml.last.attr.name.http://schemas.microsoft.com/identity/claims/dis
playname"]
```

```

    if { $static::debug } { log local0. "AZUREAD_DISPLAYNAME =
$AZUREAD_DISPLAYNAME" }

    if { !([HTTP::header exists "AZUREAD_DISPLAYNAME"]) } {

        HTTP::header insert "AZUREAD_DISPLAYNAME " $AZUREAD_DISPLAYNAME

    }

    set AZUREAD_EMAILADDRESS [ACCESS::session data get
"session.saml.last.attr.name.http://schemas.xmlsoap.org/ws/2005/05/identity/c
laims/emailaddress"]

    if { $static::debug } { log local0. "AZUREAD_EMAILADDRESS =
$AZUREAD_EMAILADDRESS" }

    if { !([HTTP::header exists "AZUREAD_EMAILADDRESS"]) } {

        HTTP::header insert "AZUREAD_EMAILADDRESS" $AZUREAD_EMAILADDRESS

    }

}

```

Step 3. Configure desired security and user access

Once the F5 is configured, you can use the familiar Azure AD Enterprise Applications blade to configure the application access and Conditional Access. With few simple configurations, the applications can be protected with risks arising due to login or user risk.

Step 4. Symantec SiteMinder to Azure AD application checklist

The following checklist will guide you through the migration process of applications from Symantec SiteMinder to Azure AD

Steps	Description	Comment	
1.	Gather the application information, its architecture, and the authentication methods <ul style="list-style-type: none">• What is the application server information (IP address, port)?• What is the webserver information (IP address, port)? (This is needed only if you must pass the requests through webserver)• What is the header information to be passed?• What other policies needed?		<input type="checkbox"/>
2.	Validate the current application integration is working with Symantec SiteMinder		<input type="checkbox"/>
3.	Integrate the application with the F5 BIG-IP APM using these instructions .		<input type="checkbox"/>
4.	Test and validate the integration making changes to hosts file using the same front-end URL		<input type="checkbox"/>
5.	Production go-live: Switch the DNS entry for the application to point to the F5 virtual server		<input type="checkbox"/>
6.	Validate the production environment and release to the end users		<input type="checkbox"/>

Frequently asked questions

Does the migration to Azure AD impact end-users and their experience?

There is a minimum impact for end-users during the migration from Symantec SiteMinder to Azure AD. Users will sign into Azure AD instead of Symantec SiteMinder. The sign in experience that Azure AD offers is more modern and optimized for a mobile experience which improves the overall [end-user adoption](#). With the Azure AD you are all set to prepare your users for the new experience.

How do I configure Azure AD for non-production environments?

You can setup an Azure AD tenant for testing in non-production environments. This tenant will have all the capabilities of the production tenant but will use test data and configurations to isolate the testing from the Azure AD tenant and integrated applications in production.

Can you integrate Azure AD with well know ERP and COTS systems like Peoplesoft or Oracle?

When you combine Azure AD with the integration options described in this document, you get support for multiple ERPs/COTS, including SAP NetWeaver, Oracle eBusiness Suite, Peoplesoft, JD Edwards and more. See [example of integrating with Peoplesoft using Azure AD and the F5 BIG-IP APM](#).

How does Azure AD replace Symantec SiteMinder integrations that are not browser based such as the Symantec SiteMinder C and Java SDKs?

Migrating these apps require changes in their source code regardless of which new identity solution you adopt. We recommend that applications with proprietary Symantec SiteMinder SDKs can replace the SDK with open-standard integrations using [Microsoft authentication libraries](#) (MSAL).

Appendix A: Modernize applications

Transition your applications to use modern authentication protocols.

Reverse proxies

Reverse proxies (such as Azure AD Application Proxy or F5 appliances) offer drop-in authentication support for applications without native support. This may be a valid choice for applications for which source code is unavailable or the framework/language lacks native libraries for modern authentication protocols. This proves one of the least-disruptive changes, as the application code itself does not need to change at all. Conversely, the network paths to those applications need to be locked down to only send and receive traffic via the reverse proxy. Reverse proxies have other disadvantages – the proxy itself needs to be sized and scoped appropriately depending on the expected application traffic, including considerations like load balancing and ongoing maintenance.

Azure-specific support

An alternative path may include migrating to Azure. Azure includes certain platform products where authentication is handled at the ‘front door’ via the host or product, instead of requiring the application code to be changed. An example of this is [Azure app service authentication/authorization](#), colloquially known as **EasyAuth**. This is a Platform-as-a-Service (PaaS) and offers to host web applications in a reliable and managed environment. It supports myriad of platforms, tools, frameworks, and languages.

The EasyAuth [configuration for Azure AD](#) either creates and configures a new application registration automatically or uses the existing pre-configured Azure AD application registration. Once configured, unauthenticated requests are handled by App Service, redirecting the user to the configured IDP which captures and validates the returned token, and allows the application access to the user.

EasyAuth works well with [Azure AD app assignment](#). By requiring user assignment to applications, only users assigned (or within assigned groups) can receive a token for that application at the IDP level – for example, Azure AD will not issue a token unless the application is assigned to a user.

Once the user is signed in with EasyAuth, the user’s ID_token and captured claims are available to the application via incoming request headers or via an [App Service-local endpoint](#).

Beyond just web applications, web APIs can also take advantage of EasyAuth. Once configured, EasyAuth validates the incoming API requests using Bearer tokens before they are sent to the web API.

Use authentication and authorization libraries

For legacy apps that you want to modernize, we recommend updating the authentication stack code for these applications from the legacy protocol to a modern protocol like [OpenIDConnect](#). The complexity of this modernization also depends on the current Symantec SiteMinder integration used (proxy/agent).

Azure AD provides an SDK [Microsoft Authentication Library \(MSAL\)](#) that takes care of the implementation of OpenIDConnect protocol.

Appendix B: Coexistence strategy

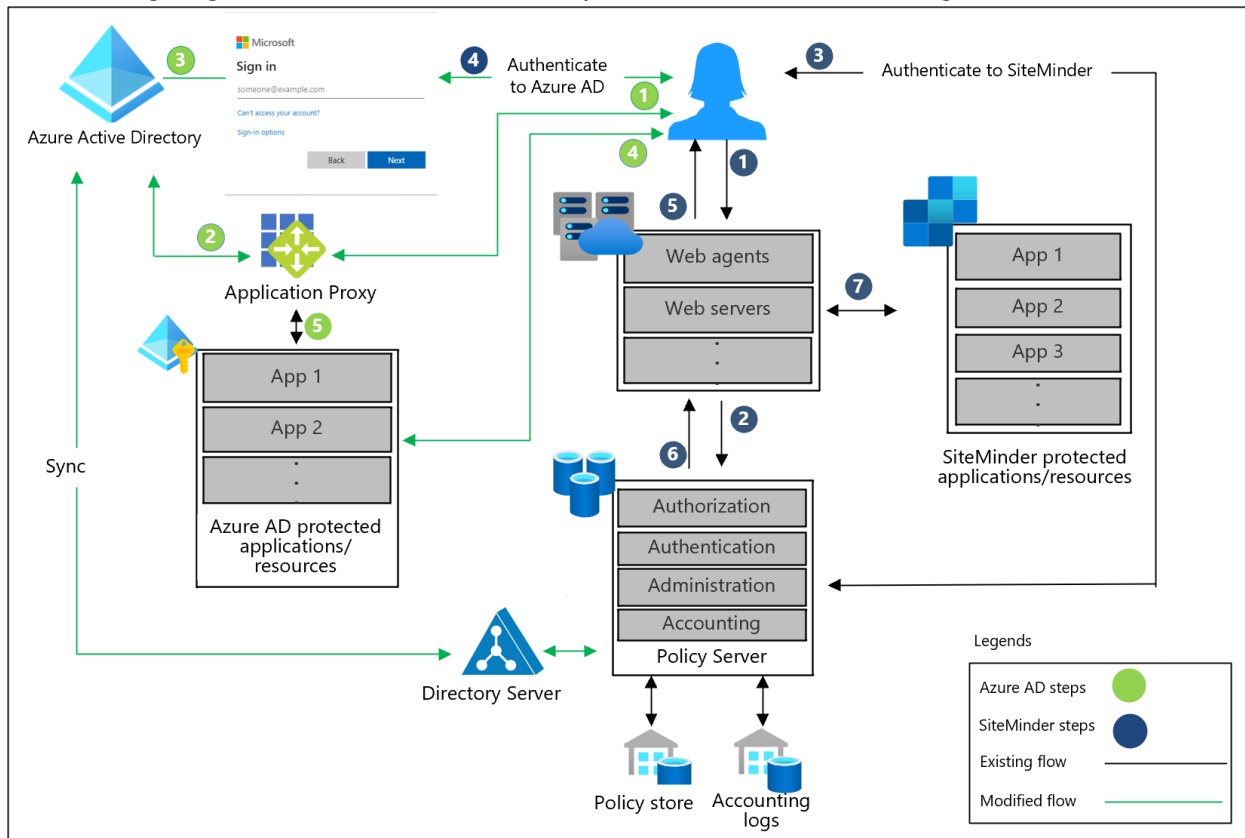
As an optional setup, you can integrate Azure AD and Symantec SiteMinder as per application release schedules and other organizational constraints by providing coexistence of the two solutions.

The integration involves configuring Azure AD as the IDP and Symantec SiteMinder as a Service Provider (SP). This allows applications that are already integrated with Symantec SiteMinder to remain unchanged until they are ready to be migrated to Azure AD. The only difference from a user standpoint is that the login will be through Azure AD rather than Symantec SiteMinder. If all applications are to be migrated at once, then this integration is not required. For all but very small organizations, it is recommended to [integrate Azure AD and Symantec SiteMinder](#) for coexistence during the migration process.

Transitional architecture – some applications migrated

In the transition or coexistence phase, the applications can be moved following an agreed upon roadmap. The following diagram shows an example of the architecture with a few applications moved to Azure AD for SSO. In this phase, users accessing Symantec SiteMinder protected applications will be redirected to Azure AD for authentication. The Symantec SiteMinder authentication has been integrated with Azure AD as a SAML Service Provider (federation) and will not present a Login page. By federating Symantec SiteMinder with Azure AD end-users still have SSO between Symantec SiteMinder protected applications and Azure AD protected applications. This allows for a smoother transition of the applications from Symantec SiteMinder to Azure AD.

The following diagram shows the Azure AD and Symantec SiteMinder co-existing architecture.



Description of workflow for applications that migrate to Azure AD (in green):

1. The user requests access to an application protected by Azure AD
2. Azure AD checks for an existing session
3. If no session exists, the end-user is asked to authenticate
4. If the credentials are valid, the end-user is redirected to the application
5. The Azure AD Application proxy serves the content to the end-user through a secure channel

Description of workflow for applications that are yet not migrated to Azure AD (in blue):

1. The user requests to access an application protected by Symantec SiteMinder
2. The Symantec SiteMinder web agent or reverse proxy checks for a session
3. If no sessions exist, the end-user is asked to authenticate
4. Azure AD validates the end-user credentials as Symantec SiteMinder is federated with Azure AD
5. The web agent or reverse proxy protecting the application checks the authorization with Symantec SiteMinder
6. The web agent or reverse proxy sends the HTTP headers to the application to be consumed by the application
7. Symantec SiteMinder serves the content to the end-user through a secure channel