<table>
<thead>
<tr>
<th>Page</th>
<th>Section</th>
</tr>
</thead>
<tbody>
<tr>
<td>03</td>
<td>INTRODUCTION</td>
</tr>
<tr>
<td>04</td>
<td>OVERVIEW OF THE FOUR MIGRATION PHASES</td>
</tr>
<tr>
<td>06</td>
<td>PLANNING PHASE</td>
</tr>
<tr>
<td>10</td>
<td>INITIAL DEPLOYMENT AND CA SINGLE SIGN-ON INTEGRATION PHASE</td>
</tr>
<tr>
<td>13</td>
<td>APPLICATION MIGRATION PHASE</td>
</tr>
<tr>
<td>14</td>
<td>FINALIZE MIGRATION PHASE</td>
</tr>
<tr>
<td>15</td>
<td>APPENDIX A: CA SINGLE SIGN-ON APPLICATION CLASSIFICATIONS</td>
</tr>
<tr>
<td>16</td>
<td>APPENDIX B: AUTHENTICATION FLOW PROCESS OPTIONS</td>
</tr>
<tr>
<td>19</td>
<td>APPENDIX C: SAMPLE CA SINGLE SIGN-ON PROTECTED APPLICATION MIGRATION SCENARIO</td>
</tr>
</tbody>
</table>
INTRODUCTION

Web access management (WAM) systems have been a part of enterprises for decades. It's critical to control access and audit applications while reducing the friction for users to interact with applications.

As business has shifted and changed in the Internet era, identity and access management systems have to change and grow to support new use cases. Traditional IAM vendors have been challenged to respond in a timely manner to these changing business requirements. Ping Identity® offers the solution with Identity Defined Security to extend and replace traditional IAM vendor products.

Ping's products are designed to provide a simple migration strategy from traditional IAM solutions. PingFederate® and PingAccess® integrate with CA SiteMinder® (now called CA Single Sign-On) to facilitate the transfer of applications without disrupting your end users. The transition from one system to Ping can happen on a timeline that supports your business.

A typical migration to the Ping Identity Platform involves the four phases discussed below. We recommend contacting one of our Platinum Service Partners to assist and guide your organization through the migration process. Information regarding a Platinum Service Partner can be found at https://www.pingidentity.com/en/partner-network.html.
OVERVIEW OF THE FOUR MIGRATION PHASES

Planning Phase
During the planning phase, your existing WAM deployment and architecture is surveyed and understood. You’ll take inventory of your applications, policies, authentication levels and methods, asking questions such as:

- What access control policies are necessary?
- What types of application integration are necessary?
- Where will authentication happen?
- What are your password management and recovery requirements?

After taking a full inventory, you’ll create a plan for your new architecture and deployment model, rationalize session management and settings, and plan the order of your application migration.

During this time, the order of application migration should be determined. You should start by identifying a pilot application to test and validate the migration plan. The pilot application is taken through the migration phases to ensure that the process is understood and to gain confidence in the Ping Identity Platform.

After the pilot application is successfully migrated, the remaining planned applications can gradually be migrated.

Initial Deployment Phase
Initial deployment starts with the installation and configuration of PingFederate and PingAccess in order to start integrating them with your existing identity management systems.

During this phase, PingFederate is integrated into the existing authentication flows. The authentication flows can support internal users stored in local directories or by delegating authentication to an existing IAM system. Additionally, the authentication flows can support federated identities from other organizations.

Both PingFederate and PingAccess should be integrated into the existing monitoring, auditing and reporting tools available in the enterprise.

Application Migration Phase
Application migration typically starts with the migration of a low-risk application from the existing identity management system into the Ping Identity Platform.

CA Single Sign-On objects and access control policies required to protect the application are first migrated. The next step is to integrate PingAccess with the application. This integration can happen through identity mappings or site authenticators in the PingAccess gateway or with the PingAccess agent deployed on a web server.
PingAccess also supports more complex migration scenarios. With PingAccess, it's possible to migrate an application with an existing CA Single Sign-On agent in place without removing the agent. PingAccess can acquire the appropriate token that the application is expecting. When the agent is removed, a simple configuration change is all that's necessary for PingAccess to continue protecting the application.

Scenarios like this are supported to reduce the difficulties of migrating applications when the department deploying PingAccess doesn't directly own the applications.

You'll repeat the migration process for the remainder of the applications targeted for migration into PingAccess. The application migration phase is completed when all applications have been migrated from the existing identity management system into Ping Identity Platform.

Finalize Migration Phase
The final step in the migration is to remove the last dependencies on your existing WAM system. Typically, this means shifting the authentication responsibilities from the system into PingFederate so that PingFederate becomes the authoritative source for authentication and takes over password management responsibilities. When all WAM dependencies are removed, the CA Single Sign-On servers can be decommissioned and recycled.
Understanding Your Architecture

The first step in planning your migration from CA Single Sign-On is to survey your deployment and understand the different WAM pieces in play. A standard WAM deployment is shown in Figure 1.

![Figure 1: A typical CA Single Sign-On WAM deployment](image-url)
Typically, a CA Single Sign-On deployment uses web agents installed on web servers that sit adjacent to each application. As you plan for the migration, it's a good time to evaluate your deployment architecture and the lessons learned from maintaining agents. The total cost of ownership related to an agent-based deployment is typically very high.

Deploying a gateway-based architecture can save deployment time as well as reduce the total cost of ownership. PingAccess can be deployed quickly, and the gateway can easily be integrated into existing applications and network traffic can be re-routed to it. A system fully migrated to PingAccess using a gateway deployment is shown in Figure 2.

Figure 2: System migrated to PingAccess
If the PingAccess gateway architecture is not feasible, the migration can still be performed with PingAccess agents following the same deployment architecture as the typical CA Single Sign-On installation. A system fully migrated to PingAccess using agents is shown in Figure 3.

PingAccess also supports both architectures simultaneously. Some applications can continue with the agent-based architecture while the rest of the applications are protected by the PingAccess gateway. This approach can also be used as an intermediary as the deployment architecture is shifted from agents to gateways.

**Application and Policy Inventory**

After understanding and planning the deployment architecture, you’ll take inventory of the applications to be migrated. You’ll also evaluate each application to understand the dependencies on CA Single Sign-On. A framework for application classification can be found in Appendix A.

For each application, you should catalog the realms, rules and rule groups to be migrated into PingAccess applications, resources, rules and rule sets.

Next, you’ll take inventory and prepare the CA Single Sign-On policies for migration. You’ll then catalog each policy and identify the protected resources, the rules and access control lists (ACLs) used and the authentication requirements used to identify users.
Authentication and Session Management
To begin this step, you’ll evaluate and ensure you understand the authentication processes in the environment while planning the migration. If CA Single Sign-On is used to authenticate users, you must decide when to migrate authentication away from those systems. There are two recommended methods to migrate authentication from CA Single Sign-On. All authentication flows are explained in Appendix B.

The first method migrates authentication from CA Single Sign-On at the beginning of the migration process. Migrating authentication at the beginning of the process makes PingFederate the source of record for authentication and identity. If this method is selected, PingFederate can be integrated with CA Single Sign-On to provide applications with those still expecting them.

The second method migrates authentication from CA Single Sign-On at the end of the migration process. Authentication will continue to occur with CA Single Sign-On even if users are accessing PingAccess protected application. PingFederate can be configured and integrated with CA Single Sign-On to trust and accept tokens issued by that system. When it’s time to decommission CA Single Sign-On, the authentication process is migrated to PingFederate.

Next, you’ll evaluate the session management process. When working with two concurrent WAM systems, it’s important to understand how the sessions integrate. Without evaluating and integrating the sessions between the systems, end users may be unnecessarily prompted to authenticate to the system.

Project Planning
After classifying the applications, cataloging the policies and understanding the authentication and session management processes, you should create a project plan to acquire the resources to install PingFederate and PingAccess, perform integration with CA Single Sign-On and migrate the applications.

Based on the application classifications, we recommend the following migration order:

1. Start with a simple application as a proof-of-concept (PoC) to understand the migration process and remove risk further in the process.

2. Migrate low complexity applications (i.e., ones with no CA Single Sign-On customizations, or those using custom CA Single Sign-On APIs) into PingAccess.

3. Migrate the remaining medium/high complexity applications. Customizations and complex authentication schemes should be migrated and configured as well.
INITIAL DEPLOYMENT AND CA SINGLE SIGN-ON INTEGRATION PHASE

PingFederate Installation
To install PingFederate, find the document here.

PingAccess Installation
To install PingAccess, find the documentation here.

PingAccess Integration with PingFederate
Connect PingAccess to PingFederate for authentication by following the documentation located here.

CA Single Sign-On Integration
CA Single Sign-On integration leverages the authentication and session management features in both environments. There are two approaches to this, and depending on your deployment needs, one or both might be used at different stages of the migration. Read about the two approaches on the following pages.
**Option 1: Leverage CA Single Sign-On Sign On**

In its existing deployment, CA Single Sign-On is likely the entry point for users in the system, dictating how authentication is performed and creating sessions once successful. The PingFederate and PingAccess infrastructure can leverage this authentication point by using the PingFederate WAM Integration Kit. This approach is a good way to try some of the PingAccess access control and session management capabilities without impacting the majority of applications or network infrastructure.

Consult the [PingFederate WAM Integration Kit documentation](#) for detailed steps on how to deploy it.

Once the PingFederate WAM Integration Kit is deployed, CA Single Sign-On sessions are created or updated when accessing applications protected by PingAccess. From that point on, if the user accesses applications using only a PingAccess session, there's a risk of the CA Single Sign-On session timing out. To prevent this behavior and effectively centralize the sessions, employ a 'session keep alive' rule or site authenticator to ensure that the CA Single Sign-On session is periodically 'refreshed' by calling a test resource on the user's behalf. Any updates to this session (i.e., new cookie values returned in a SetCookie HTTP response header) should be relayed back to the browser.

A summary system architecture diagram of this WAM migration phase is depicted below:
**Option 2: Token Mediation**

An alternative to leveraging sign-on interfaces in CA Single Sign-On is to migrate those to PingFederate as the sole entry point into the system. PingFederate provides a full-featured username/password sign-on mechanism, known as the HTML Form Adapter, and it easily connects to existing directory servers. This may be supplemented with other sign-on mechanisms such as Integrated Windows Authentication (IWA) and strong authentication (i.e., PingID, X.509 certificates, third-party OTP tokens, etc.).

When a mix of PingAccess and CA Single Sign-On protected applications exist in the environment, token mediation can be used to ensure a seamless end user SSO and session management experience. In this configuration, the PingAccess gateway exchanges its own web session cookie (known as the PA token) for the target CA Single Sign-On session, which is presented to a back-end web server on which an agent is still deployed. This may be most convenient in a phased migration when a majority of the applications are protected by PingAccess, but pockets of applications still exist that have third-party agents installed on their supporting web server that are difficult to remove.

Details of a typical token mediation are presented in the PingAccess documentation.

The token mediator site authenticator provides this capability in PingAccess and depends on the PingFederate STS with appropriate token generators installed, such as the WAM token translator. View the documentation here.

A summary system architecture diagram of this WAM migration phase is depicted below:
The first step in migrating an application from CA Single Sign-On to PingAccess is to ensure that the required integrations are complete and that PingAccess can provide the necessary identity information to the application. The next step is to create the PingAccess rules that enforce access in the same way that CA Single Sign-On enforces access. More information about defining rules can be found here.

The final step is to select the architecturally appropriate deployment option. Appendix C highlights a sample migration scenario from an agent-based architecture into either a gateway-based or proxy architecture.

Migrating Application Protection to the PingAccess Gateway
The first step is to determine if the application will continue to require the CA Single Sign-On SMSESSION session token. If it's still required (for example, if the CA Single Sign-On agent will remain on the target web server), you configure token mediation so that PingAccess will acquire a target token on behalf of the user.

Next, you configure the application in PingAccess, defining where the protected web server resides, how it’ll be exposed via the gateway, what the required web session management controls are, and how end user identity details will be passed down to the application if needed (i.e., HTTP headers using identity mappings).

Then you define your access policies using rules that are equivalent to (or a simplification of) those employed in CA Single Sign-On.

Last, you configure network routing to start sending request traffic to PingAccess instead of the application.

Migrating Application Protection to a PingAccess Agent
In scenarios where an agent model is still preferred, the PingAccess agent replaces the existing CA Single Sign-On agent.

You should start by defining the application details in PingAccess, including virtual host and path information, web session management controls and how end user identity details will be passed down to the application, if required (i.e., HTTP headers using identity mappings). The agent bootstrap configuration must be defined in PingAccess, and produces a configuration file the agent plugin will read on the target system.

Next, you define your access policies using rules that are equivalent to (or a simplification of) those employed in CA Single Sign-On.

Once configured, you uninstall the CA Single Sign-On agent on the target web server and install the PingAccess agent.

Documentation for the agents can be found here.

Deploying New Applications
Any new applications protected by the solution should be deployed behind PingAccess. They immediately benefit from the lighter weight integration and combined web and API access management features that PingAccess provides. While a gateway-based implementation is recommended to simplify ongoing maintenance, agents can be installed where required in order to accommodate existing deployment models.
FINALIZE MIGRATION PHASE

Authentication Migration
The final phase of the migration is to remove any remaining CA Single Sign-On dependencies. If authentication responsibilities haven’t been transferred to PingFederate, finalize those changes first.

Move the authentication policies and methods to PingFederate in order to provide the same security, experience and functionality that existed with CA Single Sign-On.

Application Migration
As applications are migrated to PingAccess for protection, CA Single Sign-On agents could still be left in place. It’s critical to work with the application owners to remove those agents before CA Single Sign-On is decommissioned. As agents are removed from applications, configuration should be updated in PingAccess to provide the applications the necessary information.

When the final application requiring CA Single Sign-On SMSESSION tokens is migrated to PingAccess, you remove the token mediation configuration.

Final Migration Steps
The last steps are to remove any mechanisms for synchronizing sessions between CA Single Sign-On. Finally, CA Single Sign-On can be shut down and the servers can be recycled.

The migration to PingFederate and PingAccess is now complete. If you encounter problems or challenges, please contact support@pingidentity.com.
APPENDIX A: CA SINGLE SIGN-ON APPLICATION CLASSIFICATIONS

Low Complexity Applications
Low complexity applications are protected by standard web/application agents and have the following characteristics:

- LDAP or Active Directory is typically used for authentication
- Form basic and certificate-based authentication schemes
- Simple realms, rules and policies with no custom authentication schemes/active expressions (such applications are easily migrated to PingAccess without any customizations)

Medium Complexity Applications
Medium complexity applications rely on minor CA Single Sign-On customization and have the following characteristics:

- Minimal CA Single Sign-On customizations, such as custom authentication schemes
- CA Single Sign-On authorization APIs called to perform authorization checks or using CA Single Sign-On APIs for responses (headers/cookies)

Custom code developed using the CA Single Sign-On SDK will need to be evaluated to determine if similar functionality is supported by PingAccess out-of-box functionality or can be developed using the PingAccess SDK.

High Complexity Applications
High complexity applications are similar to the medium complexity applications, but have more customization or specific integration requirements. High complexity applications have the following characteristics:

- More complex forms of authentication schemes like two-factor authentication, IWA, and impersonation
- Integration with applications like PeopleSoft, SAP, WebLogic, WebSphere, etc.

Custom code developed using CA Single Sign-On SDK will have to be evaluated to determine if similar functionality is supported by PingAccess out-of-box functionality or can be developed using the SDK. While PingAccess provides a number of out-of-box connectors/adapters for various other tools that require SSO integration, the migration may require some additional planning.
CA Single Sign-On as the Authenticator

When CA Single Sign-On is used for user authentication, there are two request flows to understand. The first flow focuses on the user accessing an application protected by CA Single Sign-On before accessing an application protected by PingAccess. The second flow focuses on the user accessing an application protected by PingAccess and then accessing an application protected by CA Single Sign-On.

Scenario 1: User Accesses an Application Protected by CA Single Sign-On and Then an Application Protected by PingAccess

The user initiates a web session by accessing a CA Single Sign-On protected application and then clicks on a URL protected by PingAccess. The following diagram shows the request flow:

Request Flow:
1. The user clicks a URL protected by CA Single Sign-On.
2. The agent intercepts the request and collects the credentials and authenticates the user with the policy server.
3. The user is then redirected to the protected web page. The agent creates an SMSESSION cookie for the user.
4. The user now clicks a URL protected by PingAccess.
5. PingAccess redirects to PingFederate for authentication.
6. Integration with PingFederate (i.e., WAM Integration Kit integrated with CA Single Sign-On) decodes the SMSESSION cookie and then validates the session with the policy server.
7. Upon successful validation, PingFederate performs an OpenID Connect based sign-on to PingAccess.
8. PingAccess validates the OpenID Connect sign-on and generates a PingAccess web session cookie (PA Token) during a redirection to the requested resource. All rules associated with the resource are evaluated for authorization, and if successful, the resource content is returned to the client.
Scenario 2: User Accesses an Application Protected by PingAccess and then an Application Protected by CA Single Sign-On

The user initiates the session by accessing a PingAccess protected application and then clicks on a URL protected by CA Single Sign-On. The following diagram depicts the request flow:

Request Flow:

1. The user accesses a URL protected by PingAccess.
2. PingAccess redirects to PingFederate for authentication.
3. Integration with PingFederate (i.e., WAM Integration Kit integrated with CA Single Sign-On) checks if there's an existing SMSESSION cookie, and if there's not, it redirects the user to a URL protected by CA Single Sign-On for authentication.
4. The agent intercepts the URL and shows the sign-on page. The user enters credentials and is authenticated by the policy server. CA Single Sign-On then creates an SMSESSION cookie.
5. PingFederate integration with CA Single Sign-On decodes the SMSESSION cookie and completes an OpenID Connect based sign-on to PingAccess.
6. PingAccess validates the OpenID Connect sign-on and generates a PingAccess web session cookie (PA token) and evaluates all the rules associated with the resource for authorization.
7. The user now clicks a URL protected by CA Single Sign-On.
8. The agent intercepts and validates the SMSESSION cookie with policy server.
9. If the SMSESSION cookie is still valid and the user is authorized, the application content returned to the browser.

PingFederate as an authenticator

When PingFederate is used for authenticating users, the requirement is that users must interact with an application protected by PingAccess first. The request flow below shows that the authentication event places both the PingAccess JSON web token (JWT) and the CA Single Sign-On SMSESSION token as cookies in the browser. After authentication, the user can access either a PingAccess protected application or a CA Single Sign-On protected application.
Scenario 3: User Accesses an Application Protected by PingAccess and then an Application Protected by CA Single Sign-On

The following steps describe how SSO is achieved between PingAccess and CA Single Sign-On when a user accesses a resource protected by PingAccess and authenticated by PingFederate.

Request Flow:

1. The user accesses a URL protected by PingAccess.
2. PingAccess redirects to PingFederate for authentication. The HTML Form Adapter (or other configured sign-on mechanism) presents the sign-on page. The user enters credentials and is authenticated.
3. PingFederate completes an OpenID Connect based sign-on to PingAccess and is redirected to protected resource.
4. The user now clicks a URL to a resource hosted on a web server with a CA Single Sign-On agent installed that is behind a PingAccess gateway.
5. The PingAccess gateway takes the PingAccess web session cookie (PA token) and sends it in a WSTrust STS request to PingFederate to request a CA Single Sign-On token (the SMSESSION cookie).
6. The PingAccess gateway puts the SMSESSION cookie in the HTTP request and then proxies it to the CA Single Sign-On protected resource.
7. The CA Single Sign-On agent checks the session with the policy server. Upon successful authentication and authorization, the web agent allows access to the resource.
8. The web server returns the resource to the browser.
APPENDIX C: SAMPLE CA SINGLE SIGN-ON PROTECTED APPLICATION MIGRATION SCENARIO

The following scenario covers how typical CA Single Sign-On protected applications are migrated to PingAccess.

Following are lists of typical CA Single Sign-On objects that have been configured in order to protect an application. These objects will need to be migrated into PingAccess to provide the same level of functionality that CA Single Sign-On provides.

1. Agent
2. Agent configuration object with the following parameters
   a. Cookiedomain
   b. Cookieprovider
   c. IgnoreURL
   d. IgnoreExt
   e. LogFile
   f. AgentName
3. Host configuration object
   a. Policy Server IP
4. Form based authentication scheme
5. Active Directory as user store
6. Application domain which would include the following:
   a. Realms
   b. Access rules
   c. Responses
   d. Policies
The following table shows the list of CA Single Sign-On objects and the corresponding PingAccess and PingFederate objects:

<table>
<thead>
<tr>
<th>CA Single Sign-on</th>
<th>PingAccess</th>
<th>PingFederate</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agent</td>
<td>Agent/Sites</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Agent configuration object</td>
<td>Web Session</td>
<td></td>
<td>Not all settings are supported/required in PingAccess</td>
</tr>
<tr>
<td>Host configuration object</td>
<td>PingFederate server details</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Authentication requirements</td>
<td></td>
<td>Adapters, connections</td>
<td></td>
</tr>
<tr>
<td>User directories</td>
<td></td>
<td>Data stores, password credential validators</td>
<td>PingFederate supports the underlying directory server password policy and can enforce reset passwords for expired password accounts and detect locked accounts. These features are supported by the PingFederate HTML Form Adapter.</td>
</tr>
<tr>
<td>Password policies</td>
<td>n/a</td>
<td>n/a</td>
<td></td>
</tr>
<tr>
<td>Domains</td>
<td>Applications</td>
<td></td>
<td>All protected sites are independent in PingAccess</td>
</tr>
<tr>
<td>Realms, sub-realms</td>
<td>Resources</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Rules</td>
<td>Rules, rule sets</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Responses</td>
<td>Identity mapping</td>
<td>OpenID Connect policies</td>
<td></td>
</tr>
<tr>
<td>Policies</td>
<td>Rules</td>
<td>Issuance criteria in access token and OpenID Connect policies</td>
<td></td>
</tr>
</tbody>
</table>

The section below describes how to migrate a simple CA Single Sign-On application to PingAccess and PingFederate. Here are the application details:

1. Application hosted on IIS application is protected by the CA Single Sign-On IIS web agent
2. Authentication scheme used is form-based authentication
3. LDAP user store for authenticating users
4. Domain HR Portal uses LDAP user store and contains the following objects
   a. Realm configured to protect /hrportal/*
   b. Rule configured GET, POST allow rule
   c. Responses configured to return headers for FIRSTNAME, LASTNAME
   d. Policy configured to allow users belonging to CN=Employees group access to the portal
The following table summarizes the CA Single Sign-On objects and corresponding PingAccess and PingFederate objects that are to be created:

<table>
<thead>
<tr>
<th>CA Single Sign-on</th>
<th>PingAccess</th>
<th>PingFederate</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agent</td>
<td>Agent</td>
<td></td>
</tr>
<tr>
<td>User store</td>
<td></td>
<td>Data store of type LDAP, password credentials validator</td>
</tr>
<tr>
<td>Authentication schemes</td>
<td>Authentication requirements</td>
<td>HTML forms adapter, selectors</td>
</tr>
<tr>
<td>Domain</td>
<td>Application, web session</td>
<td>OAuth Client</td>
</tr>
<tr>
<td>Realms</td>
<td>Resources</td>
<td></td>
</tr>
<tr>
<td>Rules</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>Responses</td>
<td>Identity mapping</td>
<td>OpenID Connect policies</td>
</tr>
<tr>
<td>Policies</td>
<td>Rules, rule sets</td>
<td></td>
</tr>
</tbody>
</table>