covisint®
Enabling information ecosystems.

appcloud™

Single Sign-On (SSO) and Application Provisioning Integration Guide

April 24, 2013

Table of Contents

About AppCloud™

AppCloud™ provides Application Providers with a single point of integration and management, utilizing self-service features, which allows an Application Provider to make their application or applications available to specific targeted communities. AppCloud also provides Application Providers with standard integration interfaces that can be utilized to support various types of bi-directional data exchanges between the targeted communities and the Application Provider. AppCloud™ provides Sponsors of Covisint hosted portal communities with a single location to obtain business relevant third-party applications for their users. With the click of a mouse, users may register or subscribe to a variety of software applications in a highly secure environment at their desktop. Once approved, the user may access the applications through Single Sign-On (SSO), avoiding the need to recall multiple user names and passwords. Additionally, users are able to utilize data within their portal that was provided by the Application Provider through AppCloud. AppCloud is an ideal solution for Application Providers that want to offer applications to an established set of targeted business communities across a variety of industries.

About this Guide

Purpose/Background

The purpose of this document is to describe the integration process and key integration tasks that must be completed by an Application Provider in order to implement an SSO and Application Provisioning integration which will ultimately allow approved users to gain access to the Application Provider's application via Single Sign-On (SSO).

Audience

IT personnel who will be responsible for completing the integration tasks required to support the processes described in this guide. It is assumed that the reader is familiar with federation and web services technologies.

Definitions, Acronyms and Abbreviations

Term	Definition
AppCloud™	Provides Application Providers with a single point of integration to make their application(s) available to user's of Covisint hosted Portal communities. Provides Sponsor's of these Portal communities with a single location to obtain business relevant third-party applications.
Application Provider (AP)	An organization that is responsible for making an application available to Sponsor Portal communities through AppCloud. From a federation perspective the Application Provider is a Service Provider for AppCloud.
Federation	The ability to utilize identities from one security domain within another using a pre-established trust relationship between the participating entities. The IdP is responsible for making an identity assertion and the SP is responsible for providing the appropriate service(s) to the user associated with the identity.
Identity Provider (IdP)	Is responsible for the creation and management of a user's identity, the authentication of the user which binds the identity to the user, and the federation of the user's identity to a Service Provider. Covisint is the Identity Provider for AppCloud.
SAML (Security Assertion Markup Language)	An OASIS XML-based framework for securely exchanging authentication and authorization data between security domains, that is, between an identity provider (a producer of assertions) and a service provider (a consumer of assertions).
Service	The terms Service and Application can be used interchangeably in this document. In general, a service is defined by a Target URL which is used to reference the application that the Service Provider will make available to a user through AppCloud.
Service Provider (SP)	Consumes an identity for the purpose of providing a service(s) to the user associated with the identity. The identity is provided to the SP through an inbound federation from an Identity Provider (IdP). The Application Provider is a Service Provider for AppCloud.
SPML (Service Provisioning Markup Language)	An OASIS XML-based framework for exchanging user, resource and service provisioning information between cooperating organizations.

Overview

SSO and Application Provisioning Integration Process

The following is an overview of the key steps that will need to be done by the Application Provider in order to complete the AppCloud SSO and Application Provisioning integration process:

1. Register as an Application Provider with AppCloud.
2. Register additional users with AppCloud so that they can become administrators (this step is optional).
3. Grant AppCloud administrator roles.
4. Create a federation connection, using the self-service features within AppCloud, to implement one of the currently supported AppCloud standard federation protocols and test the connection.
5. Add an Application to AppCloud and test SSO to the application.
6. Select an AppCloud standard application provisioning option and test ability to grant and revoke the application.
7. Obtain AppCloud certification and Sponsor acceptance.

Application Provider Registration

Overview

The Application Provider selects a person to be their organization's Security Administrator. That person will then be responsible for registering the Application Provider with AppCloud. The person selected (the registrant) will be sent an AppCloud invitation. The invitation contains a link to an online registration that will be used to provide information about the Application Provider's organization, to provide information about the registrant, and to allow the registrant to select a user name and password that will be used to sign-on to AppCloud. When the registration is completed the registrant will automatically be granted the Security Administrator role and will then be able to sign-on to AppCloud using the user name and password that was selected. The Security Administrator will be the Application Provider's primary contact for any communications from Covisint regarding AppCloud. The Security Administrator has the highest level of authority for the Application Provider, within AppCloud, and has primary responsibility for determining who can become an AppCloud administrator and which role or roles each administrator will be responsible for.

Summary of Application Provider's Responsibility

- Application Provider determines who their Security Administrator will be and provides Covisint with that person's email address.
- Person identified completes an AppCloud online registration.

Process

1. Application Provider provides Covisint with the email address of the person (the registrant) that will be completing the registration and will become the Application Provider's Security Administrator.
2. Covisint AppCloud Administrator sends an invitation to the specified registrant.
3. Registrant navigates to the AppCloud registration wizard via a link in the email invitation and submits the requested information. Upon completing the registration the registrant will automatically be granted the Security Administrator role.
4. An email is sent to the registrant, who is now the Application Provider's Security Administrator, to confirm that the registration was completed successfully. The confirmation email contains a link to the AppCloud sign-on page.

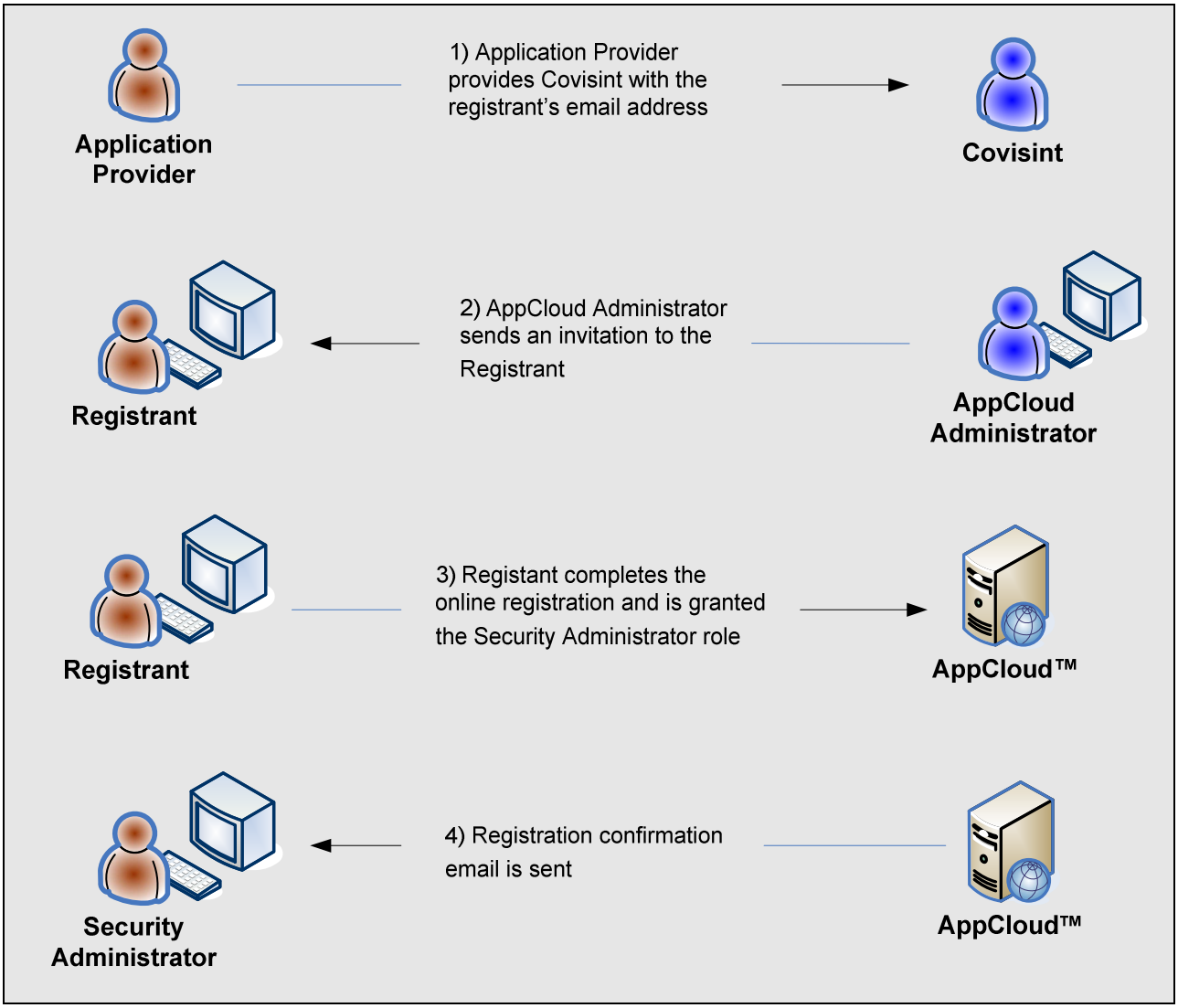

Figure 1: Application Provider Registration

User Registration

Overview

The Security Administrator can invite additional users to register with AppCloud™ so that they can become administrators for the Application Provider. The new user (the registrant) will be sent an AppCloud invitation and will then complete an online user registration that will be used to provide information about the registrant, and allow the registrant to select a user name and password that will be used to sign-on to AppCloud. After the user has registered, the Security Administrator can grant the appropriate administrator role or roles to the user.

Summary of Application Provider's Responsibility

- Security Administrator sends an invitation to a user (the registrant) from AppCloud.
- Registrant completes AppCloud user registration.

Process

1. Security Administrator signs-on to AppCloud and uses the 'Invite User' feature to send an invitation to a user (the registrant).
2. Registrant navigates to the AppCloud registration wizard via a link in the email invitation and submits the requested information.
3. An email is sent to the registrant, who is now a registered user, to confirm that the registration was completed successfully. The confirmation email contains a link to the AppCloud sign-on page.

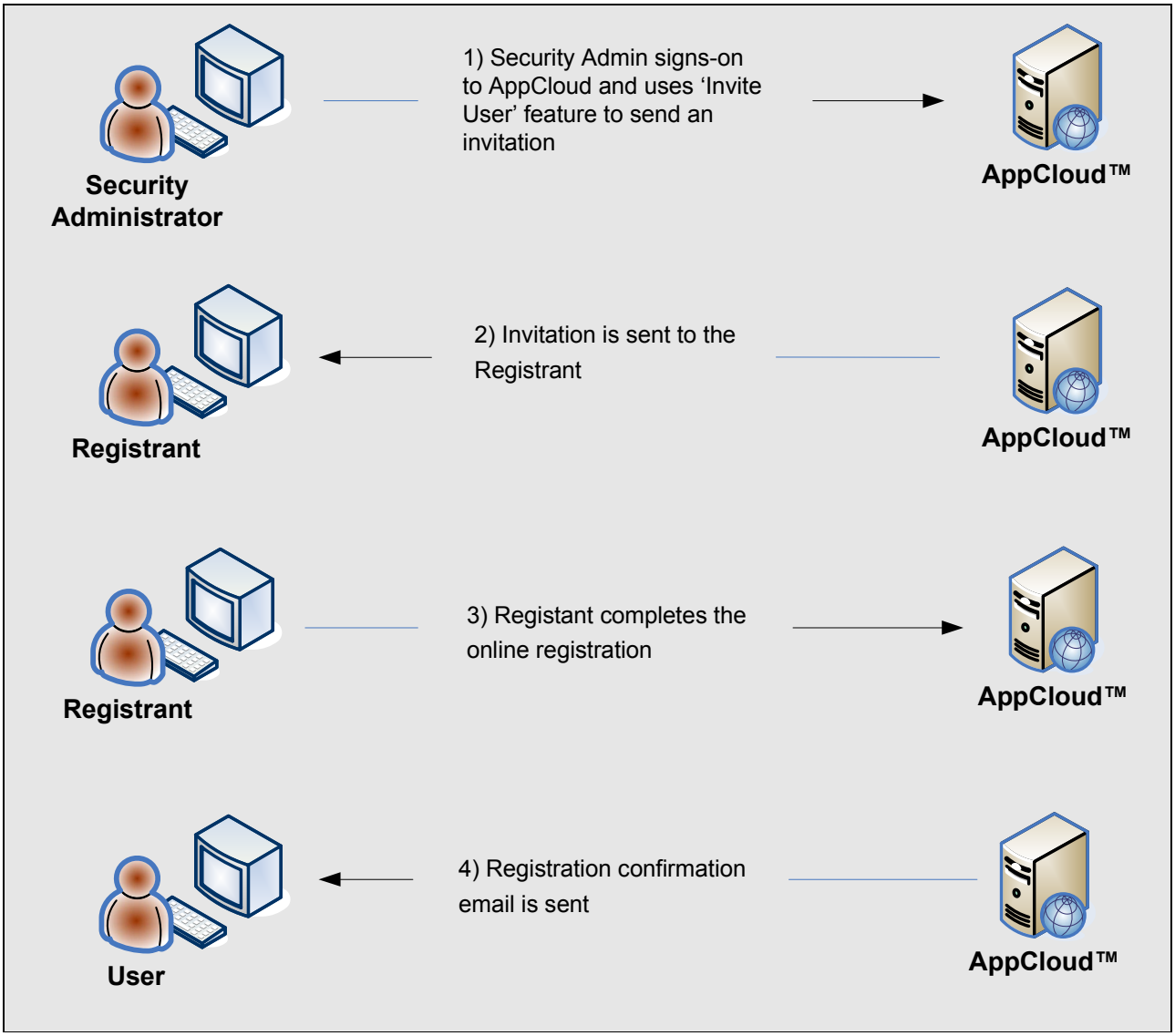

Figure 2: User Registration

Granting Administrator Roles

Overview

The Security Administrator can grant the Security Administrator, Federation Configuration Administrator, Application Configuration Administrator, and/or Application Access Administrator roles to a user.

- The *Security Administrator* role is granted to the user or users that will manage the Application Provider's AppCloud administrators.
- The *Federation Configuration Administrator* role is granted to the user or users that will create and manage the federation connection between AppCloud™ and the Application Provider.
- The *Application Configuration Administrator* role is granted to the user or users that will add and manage the Application Provider's application or applications in AppCloud.
- The *Application Access Administrator* role is granted to the user or users that will manage application grants and revokes when using the 'Admin Managed' provisioning option.

Note: If the appropriate Administrator role is *not* granted, the icon pertaining to the function that role enables will *not* be visible.

Summary of Application Provider's Responsibility

- Application Provider's Security Administrator grants administrator role(s) to the appropriate user.

Process

1. Application Provider's Security Administrator signs-on to AppCloud and uses the 'Manage Organization' feature to grant the appropriate role or roles to a user.
2. Email is sent to user to notify the user that the Administrator role(s) was granted.

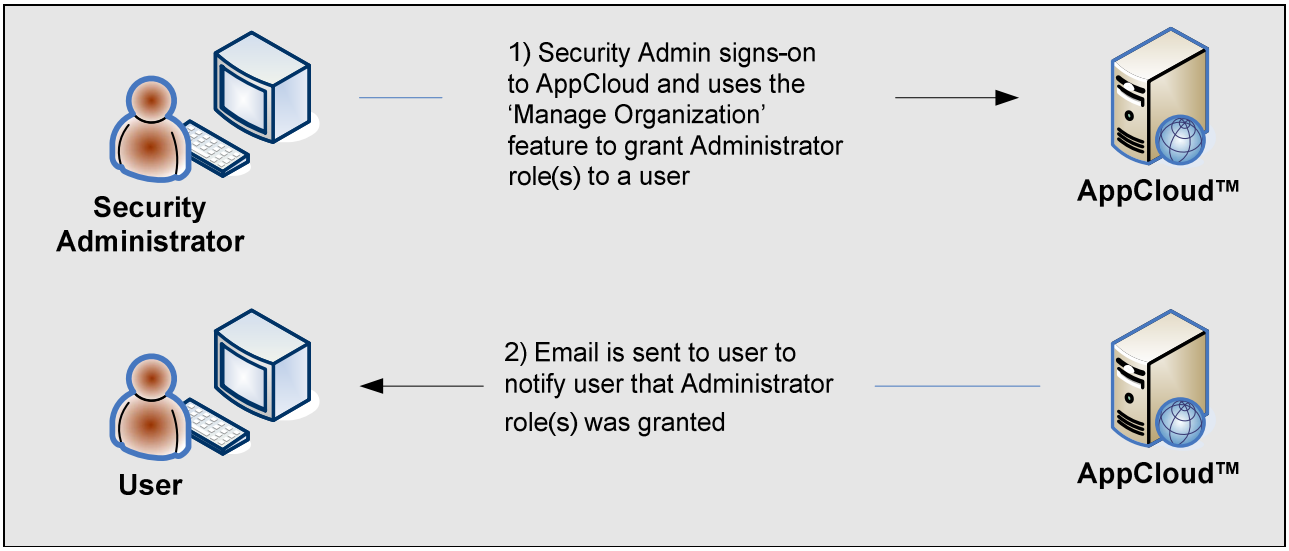

Figure 3: Granting Administrator Roles

Creating a Federation Connection

Overview

The Federation Configuration Administrator will create and manage the federation connection between AppCloud™ and the Application Provider. This is accomplished by exchanging federation configuration information with AppCloud which is used to establish a trust relationship between AppCloud and the Application Provider so that user information can be securely shared with the Application Provider. The user information is contained in a federation assertion that is generated and digitally signed by the AppCloud federation producer, the digital signature will then be validated by the Application Provider's federation consumer, and this information will ultimately be utilized by the Application Provider's application to provide access to an approved user. The *AppCloud™ Federation Integration Guide* is a supplement to this guide that provides additional details about the federation process, associated requirements, and the options which are availabe to an Application Provider that wants to integrate with AppCloud. A federation connection needs to be established prior to adding any applications to AppCloud.

Summary of Application Provider's Responsibility

- Select the federation protocol that will be used from the list of industry standard federation protocols that are supported by AppCloud.
- Implement or utilize an existing federation consumer at the Application Provider's site.
- Create a federation connection by exchanging federation configuration information with AppCloud.
- Self-verify that the Application Provider's federation consumer is able to receive a test assertion from AppCloud to insure that the federation connection has been established correctly.

Process

1. Federation Configuration Administrator signs-on to AppCloud and uses the 'Manage Federation Connections' feature to download the AppCloud signature verification certificate and the associated configuration information. Or, if using a solution that supports meta-data, downloads the meta-data file.
2. Federation Configuration Administrator uses the information that is downloaded to complete the federation configuration on the Application Provider's federation consumer (this is an offline effort that is done at the Application Provider's site)
3. Federation Configuration Administrator signs-on to AppCloud and uses the 'Manage Federation Connections' feature to select the federation protocol that will be used, from the list of industry standard protocols that are supported by AppCloud, and provides all additional configuration information that is required.
4. Once the federation connection is established the Federation Configuration Administrator selects the 'initiate test' link.
5. Test assertion is sent from AppCloud to the Application Providers' federation consumer. The Federation Configuration Administrator can then iteratively modify the configuration and test until the connection is configured correctly and a test assertion can be verified successfully.

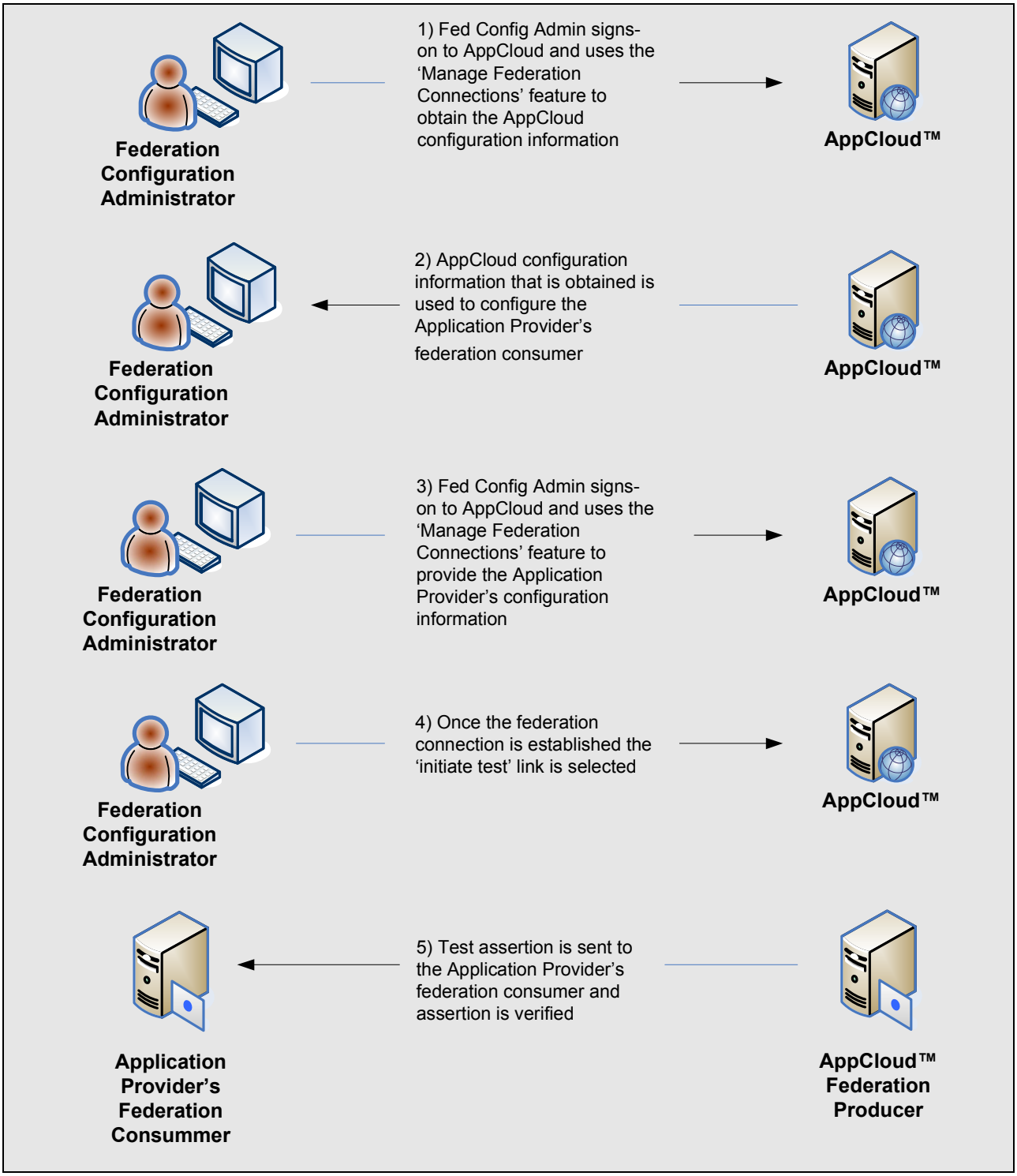

Figure 4: Creating a Federation Connection

Adding an Application

Overview

The Application Configuration Administrator will add and manage the Application Provider's application or applications in AppCloud™. The Application Configuration Administrator adds an application to AppCloud by providing the requested application configuration information and by selecting an established federation connection (see previous section for additional details about creating a federation connection) that will be used to support SSO to the application. Once the application is added, an application ID that will be used to uniquely identify the application in Covisint systems is created. This ID is called the Covisint Application ID. The Covisint Application ID will be used whenever Covisint or the Application Provider needs to uniquely identify the application.

Summary of Application Provider's Responsibility

- Provide AppCloud with the requested application configuration information and associate the application with an established federation connection.
- Self-verify that a test user is able to use SSO from AppCloud to gain access to the application successfully.

Process

1. Application Configuration Administrator signs-on to AppCloud and uses the 'Manage Applications' feature to provide the requested application configuration information and to associate the application with an established federation connection (which has already been configured between AppCloud and the Application Provider and has been self-verified). The configuration information that will be requested includes: Application name, application description, stage/test application URL, production application URL, etc. When the configuration is submitted the application is added to AppCloud and the Covisint Application ID will be created and can be viewed and referenced by the Application Configuration Administrator whenever required.
2. The Application Configuration Administrator then selects the 'initiate test' link to start the self-verification process.
3. A test assertion (which contains the user information for the Application Configuration Administrator that is performing the test) is sent from AppCloud to the Application Provider's federation consumer which will: Verify the assertion, issue the Application Provider's standard security token (which is used for session security) to the user's browser, and then redirect the browser to the application.
4. Application Configuration Administrator will be given access to the application based on the security token that was issued to the user's browser. The Application Configuration Administrator can iteratively modify the application configuration and test until the Application Configuration Administrator can gain access to the application via SSO from AppCloud successfully.

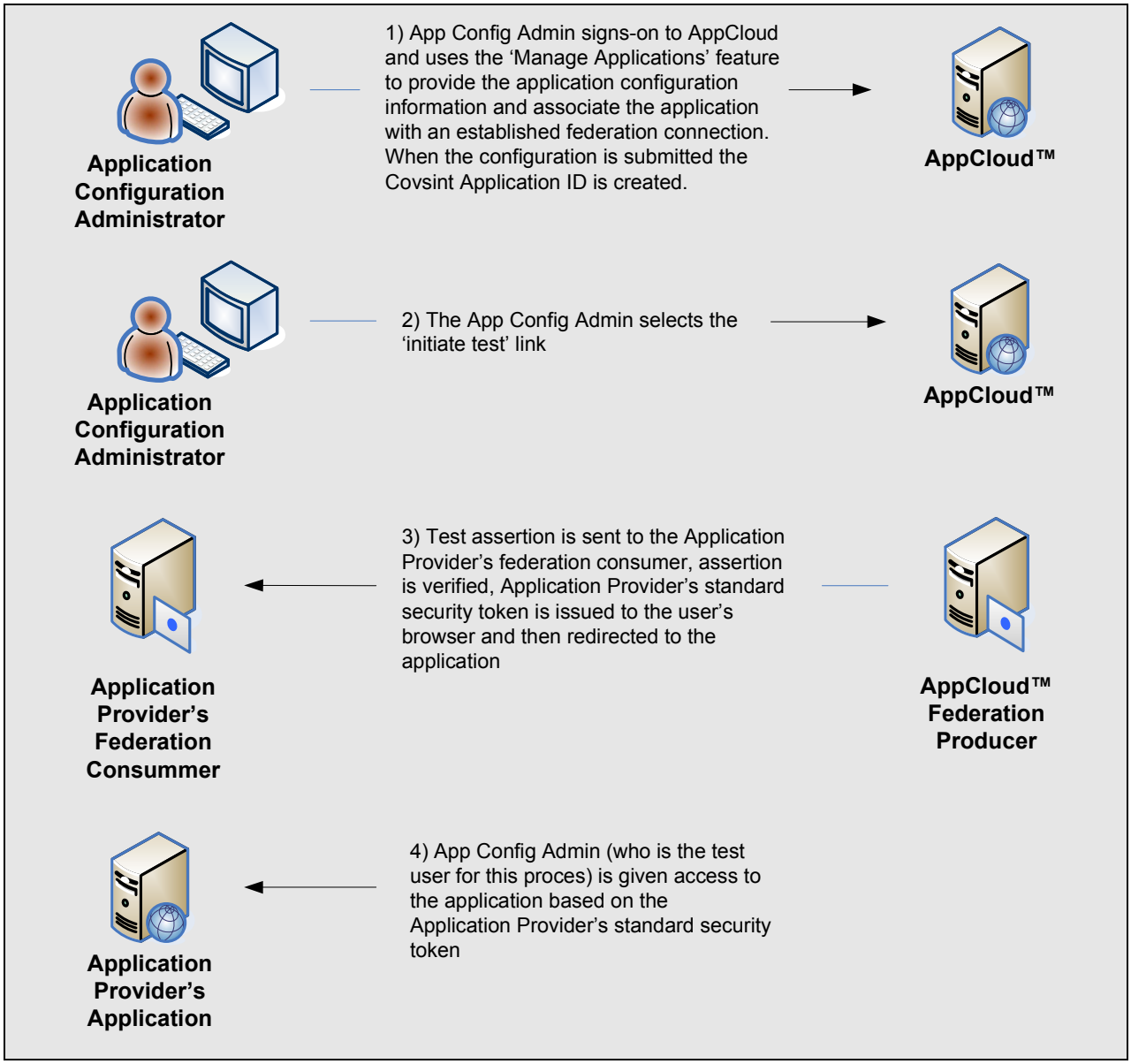

Figure 5: Adding an Application

Application Provisioning

Overview

Application Provisioning is used to grant an application to a group (i.e. an organization or practice) or user and to revoke an application from a group or user (de-provisioning). AppCloud™ currently provides support for three standard application provisioning options.

- *Admin Managed*: The Application Provider's Application Access Administrator uses the AppCloud 'Manage Access' feature to manage application grants and revokes. The Application Provider uses an appropriate out of band process (typically a standard process that already exists) to grant or revoke the application to the group or user in the Application Provider's system.
- *First Federation*: Using information in the user's federation assertion, the user is granted the application in the Application Provider's system in real-time the first time the user uses SSO to access the application.
- *Automated*: The Application Provider implements a web service server that accepts and responds to AppCloud web service requests. Based on a request from AppCloud, the service will take the appropriate corresponding action to grant or revoke the application to the group or user in the Application Provider's system. The service then responds back to AppCloud to acknowledge that the request was received and to provide the status of the requested action.

Admin Managed

The Admin Managed application provisioning option supports an administrator controlled process for granting an application to a group or user. Also, if required revoking access from a group or user. The Application Provider has two options for approving an application request: Requests can be approved for a group prior to approving requests from users associated with the group or user requests can be approved directly without an initial group approval.

When a group or user requests an application from a Sponsor's Portal, a Sponsor defined approval process is used to approve the request. Once the approval is obtained, the request is placed in the Application Provider's application request queue and an email is sent to the Application Provider's Application Access Administrator.

The Application Access Administrator then signs-on to AppCloud and reviews the list of pending group or user requests. The Application Access Administrator reviews the details associated with a specific request and determines if the request should be approved or rejected. If the request is not to be approved, the request is rejected and the process is complete. If the request is to be approved, the Application Access Administrator uses the details provided in the request to initiate the standard process that the Application Provider uses to grant the application to a group or user in the Application Provider's system. If the group or user already exists in the Application Provider's system, the Application Provider can map any new information provided in the request to the existing account.

Once the application request has been set up correctly in the Application Provider's system, the Application Access Administrator then signs-on to AppCloud and approves the request, the application is granted to the group or user, and an email notification is sent to the appropriate group administrator or the user to acknowledge that the application was granted. After an application is granted to a group it can then be made available to user's associated with the group. After an application has been granted to a user, the user is then able to gain access to the application using SSO.

If the application needs to be revoked from a user or group, the Application Access Administrator signs-on to AppCloud and reviews the list of groups and users that have been granted the application. The Application

Access Administrator then reviews the details associated with a specific grant and has the ability to revoke the application from the user or group selected. After the application has been revoked, the user will no longer be able to access the application using SSO via AppCloud. When an application is revoked from a group it is simultaneously revoked from all users that are members of the group.

Summary of Application Provider's Responsibility

- Application Access Administrator checks the application request queue in AppCloud to review the list of pending requests.
- Application Access Administrator reviews the details of the request and if it is to be approved initiates a standard Application Provider process (which is outside of AppCloud) to grant the application to the group or user in the Application Provider's system.
- Application Access Administrator approves or rejects the application request in AppCloud.
- If required, Application Access Administrator reviews the groups and/or users that have been granted the Application Provider's application.
- If required, Application Access Administrator revokes an application from a specific user or group.

Provisioning Process

1. Group Admin or user of a Sponsor's Portal requests the application (the Group Admin makes a group request and the user makes a user request) which is then approved through an appropriate Sponsor defined workflow process.
2. Request is put in the Application Access Administrator's application request queue.
3. Email notification is sent to the Application Access Administrator to indicate that a request for the application was made.
4. Application Access Administrator selects the link in the email to navigate to the details of the specific request. Or, signs-on directly to AppCloud and selects the 'Manage Access' feature to review the entire list of pending requests in the queue (both group and user requests). Details of the request are reviewed and a decision is made to approve or reject the request. If the request is rejected, the group or user is not granted the application (and the process is complete).
5. If it is determined that the request will be approved. The information provided in the details of the request is used to initiate the process that the Application Provider uses to grant the application to a group of user in the Application Provider's system. If the group or user already exists in the Application Provider's system, the Application Provider can map any new information provided to the existing account.
6. Once the group or user is set up correctly, the Application Access Administrator navigates to AppCloud and uses the 'Manage Access' feature to approve the request.
7. Group or user is then granted the application and an email notification is sent to the Group Admin or user respectively to acknowledge that the application was granted.

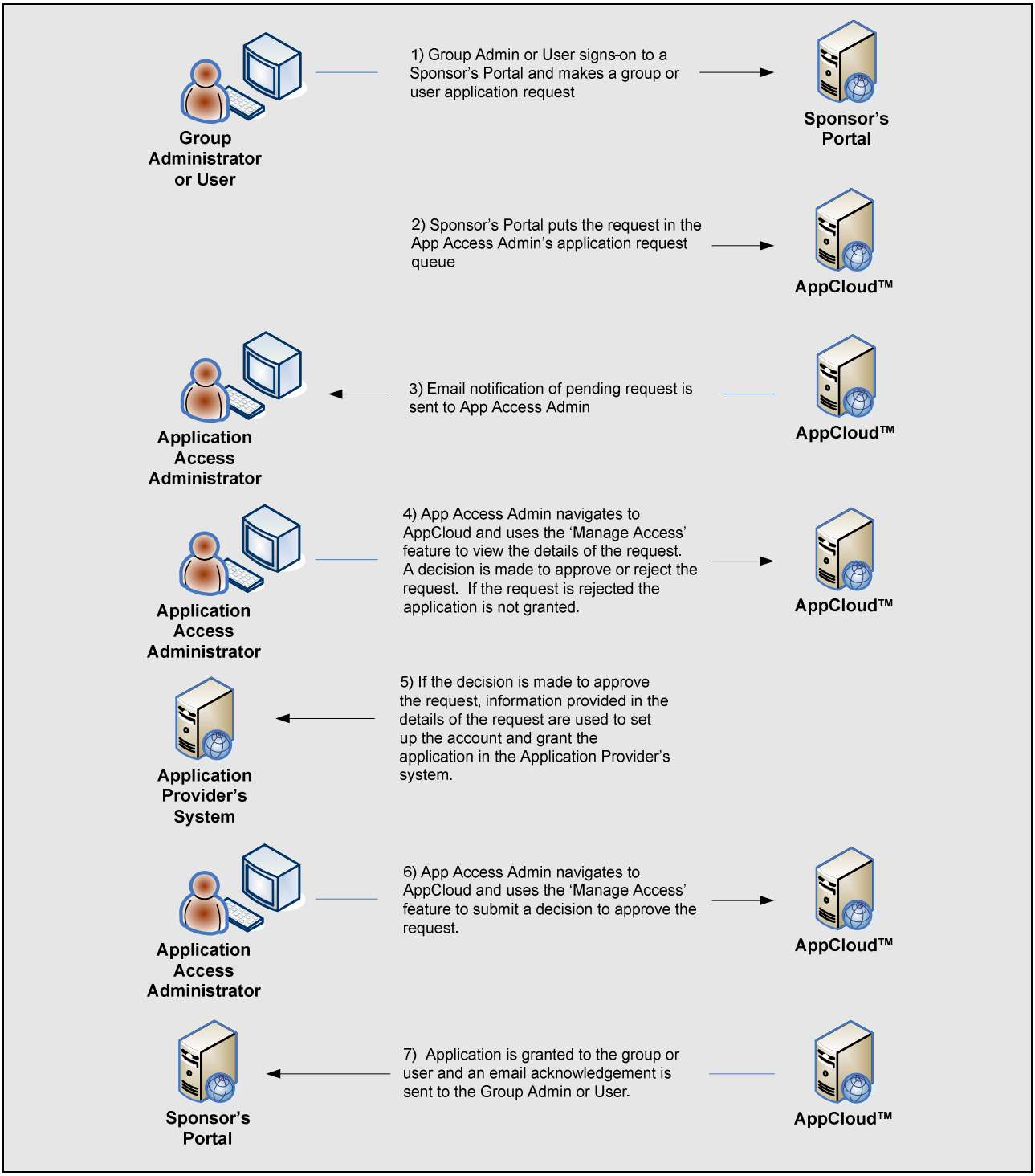

Figure 5: Admin Managed Provisioning Process

De-provisioning Process

1. Application Access Administrator signs-on to AppCloud and selects the 'Manage Access' feature to view the list of group and user grants. Details of a specific grant are selected and reviewed and the Application Access Admin submits a decision to revoke the application.
2. Application is revoked from the specific user or group submitted.

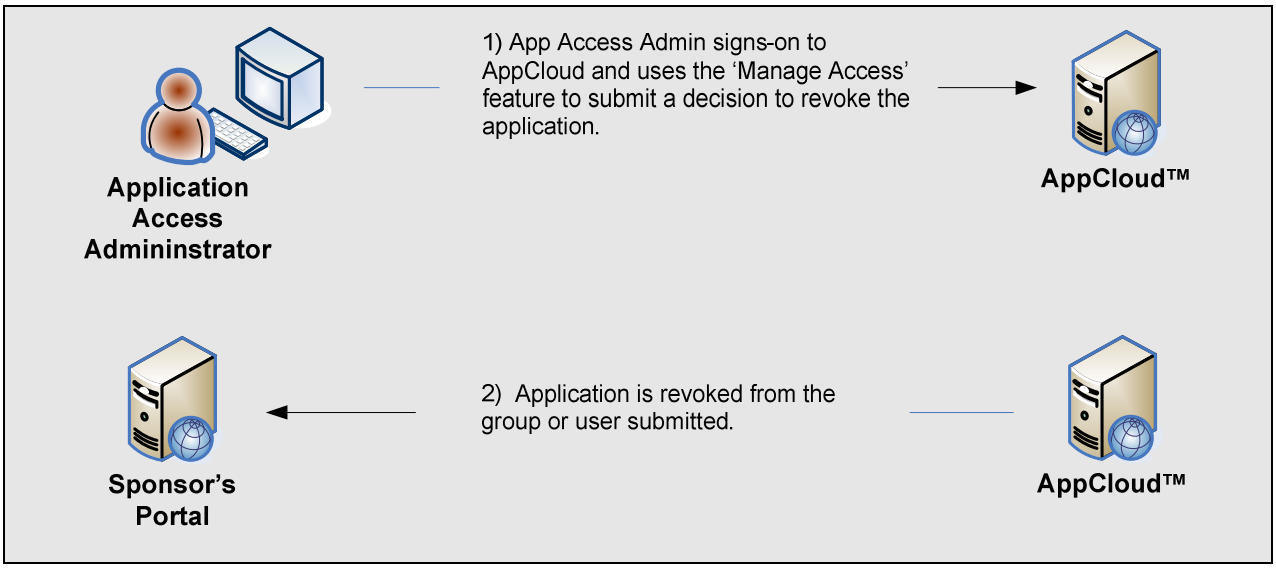

Figure 6: Admin Managed De-provisioning Process

First Federation

The First Federation application provisioning option supports a dynamic process for granting an application to a user, and is used in conjunction with the AppCloud™ 'Admin Managed' de-provisioning process described in the previous section to revoke an application from a user.

When a user requests an application from a Sponsor's Portal, a Sponsor defined approval process is used to approve the request. Once the approval is obtained, the application is granted to the user. After the application has been granted to the user, the user is then able to select the application from a list of granted applications in the Portal and federate to the application.

The first time the user federates to the Application Provider's site, information contained in the user's assertion is used to grant the application to the user in the Application Provider's system in real-time. If the Application Provider needs to provide support to users that are already in the Application Provider's system, the expected behavior is that the application will prompt the user with a question to determine if the user is an existing user or a new user. If the user is an existing user, the user is then prompted to provide the user name and password that the user uses when authenticating directly to the application (it is important to note that this would only happen during the user's first federation and would not happen on subsequent federations). Once the user has been authenticated, any new information in the user's assertion can then be mapped to the user's existing account and the user is then given access to the application. If the user is a new user, the information in the user's assertion is used to create a new user account and grant the application to the user in the Application Provider's system and the user is then given access to the application.

If the application needs to be revoked from a user, the Application Access Administrator uses the AppCloud 'Admin Managed' de-provisioning process described in the previous section.

Summary of Application Provider's Responsibility

- Implement a solution to grant the application to the user in the Application Provider's system in real-time the first time the user federates to the application.
- If required, Application Access Administrator uses the AppCloud 'Admin Managed' feature to revoke an application from a specific user.

Provisioning Process

1. A user signs-on to a Sponsor's Portal and requests the application. The request is then approved through a Sponsor defined approval process and the application is granted to the user.
2. After the application has been granted, the user selects the application from a list of applications that have been granted to the user in the Sponsor's Portal.
3. The user is then federated to the application for the first time.
4. Using information which is available in the user's assertion, the user account is either created and the application is granted or updates are made to an existing user account in the Application Provider's system and the user is then given access to the application.

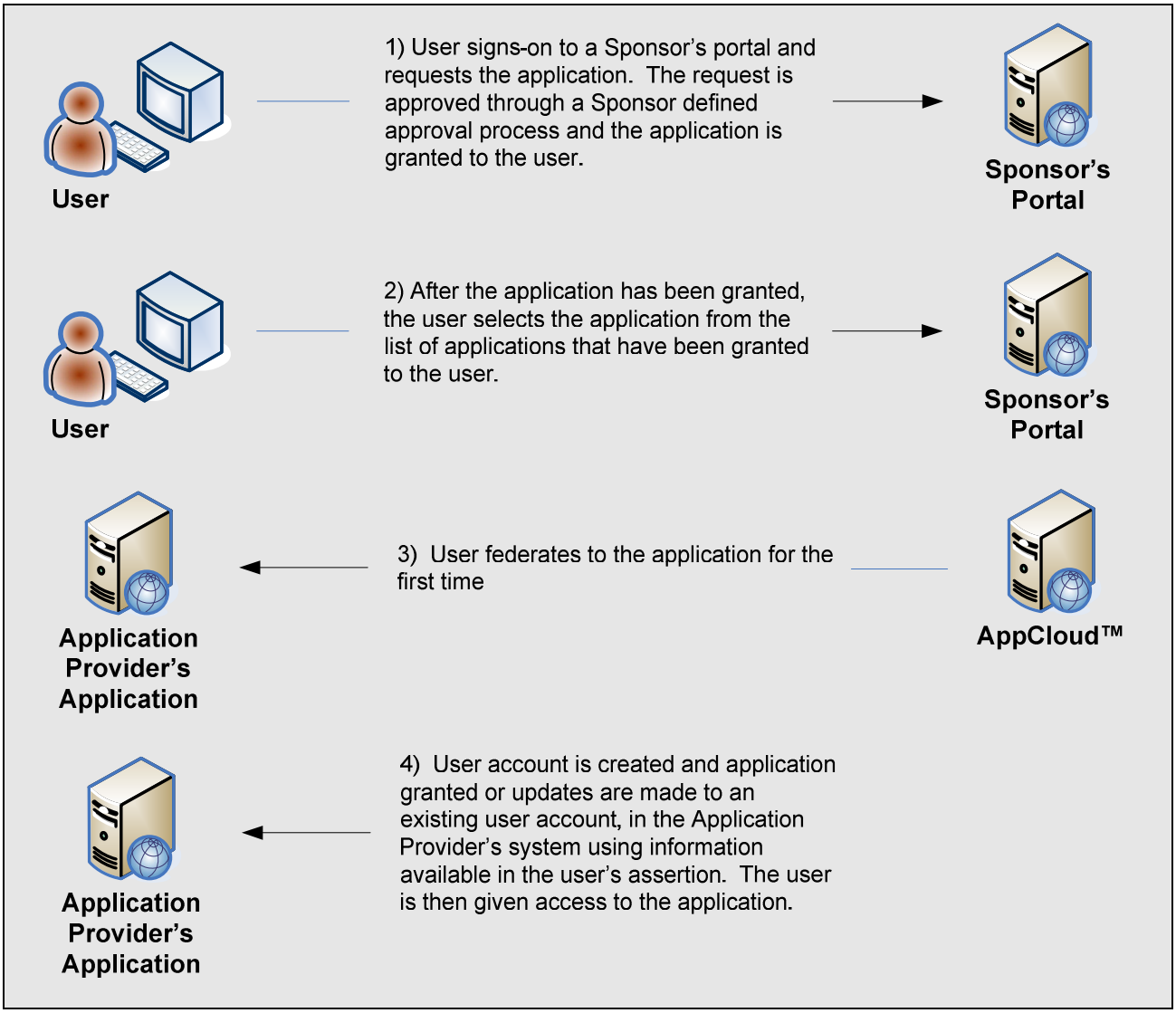

Figure 7: First Federation Provisioning Process

De-Provisioning Process

- The AppCloud 'Admin Managed' de-provisioning process described in the previous section is used to revoke an application from a user that was provisioned the application using the first federation provisioning option.

Automated

The application provisioning process can be automated through the use of web services which are implemented at the Application Provider's site and at Covisint. Web services are used to grant an application to a group (i.e. an organization or practice) and/or user and to revoke an application from a group and/or user.

When a specific group requests an application from a Sponsor's Portal, a Sponsor defined approval process is used to approve the request. When the approval is obtained, AppCloud sends a web service request to the Application Provider's GrantAppToGroup service and the application is granted to the group in the Application Provider's system. A web service response is then sent back to AppCloud to acknowledge successful completion of the request. When the response is received, the group is granted the application and the application is then available to the group.

When a specific user requests an application from a Sponsor's Portal, a Sponsor defined approval process is used to approve the request. When the approval is obtained, AppCloud sends a web service request to the Application Provider's GrantAppToUser service and the application is granted to the user in the Application Provider's system. A web service response is then sent back to AppCloud to acknowledge successful completion of the request. When the response is received, the user is granted the application and the application is then available to the user.

When an application is revoked from a user, AppCloud sends a web service request to the Application Provider's RevokeAppFromUser service and the application is revoked from the user in the Application Provider's system. A web service response is then sent back to AppCloud to acknowledge successful completion of the request.

When an application is revoked from a group, AppCloud sends a web service request to the Application Provider's RevokeAppFromGroup service and the application is revoked from the group and simultaneously revoked from all users associated with the group in the Application Provider's system. A web service response is then sent back to AppCloud to acknowledge successful completion of the request.

The *AppCloud™ Automated Provisioning Integration Guide* is a supplement to this guide that provides additional details about these web services, associated requirements, and the options that are availabe to an Application Provider that wants to integrate with AppCloud to implement automated provisioning.

Summary of Application Provider's Responsibility

- Implement a web service server that supports the GrantAppToGroup, GrantAppToUser, RevokeAppFromUser, and RevokeAppFromGroup services.
- Exchange digital certificates with Covisint. The keys associated with these certificates will be used to generate and verify digital signatures.
- Implement associated system changes to support the behaviors defined for each service.
- Provide Covisint with the URLs for the services.

Group Provisioning Process

1. Group Administrator signs-on to the Sponsor's Portal and requests the application for the group. Request is approved through Sponsor defined approval process.
2. AppCloud sends a web service request to the Application Provider's GrantAppToGroup service.
3. Application Provider grants the application to the group in the Application Provider's system and then sends a web service response back to AppCloud to acknowledge successful completion of the request.
4. When the response is received, the application is granted to the group.
5. Group Administrator is notified that the request was approved.

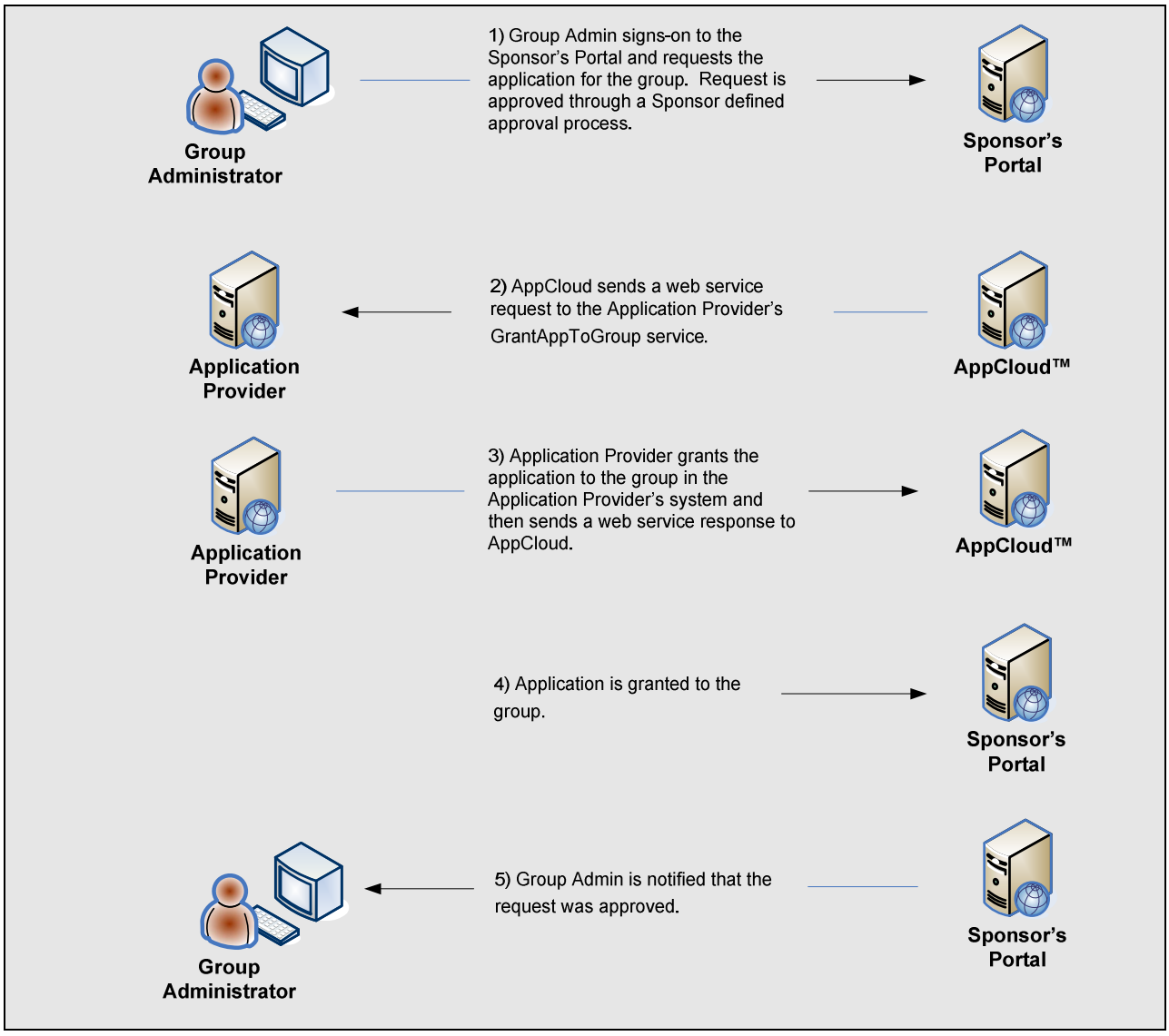

Figure 7: Automated Group Provisioning Process

User Provisioning Process

1. User signs-on to the Sponsor's Portal and requests the application. Request is approved through a Sponsor defined approval process.
2. AppCloud sends a web service request to the Application Provider's GrantAppToUser service
3. Application Provider grants the application to the user in the Application Provider's system and then sends a web service response to AppCloud
4. Application is granted to the user.
5. User is notified that the request was approved.

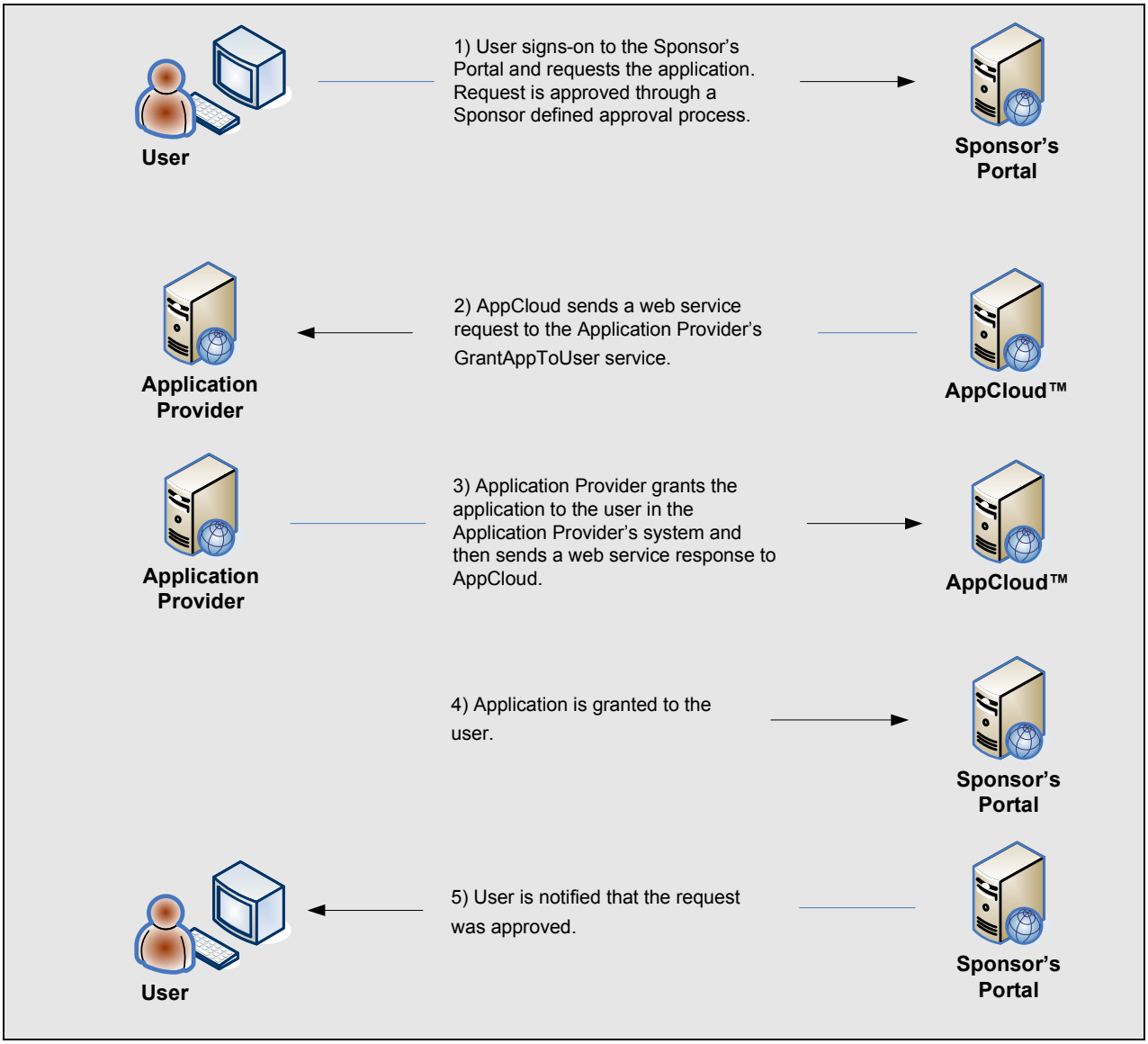

Figure 8: Automated User Provisioning Process

User De-provisioning Process

1. Group Administrator signs-on to the Sponsor's Portal and revokes the application from a user.
2. AppCloud sends a web service request to the Application Provider's RevokeAppFromUser service.
3. Application Provider revokes the application from the user in the Application Provider's system and then sends a web service response to AppCloud

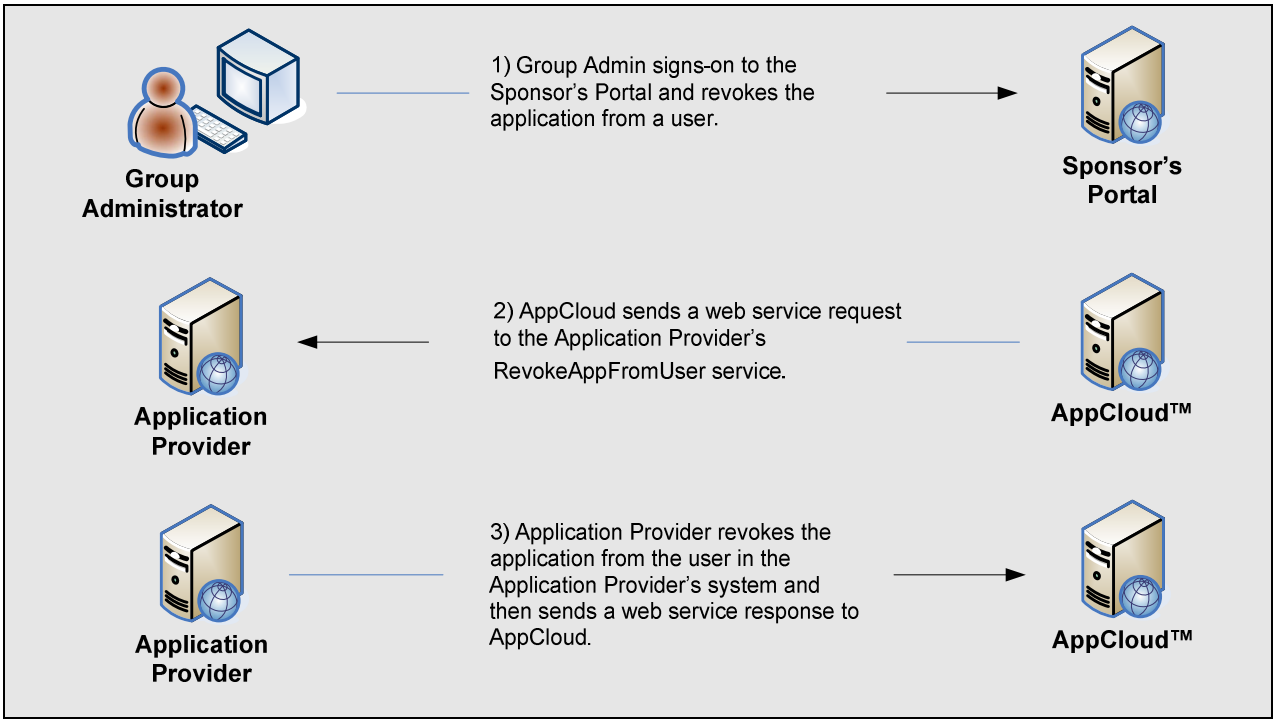

Figure 9: Automated User De-provisioning Process

Group De-provisioning Process

1. Group Administrator signs-on to the Sponsor's Portal and revokes the application from a group.
2. AppCloud sends a web service request to the Application Provider's RevokeAppFromGroup service.
3. Application Provider revokes the application from the group and from all the users associated with the group in the Application Provider's system and then sends a web service response to AppCloud.

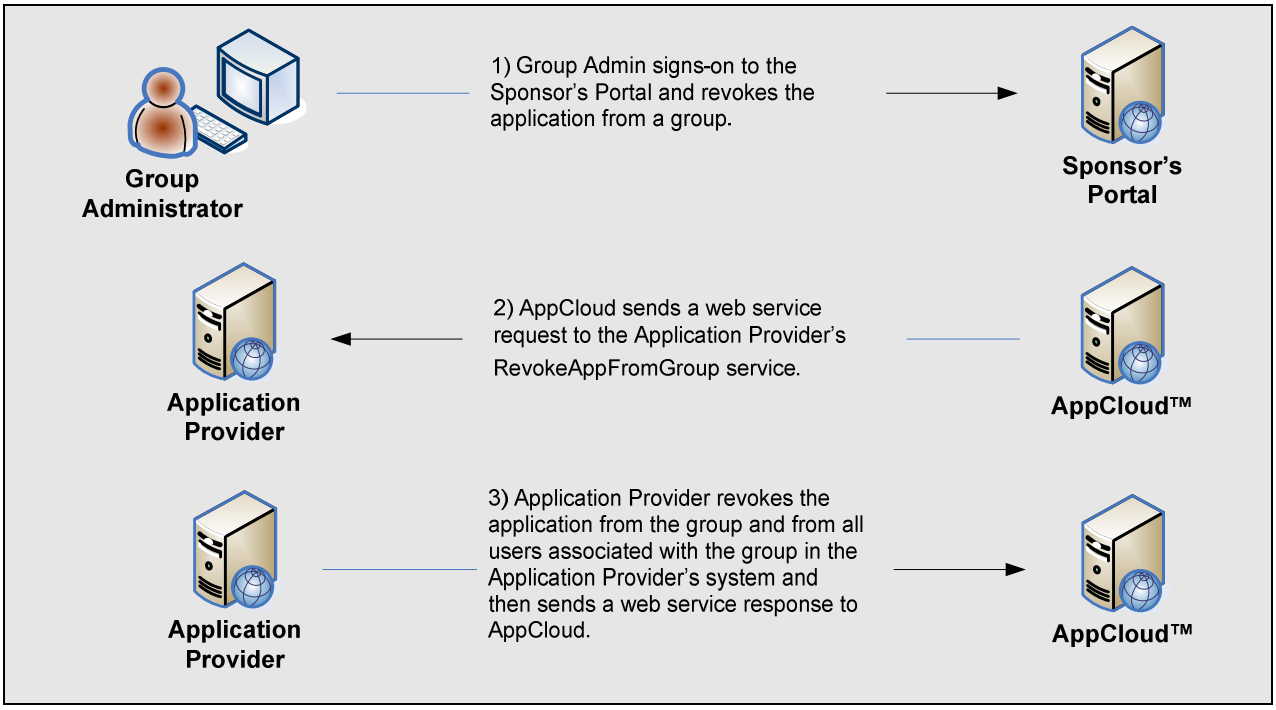

Figure 10: Automated Group De-provisioning Process

Certification and Sponsor Acceptance

Overview

Users associated with a specific Sponsor's Portal will be using applications from a variety of Application Providers. The certification process is used to insure that the integration has been implemented correctly and to insure that the user experience across all applications will be as consistent as possible. A production readiness review will also be conducted to insure that the Application Provider understands and is ready to perform the roles required to support the expected standard processes described in this guide. An additional goal is to insure that any and all areas of non-compliance are documented and understood by the Sponsor. The Sponsor will be required to approve any identified non-compliance.

Expected Behaviors

In order to insure a consistent user experience across all the applications that a user will be accessing via SSO the following behaviors have been defined. It is expected that the Application Provider's application(s) will be compliant with these behaviors.

Single Sign-On

1. User signs-on to Sponsor's Portal.
2. User selects link to the application from a portlet that contains a list of all SSO applications that have been granted to the user.
3. New window pops up and displays the application.

Mapping To Existing User Accounts

This use case only applies when the first federation application provisioning option is used to provision the application. And is only required the first time the user federates to the application.

1. When a user selects the application for the first time, the application displays a message which asks if the user is a new user or an existing user.

If a new user:

2. Account is created in real time in the Application Provider's system using the information that is provided in the user's federation assertion.
3. The user is given access to the application.

If an existing user:

2. User is prompted for the user name and password that the user uses when authenticating directly to the application.
3. Covisint Unique ID (CUID) and any other new information about the user, which is provided in the user's federation assertion, is mapped to the existing user account in real time in the Application Provider's system.
4. The user is given access to the application.

Application Session Security Timeout

1. Application Provider's Web Access Management solution enacts session security timeout.
2. Application displays a message to the user informing the user that session security timeout has occurred and that the user needs to close the window that the application session is running in and reselect the application link from the Portal if access to the application is still required.

Application Logout

1. User selects “logout” from the application.
2. Application closes the window that the application’s session is running in.

Production Readiness

A production readiness review will be conducted to insure that the Application Provider understands and is ready to perform the roles required to support the expected standard processes described in this guide.

Systems

- Application Provider will support a stage/test environment that is readily available for joint Covisint and Application Provider testing as required to support issues resolution.
- Application Provider will support a Covisint Test ID in both stage/test and production environments to support issues resolutions, site integration validations, and production monitoring.

Sponsor Acceptance

Covisint will work with the Application Provider to document all areas of non-compliance and insure that this non-compliance is understood by the Sponsor. The Sponsor will be required to approve any non-compliance.

Application Provider Responsibilities Summary

This section provides a summary of the Application Provider's responsibilities associated with each of the key integration steps.

1. Register as an Application Provider with AppCloud™.
   - Application Provider determines who their Security Administrator will be and provides Covisint with that person's email address.
   - Person identified completes an AppCloud online registration.
2. Register additional users with AppCloud so that they can become administrators (this step is optional)
   - Security Administrator sends an invitation to a user (the registrant) from AppCloud.
   - Registrant completes an AppCloud online registration.
3. Grant AppCloud administrator roles
   - Application Provider's Security Administrator grants administrator role(s) to the appropriate user(s).
4. Create a federation connection with AppCloud using one of the currently supported AppCloud standard federation protocols and test the connection
   - Select the federation protocol that will be used from the list of industry standard federation protocols that are supported by AppCloud.
   - Implement or utilize an existing federation consumer at the Application Provider's site.
   - Create a federation connection by exchanging federation configuration information with AppCloud.
   - Self-verify that the Application Provider's federation consumer is able to receive a test assertion from AppCloud to insure that the federation connection has been established correctly.
5. Add an application to AppCloud and test SSO to the application
   - Provide AppCloud with the requested application configuration information and associate the application with an established federation connection.
   - Self-verify that a test user is able to use SSO from AppCloud to gain access to the application successfully.
6. Select an AppCloud standard application provisioning option and test ability to grant and revoke the application
   - Select the standard provisioning option that will be used to provision the application. Once the option has been selected review the associated responsibilities.
     - *Admin Managed*:
       - Application Access Administrator checks the application request queue in AppCloud to review the list of pending requests.
       - Application Access Administrator reviews the details of the request and if it is to be approved initiates an Application Provider process (which is outside of AppCloud) to grant the application to the group or user in the Application Provider's system.
       - Application Access Administrator approves or rejects the application request in AppCloud.
       - If required, Application Access Administrator reviews the groups and/or users that have been granted the Application Provider's application.
       - If required, Application Access Administrator revokes an application from a specific user or group.
     - *First Federation*:
       - Implement a solution to grant the application to the user in the Application Provider's system in real-time the first time the user federates to the application.
       - If required, Application Access Administrator uses the AppCloud 'Admin Managed' feature to revoke an application from a specific user.
     - *Automated*:
       - Implement a web service server that supports the GrantAppToGroup, GrantAppToUser, RevokeAppFromUser, and RevokeAppFromGroup services.

        - Exchange digital certificates with Covisint. The keys associated with these certificates will be used to generate and verify digital signatures.
        - Implement associated system changes to support the behaviors defined for each service.
        - Provide Covisint with the URLs for the services.
    - Work with Covisint to verify that an application can be granted to a test group and/or test user for a specific Sponsor and verify that a test user can gain access to the application successfully using SSO.
    - Work with Covisint to verify that the application can be revoked from a test user and/or test group for a specific Sponsor and confirm that the test user can no longer gain access the application.
7. Obtain AppCloud certification and Sponsor acceptance
    - Work with Covisint to QA test the SSO integration in a test/stage environment.
    - Work with Covisint to certify that the SSO integration complies with all AppCloud requirements and expected behaviors.
    - Complete systems certification.
    - If required, document any variations to the standard AppCloud processes and expected application behaviors. Any non-compliance will require sign-off from each Sponsor that will be using the application.
    - Work with Covisint to insure production readiness and to verify the Application Provider's ability to perform the required tasks associated with the user on-boarding process.
    - Work with Covisint and the Sponsor to obtain Sponsor acceptance.
    - Work with Covisint and the Sponsor to validate the SSO integration in production.