

Integración de PostilionPRM con ReD Shield

PostillónPRM

Versión 2.0

7 febrero 2018

ACI en todo el mundo

Oficinas en las principales ciudades del mundo

www.aciworldwide.com

América +1 402 390 7600 Asia

Pacífico +65 6334 4843

Europa, Medio Oriente, África +44 (0) 1923 816393

Fecha de publicación: febrero de 2018

© Derechos de autor ACI Worldwide, Inc. 2018

Toda la información contenida en esta documentación, así como el software descrito en ella, es confidencial y propiedad de ACI Worldwide, Inc., o una de sus subsidiarias, está sujeta a un acuerdo de licencia y puede usarse o copiarse solo de acuerdo con los términos de dicha licencia. Salvo que lo permita dicha licencia, ninguna parte de esta documentación puede reproducirse, almacenarse en un sistema de recuperación o transmitirse de ninguna forma ni por medios electrónicos, mecánicos, de grabación o de otro tipo, sin el permiso previo por escrito de ACI Worldwide, Inc., o una de sus subsidiarias.

ACI, ACI Payment Systems, el logotipo de ACI, ACI Universal Payments, UP, el logotipo de UP, ReD y todos los nombres de productos de ACI son marcas comerciales o marcas comerciales registradas de ACI Worldwide, Inc., o una de sus subsidiarias, en los Estados Unidos, otros países o ambos. Las marcas comerciales de terceros a las que se hace referencia son propiedad de sus respectivos dueños.

Acerca de ACI en todo el mundo

ACI Worldwide, la compañía de Universal Payments (UP), impulsa los pagos electrónicos para más de 5100 organizaciones en todo el mundo. Más de 1000 de las instituciones financieras e intermediarios más grandes, así como miles de comerciantes líderes a nivel mundial, confían en ACI para ejecutar \$14 billones cada día en pagos. Además, miles de organizaciones utilizan nuestros servicios de pago y presentación electrónica de facturas. A través de nuestro conjunto integral de software y soluciones basadas en SaaS, brindamos capacidades de pago en tiempo real, de cualquier a cualquier persona y habilitamos la experiencia de pagos omnicanal más completa de la industria. Para obtener más información sobre ACI, visite <http://www.aciworldwide.com> . También puedes encontrarnos en Twitter [@ACI_Worldwide](https://twitter.com/ACI_Worldwide) .

Contenido

Lista de Figuras	5
Acerca de esta publicación.....	6
Audiencia	6
Terminología.....	6
Sección 1: Introducción.....	8
Visión de conjunto	8
Requisitos del sistema	8
Resumen arquitectónico	9
Flujo de mensajes de análisis de riesgos en tiempo real.....	10
Flujo de mensajes de análisis de riesgos casi en tiempo real.....	11
Descripción general del servicio	12
Servicio RetailPaymentsRiskAnalyze.....	12
Limitaciones.....	12
Sistema operativo.....	12
Servicio de Modificación del Estado de la Tarjeta	12
Servicio de carga de datos demográficos	12
Prevención de duplicación de registros	12
Activo/activo con UPF (MCAS).....	12
Sección 2: Configuración del servicio.....	14
Sección 3: Configuración UPF (MCAS)	dieciséis
Conexión del registro de servicios estáticos.....	dieciséis
Conexión del registro de servicios dinámicos	17
Sección 4: Configuración del intercambio.....	18
Servicio RetailPaymentsRiskAnalyze.....	18
Mapeador de campo genérico	20
Sección 5: Configuración activa/activa	21
Configuración del Configurador de servicios	21
Identificación del servidor	21
Coordinación activo/activo y recuperación de fallos.....	21
Sección 6: Configuración de SSL.....	22
Sección 7: Configuración opcional	23

Configuración de rastreo.....	23
Seguimiento de eventos de postillón	23
Rastreo de eventos de Infraestructura de servicios empresariales	23
Seguimiento de eventos del marco universal de pagos	23

Lista de Figuras

Figura 1: Vista general de la arquitectura9

Figura 2: Flujo de mensajes en tiempo real10

Figura 3: Flujo de mensajes casi en tiempo real.....11

Figura 4: Ejemplo: administrador de plataforma UPF (MCAS) configuradodieciséis

Acerca de esta publicación

Audiencia

Este documento está destinado a los operadores responsables de configurar la interfaz PostilionPRM para integrarse correctamente con un ACI ReD Shield.® y el despliegue del Marco Universal de Pagos (UPF). El personal que utilice esta información debe tener el conocimiento y la experiencia adecuados en la configuración de un sistema Postilion.

Terminología

En este documento se utilizan los siguientes acrónimos:

Acrónimo	Término
TM	Gerente de transacciones
RPRA	RetailPagosRiskAnalyze
MCAS	Servidor de aplicaciones de misión crítica
UPF	Marco de pagos universales
RSS	Registro de servicios estáticos
DSR	Registro de servicio dinámico
BSI	Infraestructura de servicios comerciales

En este documento se utilizan los siguientes conceptos:

Concepto	Definición
transacción externa Procesando	Procesamiento realizado por una entidad externa a Transaction Manager para una transacción en particular. Ver el <i>Guía del usuario de Realtime Framework</i> para más información.
transacción del cliente	La transacción original iniciada por el cliente involucrado en una cadena de transacciones que requiere un procesamiento externo de transacciones.
Procesamiento externo transacción	La transacción auxiliar generada por Transaction Manager al realizar el procesamiento de transacciones externas en una transacción de cliente. La transacción de procesamiento externo está asociada con la transacción del cliente.

Gerente de plataforma	La aplicación que permite el seguimiento y gestión de la UPF(MCAS). Es una aplicación on-line y necesita estar conectada a una instancia UPF(MCAS) para llevar a cabo sus funciones. Consulte la sección "Herramientas de aplicación" de la <i>Guía de operaciones de la UPF</i> para más detalles.
-----------------------	---

Sección 1: Introducción

Visión de conjunto

ReD Shield está integrado con la interfaz de PostilionPRM mediante el servicio RetailPaymentsRiskAnalyze. Se utiliza una arquitectura basada en servicios para facilitar la comunicación entre un sistema Postilion y un servidor ReD Shield a través de UPF (MCAS).

Para integrar Red Shield con la interfaz de PostilionPRM, haga lo siguiente:

Nota: Los nodos receptores que se utilizarán para el análisis de riesgos ya deben haberse configurado en Transaction Manager antes de iniciar estos pasos de configuración.

1. Configure el servicio PostilionPRM. (Ver el [Configuración del servicio](#) sección)
2. Configure la interfaz de PostilionPRM para comunicarse con UPF (MCAS). (Ver el [Configuración UPF \(MCAS\)](#) sección)
3. Configure el nodo de control y procesamiento externo necesario. Consulte las secciones "Configuración de nodos de procesamiento externo" y "Configuración de nodos de control" del *Guía del usuario de Realtime Framework* para obtener información sobre la configuración de estos nodos.
4. Configurar el intercambio o intercambios (Ver el [Configuración de intercambio](#) sección)
5. Configurar activo/activo (opcional) (Ver el [Configuración activo/activo](#) sección)
6. Configure SSL para asegurar la comunicación entre PostilionPRM y UPF (MCAS) (Consulte el [configuración SSL](#) sección)
7. Configure el seguimiento (opcional) (Consulte la [Configuración de rastreo](#) sección)

Requisitos del sistema

Al integrar PostilionPRM con ReD Shield, se admiten los siguientes sistemas operativos y versiones mínimas:

- Sistema operativo Windows
- Marco en tiempo real v5.6
- PostilionPRM v2.0 Parche 15
- Marco de pago universal v3.2.2

Resumen arquitectónico

El siguiente diagrama muestra cómo encaja la interfaz PostilionPRM en un sistema Postilion cuando se integra con ReD Shield:

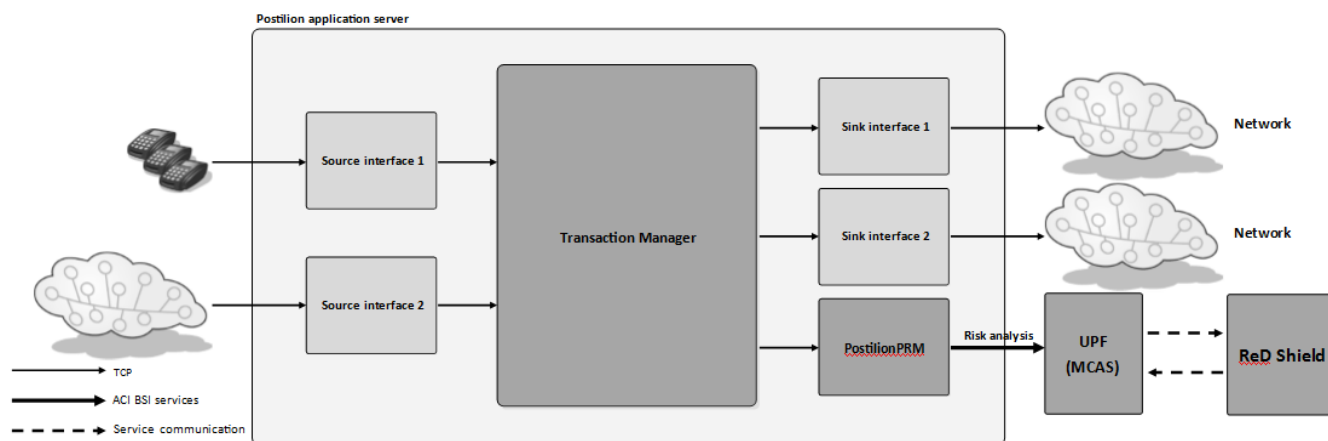


Figura 1: Resumen arquitectónico

La interfaz PostilionPRM está configurada como un intercambio receptor en el sistema Postilion:

- En el nodo sumidero de procesamiento externo, los mensajes de solicitud de transacción de Transaction Manager se envían al servidor ReD Shield. Estos mensajes solicitan al servidor ReD Shield que realice **análisis de riesgos en tiempo real** mientras se autoriza la transacción. Transaction Manager considera el resultado del análisis de riesgo y puede rechazar y posiblemente revertir la transacción como resultado.
- En el nodo de control, los mensajes de notificación de transacciones de Transaction Manager se envían al servidor ReD Shield. Estos mensajes notifican al servidor ReD Shield de las transacciones que ya han sido procesadas por el sistema Postilion. El servidor ReD Shield realiza **análisis de riesgo casi en tiempo real** sobre estas transacciones. Debido a que el análisis de riesgo se realiza después de que la transacción ya está autorizada, no afecta el resultado de la autorización.

Nota: Al integrar PostilionPRM con ReD Shield, debe configurar intercambios de análisis de riesgos en tiempo real y casi en tiempo real. Todos los mensajes 0100/0200 (mensajes de solicitud) son manejados por el canal en tiempo real, mientras que los mensajes 0220 (avisos independientes) son manejados por el canal de análisis de riesgo casi en tiempo real. ReD Shield no diferencia entre solicitudes en tiempo real y casi en tiempo real.

Flujo de mensajes de análisis de riesgos en tiempo real

El siguiente diagrama y los pasos describen cómo Transaction Manager interactúa con PostilionPRM para realizar un análisis de riesgo en tiempo real en un mensaje 0200 (solicitud de transacción):

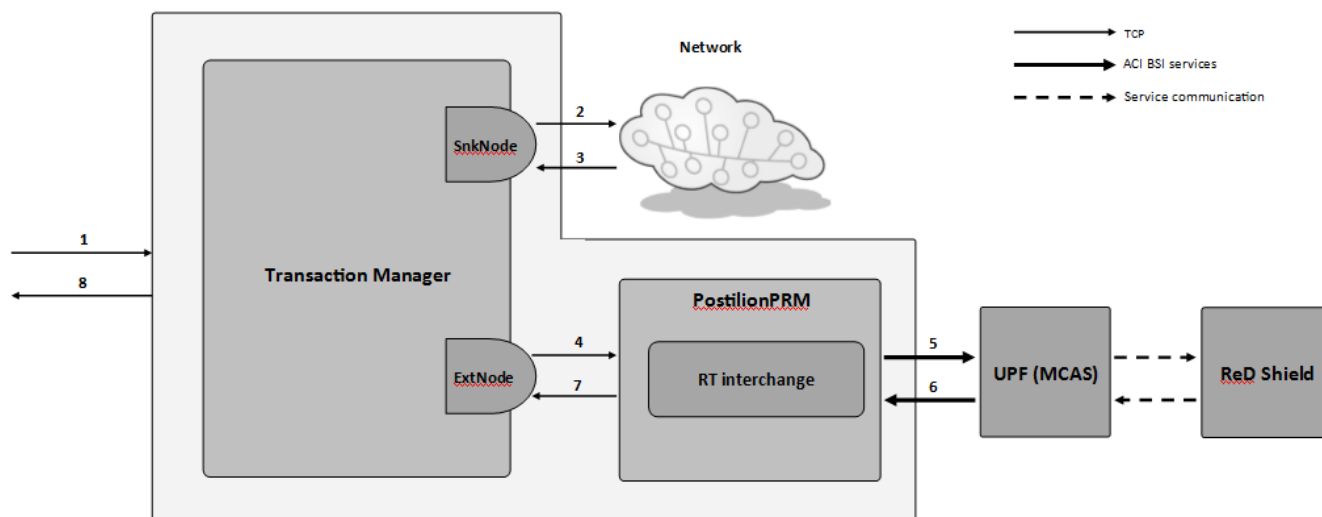


Figura 2: flujo de mensajes en tiempo real

1. Transaction Manager recibe un mensaje 0200 (solicitud de transacción) de un nodo de origen y luego envía el mensaje 0200 al nodo sumidero correspondiente.
2. La interfaz del nodo sumidero envía una solicitud a la entidad ascendente.
3. La interfaz del nodo sumidero recibe una respuesta de la entidad ascendente.
4. Transaction Manager envía un mensaje a la correspondiente **nodo sumidero de procesamiento externo**, que envía un mensaje a PostilionPRM.
5. PostilionPRM envía un mensaje de solicitud de análisis de riesgos en tiempo real a ReD Shield a través de la UPF (MCAS).
6. ReD Shield envía una respuesta de análisis de riesgo. PostilionPRM recibe esta respuesta de ReD Shield a través de la UPF (MCAS).
7. PostilionPRM envía un mensaje 0210 (respuesta de solicitud de transacción) a Transaction Manager.
8. Transaction Manager envía el mensaje 0210 al nodo de origen.

Nota: El flujo anterior representa un nodo sumidero de procesamiento externo configurado para el análisis de riesgo posterior a la autorización. Si se configura el análisis de riesgo de autorización previa, el análisis de riesgo se realizará antes de enviar la solicitud a la entidad ascendente.

Flujo de mensajes de análisis de riesgos casi en tiempo real

El siguiente diagrama y los pasos describen cómo Transaction Manager interactúa con PostilionPRM para realizar un análisis de riesgo casi en tiempo real en un mensaje 0220 (solicitud de transacción).

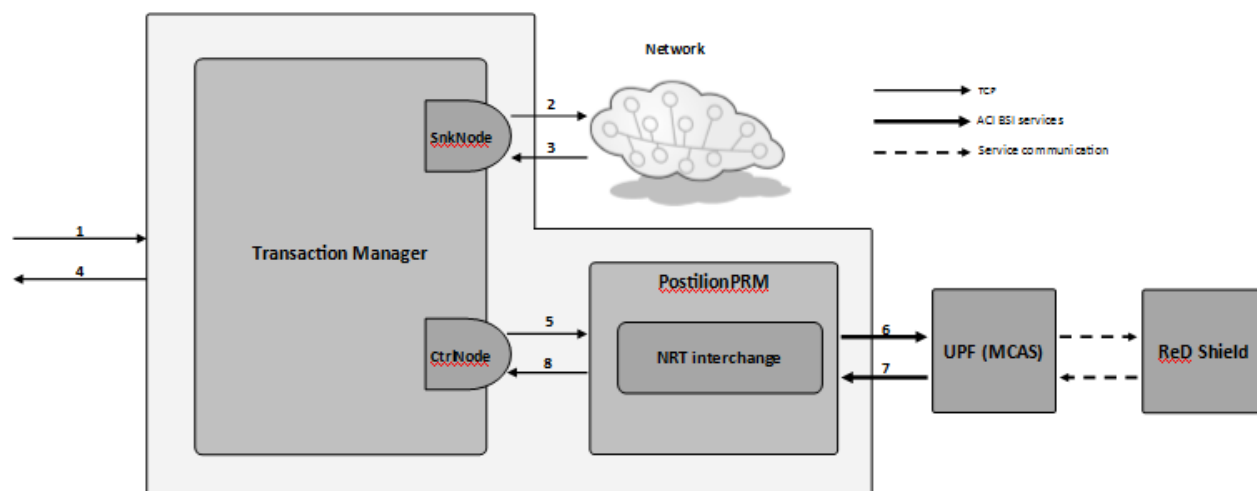


Figura 3: Flujo de mensajes casi en tiempo real

1. Transaction Manager recibe un mensaje 0220 (consejo de transacción) de un nodo de origen y luego envía el mensaje 0220 al nodo sumidero aplicable.
2. La interfaz del nodo sumidero envía una solicitud a la entidad ascendente.
3. La interfaz del nodo sumidero recibe una respuesta de la entidad ascendente.
4. Transaction Manager envía un mensaje 0230 al nodo de origen.
5. Transaction Manager envía un mensaje 9220 (notificación de transacción) a la interfaz del nodo sumidero de PostilionPRM. El intercambio está asociado con un nodo sumidero que está configurado como un **nodo de control** para la ruta seleccionada para el mensaje 0220, y proporcionará un servicio RetailPaymentsRiskAnalyze casi en tiempo real (NRT).
6. PostilionPRM envía un mensaje a través de la UPF (MCAS) a ReD Shield para el análisis de riesgos.
7. PostilionPRM recibe una respuesta de análisis de riesgo de ReD Shield a través de la UPF (MCAS).
8. PostilionPRM envía un mensaje 9230 (respuesta de notificación de transacción) a Transaction Manager.

Descripción general del servicio

ReD Shield está integrado con la interfaz de PostilionPRM mediante el servicio RetailPaymentsRiskAnalyze. Este servicio habilita el componente de alto nivel Análisis de riesgo de pagos minoristas. Consulte la sección "Resumen" de la *Guía del usuario de PostilionPRM* para obtener más detalles sobre cada componente de alto nivel.

Servicio RetailPaymentsRiskAnalyze

El servicio RetailPaymentsRiskAnalyze lo proporciona ReD Shield a través de UPF (MCAS) y lo utiliza la interfaz PostilionPRM para realizar análisis de riesgo en las transacciones que procesa el sistema Postilion. PostilionPRM puede realizar análisis de riesgo casi en tiempo real y en tiempo real cuando está completamente integrado con ReD Shield y UPF (MCAS).

Limitaciones

Sistema operativo

La integración de PostilionPRM y ReD Shield solo se admite en un sistema operativo Windows.

Servicio de Modificación del Estado de la Tarjeta

Escudo rojo **haceno** admitir el servicio de modificación del estado de la tarjeta que ofrece PostilionPRM.

Servicio de carga de datos demográficos

Escudo rojo **haceno** Admite extracciones y cargas de datos demográficos. Como tal, el trabajo programado *PostilionPRM - Extracto - Datos demográficos*, que se instala con PostilionPRM, debe ser **deshabilitado manualmente**. Ver el *Guía del usuario de Realtime Framework* para obtener información sobre cómo deshabilitar trabajos programados.

Prevención de duplicación de registros

ReD Shield no admite múltiples solicitudes de análisis de riesgo para la misma transacción. Para evitar la duplicación de registros, los nodos de control configurados con PostilionPRM deben configurarse con el *Límite de transmisión de cola de almacenamiento y reenvío* opción de nodo sumidero establecida en 1.

Activo/ activo con UPF (MCAS)

La conmutación por error automática de un servidor UPF (MCAS) a otro solo se admite cuando se utiliza la configuración BSI del Registro de servicio estático (SSR). El archivo de respuesta de Service Configurator para ReD Shield solo admite una única ubicación de conmutación por error. Comuníquese con su proveedor de soporte principal si se requieren más ubicaciones de conmutación por error.

Cuando se especifica una ubicación de conmutación por error en el archivo de respuesta, la selección de ubicación se configurará como *primero disponible*. Esta es una configuración de BSI opcional que permite que la interfaz de PostilionPRM use siempre la ubicación principal de UPF (MCAS) y solo use la segunda o las ubicaciones restantes si todas las ubicaciones anteriores no están disponibles. Esto significa que el servidor UPF (MCAS) configurado como *servicios.venta minoristapagosanálisisderiesgo.consumidores* en el archivo de respuesta de Service Configurator siempre se utilizará cuando ambas ubicaciones estén en línea. El servidor UPF (MCAS) configurado como

services.retailpaymentsriskanalyze.consumer.failover solo se usará cuando el principal se desconecte. A partir de entonces si *servicios.venta minorista pagos análisis de riesgo.consumidor* vuelve a estar en línea, se le volverán a enviar todas las solicitudes de procesamiento externo.

Sección 2: Configuración del servicio

El servicio de PostilionPRM se configura mediante el asistente del configurador de servicios. Este asistente creará o actualizará los archivos de configuración necesarios para habilitar la comunicación con UPF (MCAS) y ReD Shield. Consulte la sección "Configuración del servicio" en la *Guía del usuario de PostilionPRM* para obtener información sobre cómo configurar el servicio PostilionPRM. Tenga en cuenta que ejecutar el Configurador de servicios anulará cualquier configuración personalizada manual realizada en los archivos de configuración.

Las siguientes propiedades deben configurarse en el archivo de respuesta apropiado:

Propiedad	Ajuste
service.serviceregistry.type	Ajustado a estático . Esto indicará que PostilionPRM debe conectarse a través de un Registro de servicios estáticos (SSR) al consumir o proporcionar servicios.
services.risk.engine.type	Ajustado a RS . Esto indicará que PostilionPRM se integrará con Escudo rojo .
services.primary.siteid	Propiedad opcional para configurar el ID del sitio donde se encuentra el servidor primario UPF (MCAS). El valor predeterminado es "Sitio1". Este valor debe alinearse con el sitio del proveedor configurado en Platform Manager. Ver el " Configuración UPF (MCAS) sección " para más detalles
services.retailpaymentsriskanalyze.providerid	Propiedad opcional para configurar el ID del proveedor. El valor predeterminado es "Análisis de riesgo de pagos minoristas 1". Este valor debe alinearse con la identificación del proveedor configurado en Platform Manager. Ver el " Configuración UPF (MCAS) sección " para más detalles
services.retailpaymentsriskanalyze.consumer.address services.retailpaymentsriskanalyze.consumer.port	<i>habla a</i> debe ser el nombre de host remoto o la dirección IP donde PostilionPRM debe enviar solicitudes para este servicio <i>Puerto</i> debe ser el puerto configurado para el servicio RetailPaymentsRiskAnalyze proporcionado por el servidor ReD Shield.

<p>servicios.pagos.minoristasanalizar.el.riesgo.del.consumidor.conmutación.por.error. habla a</p> <p>servicios.pagos.minoristasanalizar.el.riesgo.del.consumidor.conmutación.por.error. Puerto</p>	<p>Propiedades opcionales para configurar el sitio de conmutación por error. Si no se requiere conmutación por error para este servicio, deje estos valores de propiedad en blanco.</p> <p><i>habla a</i> debe ser el nombre de host remoto o la dirección IP donde PostilionPRM debe enviar solicitudes para este servicio</p> <p><i>Puerto</i> debe ser el puerto configurado para el servicio RetailPaymentsRiskAnalyze proporcionado por el servidor ReD Shield.</p>
<p>services.retailpaymentsriskanalyze.response.address</p> <p>servicios.retailpaymentsriskanalyze.response.port</p>	<p><i>habla a</i> debe ser el nombre de host accesible externamente o la dirección IP del sistema donde está instalado PostilionPRM.</p> <p><i>Puerto</i> debe ser cualquier puerto no utilizado al que se pueda acceder desde el sistema UPF (MCAS).</p>

Seccion 3:Configuración UPF (MCAS)

UPF (MCAS) se comunica con el sistema ReD Shield para proporcionar la interfaz PostilionPRM con el servicio RetailPaymentsRiskAnalyze. Para que la interfaz de PostilionPRM se integre correctamente con ReD Shield, PostilionPRM debe estar configurado para comunicarse con UPF (MCAS).

El ID de aplicación de PostilionPRM debe configurarse en Platform Manager for UPF (MCAS) para reconocer a PostilionPRM como consumidor. Un ID de aplicación se configura como un subconjunto de un ID de sitio existente mediante Platform Manager. El valor predeterminado para el ID de aplicación de PostilionPRM es "PostilionPRM".

El ID del sitio y el ID del proveedor configurados en el archivo de respuesta del configurador de servicios deben tener el mismo valor (distingue entre mayúsculas y minúsculas) que en Platform Manager. Sus valores deben alinearse con lo que está en la columna "Id. del proveedor" y la columna "Sitio" en Platform Manager, como se muestra en la Figura 4. Consulte el "[Configuración del servicio](#)" para saber cómo configurar el ID del sitio y el ID del proveedor en PostilionPRM.

Load Generation

Security Devices

File Loads

Batch File Control

Logs

Statistics

SSL

Tx Tracing

Dynamic Service Registry

Scheduling Service

Monitor & Management

Provisioning

Notification Services

Application Id.	Provider Id.	RE	EN	Look-ups	Site	URL	ONL	Successful Notifications	Last Notification

15:24:34

0 : 0

Providers

Service	Provider Id.	URL	Site	Application Id.	UPF ...	RE	EN	Look-ups	Se...	Instanc...	UPF Endpoint	Start Ver...	End Versi...
RetailPaymentsRiskAnalyze	RetailPaymentsRiskAnalyze1	bsi:tcpip://172.16.120.74:8101	Site2	UPP		Y	Y	0	RPR...	UPP		1	1
RetailPaymentsRiskAnalyze	S_RPRA	bsi:tcpip://10.13.24.97:5001	Site2	UPP	RPRA	Y	Y	0				1	1

15:24:34

0 : 2

Consumers

Consumer Id.	Application Id.	URL	Look-ups	Site	RE	EN
PostilionPRM	PostilionPRM	bsi:tcpip://172.16.120.74:3136	4	Site2	Y	Y
UPP	UPP	bsi:tcpip://10.13.24.97:5001	0	Site2	Y	Y

Figura 4: Ejemplo: administrador de plataforma UPF (MCAS) configurado

Nota: Es posible configurar PostilionPRM para usar el registro de servicio dinámico (DSR) para conectarse a UPF (MCAS). Sin embargo, se recomienda utilizar el registro de servicio estático (SSR).

Conexión del registro de servicios estáticos

La configuración del servicio para la interfaz de PostilionPRM es necesaria para que PostilionPRM se conecte correctamente al registro de servicio estático (SSR) en la UPF (MCAS). Las siguientes propiedades deben configurarse en el archivo de respuesta para reflejar la dirección y el puerto correctos en los que el servicio SSR está escuchando en UPF (MCAS):

- `servicios.pagos.minoristasanálisis.de.riesgos.dirección.del.consumidor`
- `services.retailpaymentsriskanalyze.consumer.port`

Consulte "Configuración del servicio" en esta guía y la sección "Configuración del servicio" en la *Guía del usuario de PostilionPRM*, para más información.

Conexión del registro de servicios dinámicos

La configuración del servicio para la interfaz de PostilionPRM es necesaria para que PostilionPRM se conecte correctamente al Registro de servicios dinámicos (DSR) en UPF (MCAS). Las siguientes propiedades deben configurarse en el archivo de respuesta para reflejar la dirección y el puerto correctos en los que el servicio DSR está escuchando en UPF (MCAS):

- `services.dynamicserviceregistry.address`
- `services.dynamicserviceregistry.port`

Consulte "Configuración del servicio" en esta guía y la sección "Configuración del servicio" en la *Guía del usuario de PostilionPRM*, para más información.

Sección 4: Configuración de intercambio

Selecciona el **Intercambios** en el configurador de aplicaciones Realtime para configurar la interfaz PostilionPRM dentro del sistema Postilion.

Servicio RetailPaymentsRiskAnalyze

PostilionPRM se puede configurar para consumir el servicio RetailPaymentsRiskAnalyze para realizar análisis de riesgo casi en tiempo real. Se debe configurar un único intercambio para cada consumidor de servicios.

Nota: Antes de configurar los intercambios de PostilionPRM, los nodos sumideros que se utilizarán para el análisis de riesgos ya deben estar configurados en el *Gerente de transacciones* consola en Realtime Framework, y se debe tener en cuenta lo siguiente:

- Un **nodo sumidero de procesamiento externo** debe estar configurado para el canal de análisis de riesgos en tiempo real.
- Un **nodo de control nodo sumidero** debe configurarse para el canal de análisis de riesgos casi en tiempo real.

Tanto los intercambios en tiempo real como en tiempo casi real deben configurarse al integrarse con ReD Shield. ReD Shield admite los siguientes tipos de mensajes en el canal dado:

Tipo de mensaje	Canal
0100	Tiempo real
0200	Tiempo real
9120	Casi en tiempo real
9220	Casi en tiempo real

Actualmente, ReD Shield no admite tipos de mensajes que no sean los especificados anteriormente.

Para configurar un intercambio PostilionPRM, vaya a la **Intercambios** pestaña en la consola de configuración de Aplicaciones y complete los siguientes pasos:

1. Cree una nueva entrada para el servicio RetailPaymentsRiskAnalyze en la categoría Intercambios:

Variable	Ajuste
Interfaz	Seleccione <i>PostillónPRM</i>
Intercambio	Proporcione un nombre para el intercambio. Por ejemplo, <i>PostAuthRiskAnalyze</i> .
Parámetros de usuario	<p>Nota: Los parámetros deben especificarse mediante la siguiente plantilla y deben utilizar las claves predefinidas donde los valores deben estar encapsulados entre comillas simples y separados por una coma. Por ejemplo, <i>clave1='valor1', clave2='valor2', clave3='valor3'</i>.</p> <ul style="list-style-type: none"> Proporcione el ID de la institución adquirente (longitud variable de hasta 11 caracteres) que se usará para identificar las transacciones del adquirente en PostilionPRM. Por ejemplo, <i>AcquiringInstId='ACQ00001'</i>. Consulte la sección "Identificación de mensajes" en la <i>Guía del usuario de PostilionPRM</i> para más información. <Opcional>: Proporcione el valor del identificador del servidor (longitud variable de hasta 4 caracteres) que se usará para identificar al socio activo/activo que envía las transacciones a PostilionPRM. El valor debe configurarse de forma única entre los socios activos/activos. Por ejemplo. <i>ID del servidor = 'PST1'</i> y <i>ID del servidor = 'PST2'</i>. <Opcional>: Proporcione el valor del sistema de gestión de riesgos que se utilizará para identificar qué sistema de gestión de riesgos utilizar. <i>Sistema de gestión de riesgos = 'RS'</i> debe especificarse al integrarse con ReD Shield. Si no se especifica este parámetro, el valor del parámetro predeterminado de <i>Sistema de gestión de riesgos = 'PRM'</i> se utilizará.
Nodo sumidero	<p>Seleccione el nombre de un nodo sumidero creado en el Nodos sumideros página de Transaction Manager Configurator.</p> <p>Nota: Asegúrese de elegir el nodo sumidero correcto. Si el intercambio está configurado para realizar casi en tiempo real análisis de riesgo, entonces el nodo sumidero debe configurarse como un nodo de control. Si el intercambio está configurado para realizar tiempo real análisis de riesgo, entonces el nodo sumidero debe configurarse como un nodo de procesamiento externo. El tipo de procesamiento externo en el nodo sumidero de procesamiento externo se puede establecer en <i>Análisis de riesgo de preautorización</i> o <i>Análisis de riesgo posterior a la autorización</i>. Consulte las secciones sobre configuración de nodos en la sección "Configuración de enrutamiento" del <i>Guía del usuario de PostilionPRM</i> para más información.</p>

2. Cree un punto de acceso al servicio (SAP) en el **SAP** categoría para cada entrada de servicio RetailPaymentsRiskAnalyze configurada en el paso anterior:

Variable	Ajuste
SAVIA	Cualquier nombre. Sugerencia: Utilice el mismo nombre que el utilizado para el intercambio. Por ejemplo, <i>PostAuthRiskAnálisis</i> .
Escribe	Selecione cliente .
Protocolo	Selecione Protocolo Genérico .
Clase de fábrica de SAP Nombre	Ingresa <code>postilion.realtime.postilionprm.ipc.SapFactory</code>
Habla a	deja esto en blanco
Datos de configuración	Ingresa <code>postilion.realtime.postilionprm.service.retailpaymentsriskanalyz e.RPRAProxyDriver</code> . Esto configura un consumidor del servicio RetailPaymentsRiskAnalyze para configurar ReD Shield para realizar análisis de riesgo.

3. Cree una conexión para el cliente SAP configurado para la entrada de servicio RetailPaymentsRiskAnalyze:

Variable	Ajuste
Dirección	Selecione Doble
Prioridad	Selecione Elevado
Conecte bajo demanda	No habilite esta opción (el valor predeterminado es discapacitado)
Tiempo de espera de conexión	Ingresa <code>0</code>
tiempo de inactividad	Ingresa <code>0</code>
Habla a	Ingresa <code>RetailPagosRiskAnalyze</code> como el nombre del servicio
Datos de configuración	deja esto en blanco

Mapeador de campo genérico

Las ubicaciones de algunos campos de origen en los mensajes a la aplicación PRM (que se copiarán en ubicaciones en el mensaje a ReD Shield) son configurables. Consulte la sección "Configuración del mapeador de campo genérico" en la *Guía del usuario de PRM* para obtener instrucciones sobre cómo configurar estas asignaciones de campo para adaptarse a la configuración particular del sistema. Si no se realiza esta configuración, se utilizarán las ubicaciones de origen predeterminadas para estos campos.

Sección 5: Configuración activo/activo

Las interfaces de PostilionPRM se pueden conectar a una única instancia de UPF (MCAS) o a varias instancias de UPF (MCAS).

Para cada instancia de UPF (MCAS) a la que se conecta PostilionPRM, configurar el lado de Postilion implica ejecutar el configurador de servicios para duplicar la configuración en cada socio activo/activo de Realtime. Consulte los pasos descritos en la sección "Configuración del servicio" del *Guía del usuario de PostilionPRM* para más detalles.

Las secciones "Configuración del configurador de servicios" e "Identificación del servidor" de esta guía describen los requisitos para activo/activo.

Nota: Para que estos cambios surtan efecto, deberá RESINCRONIZAR. Ver el *Guía del usuario de Realtime Framework* para obtener más información sobre cómo realizar una resincronización.

Configuración del configurador de servicios

Se puede configurar una interfaz PostilionPRM para comunicarse con múltiples instancias UPF (MCAS). Esta configuración es opcional.

Nota: Ver el "[Configuración del servicio](#)" para obtener detalles sobre la configuración de una instancia UPF de conmutación por error (MCAS).

Identificación del servidor

Para que las instancias de PostilionPRM activas/activas realicen transacciones con ReD Shield, se debe configurar un identificador para cada uno de los socios activos/activos. PostilionPRM lo utiliza internamente para que las transacciones de cada uno de los socios activos/activos se identifiquen de forma única. Se debe proporcionar un valor de identificación de servidor único en el parámetro de usuario para cada socio.

Ver el "[Configuración de intercambio](#)" para obtener más información sobre cómo configurar los parámetros de usuario para el servicio RetailPaymentsRiskAnalyze.

Coordinación activa/activa y recuperación de fallas

Se admite la conmutación por error automática de una instancia principal a una UPF asociada (MCAS). Sin embargo, existen algunas limitaciones en este proceso. Ver el "[Limitaciones](#)" para más información.

Sección 6: configuración SSL

Se recomienda que toda la comunicación entre PostilionPRM y la UPF (MCAS) sea segura ya que contiene datos que podrían considerarse sensibles. PostilionPRM admite el uso de SSL/TLS para proteger las comunicaciones.

La comunicación para cada sistema se divide en dos canales distintos. Un canal entrante (servidor) que se usa para recibir mensajes y un canal saliente (cliente) que se usa para enviar mensajes. Se puede utilizar un único certificado SSL para proteger ambos canales de comunicación en el sistema PostilionPRM. Este es el enfoque recomendado, pero también se admite el uso de certificados SSL independientes para los canales de cliente y servidor.

La configuración debe realizarse tanto en PostilionPRM como en UPF (MCAS) para realizar el cifrado SSL. Para la configuración específica de PostilionPRM, consulte las secciones "Configuración del servicio" y "Configuración de SSL/TLS" en el *Guía del usuario de PostilionPRM*

Para la configuración específica de UPF (MCAS), consulte la "Configuración de SSL" sección de la *Guía de operaciones de la UPF*.

Sección 7: Configuración opcional

Configuración de rastreo

El seguimiento se puede habilitar para eventos relevantes para la interfaz de PostilionPRM. Los siguientes tipos de eventos se registran en las trazas de Postillón y UPF (MCAS):

- Eventos de postillón
- Eventos de infraestructura de servicios empresariales (BSI)
- Eventos UPF (MCAS)

Ver el *Guía del usuario de Realtime Framework* para obtener más información sobre la configuración de las propiedades del sistema.

Seguimiento de eventos de postillón

Para habilitar el seguimiento, configure la siguiente propiedad del sistema:

Solicitud	Nombre de propiedad del sistema	Descripción
PostillónPRM	postilion.env.enable_tracing_at_startup	Ajustado aciertop para habilitar el rastreo.

Seguimiento de eventos de infraestructura de servicios empresariales

La interfaz PostilionPRM utiliza el marco BSI para consumir y proporcionar servicios empresariales. Los eventos detallados generados por el marco BSI se pueden rastrear mediante la interfaz de PostilionPRM. La siguiente propiedad del sistema se utiliza para determinar si estos eventos detallados deben incluirse en los seguimientos de la aplicación.

Solicitud	Nombre de propiedad del sistema	Descripción
PostillónPRM	postilionprm.bsi.include_detailed_tracing	Ajustado aciertop para indicar que los eventos BSI detallados deben incluirse en el seguimiento de la aplicación. Nota: Este comportamiento se puede controlar en tiempo de ejecución con un comando SET.

Rastreo de eventos de Universal Payments Framework

Consulte la sección "Mensajes de seguimiento" de la *Guía de Seguimiento de Mensajes UPF* para obtener más información sobre cómo habilitar y configurar el seguimiento de mensajes en Platform Manager. El seguimiento de mensajes es el proceso de capturar información adicional sobre lo que ocurre durante el procesamiento de mensajes. La información capturada durante el seguimiento ayuda a solucionar problemas y confirma que los mensajes son

procesado como se esperaba y como se define por las reglas de negocio. Platform Manager es la interfaz utilizada para crear, personalizar, habilitar, deshabilitar, iniciar y detener un seguimiento.