



ATIOnet Local Agent

Acerca de: Este documento describe las características técnicas del aplicativo **Ationet Local Agent**, para facilitar la evaluación de los requerimientos de instalación y operación, por parte de una organización de TI.

Información del Documento	
File:	AN-Local Agent-GuiaEvaluacion
Versión del documento:	1.0
Fecha documento:	05/Jul/2015
Autor:	ATIO International LLC

Registro de cambios		
Ver.	Fecha	Resumen del cambio
1.0	05/Jul/2015	Versión inicial

Contenidos

- Introducción
- Escenarios de Despliegue
- Tecnología
- Soporte de datos
- Conectividad y Mensajería
- Seguridad
- Logs de Ejecución
- Instalación
- Soporte

Introducción

El Local Agent de ATIONet es una pieza de software que actúa como proxy en la comunicación entre algunos Sistemas de Captura (SdC) y ATIONet. Adicionalmente, el Local Agent puede proveer un soporte de autorización fuera de línea cuando la conexión a internet no está disponible.

El Local Agent de ATIONet se provee como un componente adicional, dependiendo de las características y necesidades del sitio o red de sitios y está disponible como un paquete de software o como un integrado hardware y software, preinstalado y pre-configurado por un Distribuidor certificado de ATIONet.

ATIONet Local Agent brinda los siguientes servicios al Sistema de Captura:

- **Servicio de Proxy al Host ATIONet con conversión de protocolo.** El SdC se conecta al Local Agent en una LAN, WAN, o VPN vía sockets de TCP/IP y este reenvía la mensajería en línea utilizando el protocolo Nativo de ATIONet con encriptación SSL.
- **Autorización Offline.** En caso de caída del vínculo con internet, si está habilitado, el Local Agent puede autorizar localmente las transacción del SdC, que quedan encoladas hasta que se restablezca la comunicación. En cuanto se soluciona el inconveniente, la re-sincronización de transacciones encoladas y actualización de saldos se realiza automáticamente. Este mecanismo hace que la caída y recuperación pasen inadvertidas al SdC.

Escenarios de Despliegue

ATIONet Local Agent es capaz de atender a varios sistemas de captura a la vez, esto da flexibilidad a la hora de definir la topología de la red. La regla general es que, por ser un proxy, el Local Agent debe ser instalado entre el SdC e internet. Entre el SdC y el Local Agent debe existir un acceso IP directo, sea físico o virtualizado; entre el Local Agent e Internet puede existir cualquier clase de conectividad que permita conexión HTTP/HTTPS con el Host de ATIONet.

Local al Sistema de Captura

En este caso, el Local Agent atiende a un solo SdC. Es el escenario más común, donde hay un solo puesto de abastecimiento en la locación, y la salida a internet es directa desde la locación.

Remoto al Sistema de Captura

Típicamente, hay dos escenarios que llevan a esta topología. En primer lugar, que las condiciones físicas del sitio no soporten la instalación local de un sistema PC, ni siquiera en la variante de integrada HW/SW en un PC industrial, o bien que las políticas de TI de la organización no lo admitan. En segundo lugar, es que en la misma locación haya múltiples estaciones de abastecimiento, cada una con su propio SdC, y se instale una única instancia del Local Agent controlando todos los SdC. Usualmente en esta variante, el Local Agent se instala en un servidor corporativo, bajo política de la organización.

En este caso, si el vínculo interno entre el SdC y el Local Agent se interrumpe, la operación no se beneficiará del mecanismo Offline.

Tecnología

El Local Agent de ATIONet es un programa Windows x86, compatible con sistemas operativos de 32 y 64 bits, que se instala como un servicio windows de inicio automático. Presenta bajos requerimientos de hardware, siendo capaz de ejecutarse en un procesador Atom dual-core con 1GB de memoria RAM; los requerimientos de disco son verdaderamente nominales, la imagen del aplicativo instalado es de menos de 20MB. El paquete completo se instala de manera desatendida y opera sin ninguna interface de usuario, ya que no requiere ninguna clase de gestión o mantenimiento.

Características

Característica	Descripción
Sistema Operativo	Windows 7 o superior 32/64bits
	Windows Server 2012 o superior 32/64bits
Memoria	1 Gb
Disco	15 Mb
RDBMS	SQL Server Express 2008 R2
Lenguaje	C#
Pre-requisitos	.net 4.5, Windows Installer
Instalador	Silencioso, con archivo de pre-configuración 1.6MB
Servicio	ATIONet Local Agent Service
Conectividad	Local: Socket TCP en el puerto 33173
	Internet: HTTPS con SSL

El SQL Server Express y el Framework .net 4.5 son instalados por el instalador de la aplicación.

Soporte de datos

El servicio del ATIONet Local Agent requiere como mínimo una instancia SQL Server Express 2008 R2. Como parte de las medidas de seguridad y robustez del aplicatvo, el instalador siempre genera una instancia separada de SQL para uso propio y exclusivo del aplicativo. Esta instancia se configura con seguridad *mixta*, se le deniega el acceso a los grupos administrativos del sistema operativo y se establece una contraseña de *sa* que sólo el aplicativo conoce y que se almacena por separado y en forma encriptada.

En caso de detectarse problemas con la base de datos o en oportunidad de un cambio de versión que incluya cambios en el modelo de datos, el instalador tiene la lógica necesaria para borrar y volver a generar la base desde cero en forma completamente desatendida.

Conectividad y Mensajería

El servicio del ATIONet Local Agent establece dos vínculos de comunicación, uno con el Sistema de Captura y otro con el Host de ATIONet.

- **Sistema de Captura:** El servicio levanta un servidor de sockets de TCP/IP y lo mantiene abierto durante toda la operación. El puerto es configurable, y por defecto se establece en el puerto 33173 de TCP.
- **Host ATIONet:** Entre el servicio ATIONet Local Agent Service y el Host ATIONet se mantienen varias clases de intercambios, todos a través de mensajes HTTPS encriptados por SSL.
 - **Transacciones:** Mensajes encriptados HTTPS de formato JSON con los requerimientos y respuestas de transacciones originadas en el SdC y retransmitidas por el Local Agent. Estos mensajes incluyen tanto transacciones en línea como el envío de transacciones encoladas, como parte de la recuperación luego de operar con autorización local Offline. A demanda.
 - **HeartBit:** Mensaje tipo ECHO que permite al Host saber el estado de conectividad de los sitios. Configurable, por defecto cada 1 minuto.
 - **Consulta Offline:** Mensaje de consulta de novedades offline. Por esta mensajería, el Local Agent, obtiene la lista de paquetes de datos offline que debe descargarse. Cada 15 minutos.
 - **Descarga Offline:** Descarga de paquetes de datos Offline para autorización local, según el resultado de la consulta de novedades.

Seguridad

El ATIONet Local Agent fue diseñado como un proxy, y autorizador en contingencia offline para el procesamiento de transacciones de entrega y pago de medios de pago privados, por esto se incluyeron una serie de medidas de seguridad propias de un gateway de pago.

- **Encriptación de datos sensibles en la base:** Tanto los balances, como los datos sensibles de tarjetas y vehículos, se almacenan protegidos mediante encriptación o *hashing*.
- **Transacciones:** Las transacciones autorizadas localmente durante una contingencia Offline son guardadas temporalmente en la base de datos de manera encriptada, y son eliminadas de manera segura inmediatamente después de que se confirma la recepción por el Host de ATIONet.
- **Logs:** En los niveles más altos de logeo donde se incluye información de transacciones, las tramas de los mensajes se muestran encriptados para evitar el acceso a los datos sensibles de las tarjetas, balances y cuentas.
- **Archivo .app.config encriptado:** El archivo de configuración de las aplicaciones .net contiene información que puede ser sensible en cuanto a seguridad, por ejemplo los datos de conexión a la base. En el ATIONet Local Agent Service, el *app.config* se mantiene encriptado con claves generadas por el mismo aplicativo.

Logs de Ejecución

El servicio ATIONet Local Agent Service genera un log técnico que puede ser configurado en el Install.config en varios niveles:

FATAL, ERROR, WARN, INFO, DEBUG, ALL Es común operar permanentemente en ALL ya que en este nivel se registran las entradas de todo tipo y aún así el log habitualmente suma 10MB por día.

La configuración del log permite establecer límites de cantidad de archivos para que se depuren automáticamente.

El log se guarda en una carpeta \Logs bajo la carpeta de instalación del aplicativo; los archivos tienen el siguiente formato:

service_aaaamdd.log

Instalación

El mismo proceso de instalación sirve para instalar el producto desde cero o para hacer una actualización de versión.

El paquete de instalación está compuesto por los siguientes componentes:

- **Setup:** Es el paquete de instalación propiamente dicho, en formato de archivo ZIP
- **install.config** Es un archivo de configuración específico para cada sitio, que contiene todos los parámetros necesarios para la operación. Este archivo no es trasladable a otras instalaciones y sólo puede ser generado por el Distribuidor ATIONet a cargo de la instalación.
- **Prerequisitos:** [Opcional] Son los instaladores estándares de SQL Server Express 2008 R2, Windows Installer y .net Framework 4.5

Proceso de instalación

Una vez descargado el paquete de instalación (opcionalmente con sus pre-requisitos), se ejecuta el Setup.exe. El Setup puede correr en modo silencioso o bien solicitar: (a) confirmación de la creación de una nueva instancia de SQL, si es que ya encuentra un motor instalado y (b) la ubicación del archivo install.config

El resto de la instalación se completa sin intervención del usuario, e incluye la creación e inicio del servicio windows.

Si el sitio ATIONet que tiene configurado el Local Agent posee Offline, inmediatamente se comienza con la bajada y aplicación de paquetes de datos Offline.

Soporte

El soporte a una instancia de ATIONet Local Agent es en general prestado por el Distribuidor ATIONet en los niveles 1 y 2, y directamente por ATIONet en el nivel 3.

Para el reporte de un problema con el servicio usualmente sólo es necesario indicar la falla detectada y enviar el archivo log correspondiente al día en que se produjo la falla.

Todos los datos contenidos en la base de datos son regenerables por el instalador con un archivo Install.config, excepto por las transacciones autorizadas fuera de línea que no hubieran llegado aún al Host ATIONet; aunque dado que el acceso a la base tiene un doble mecanismo de seguridad (clave de sa de SQL generada por sistema y tabla de transacciones encriptada), esto es un proceso de excepción y que sólo puede ser ejecutado directamente por nivel 3 de ATIONet.

Para darle mayor fluidez al proceso de soporte y despliegue de actualizaciones, se requiere acceso de control remoto al PC que corra el servicio. Se recomienda que este acceso esté configurado, pero solo habilitado temporalmente cuando se lo solicite y debe cumplir con los requerimientos de seguridad de la organización.

Documentación complementaria: AN-Native_Offline-TechGuide. Guía de funcionamiento del mecanismo de autorización Offline.