

White Paper de Seguridad

El Agente HelloID

Tabla de Contenido

Introducción	3
Instalación, verificación y comunicación del Agente	3
Configuración	4
Verificación.....	4
Comunicación	4
Los servicios del Agente	4
Access Management	4
Provisioning	5
Service Automation.....	5



Introducción

HelloID es una plataforma Cloud de gestión de identidades (IDaaS). Ésta facilita el control de acceso (SSO y MFA) y el aprovisionamiento de cuentas de usuarios en los sistemas y aplicaciones de servicios informáticos.

Si la infraestructura informática de su compañía ya es 100% cloud, HelloID puede funcionar sin ningún componente on-premise. Pero si tiene infraestructura on-premise HelloID permite instalación de **Agentes** on-premise.

El Agente es un conjunto de tres pequeños servicios Windows que se instalan en la red de su compañía. Estos permiten la comunicación con HelloID. En otras palabras, el Agente actúa como un “bróker” que intercambia datos y ejecuta acciones en la red. Esto incluye balanceo de carga, tolerancia a fallos y monitorización.

Este documento describe las medidas de seguridad incorporadas en el Agente y que incluye:

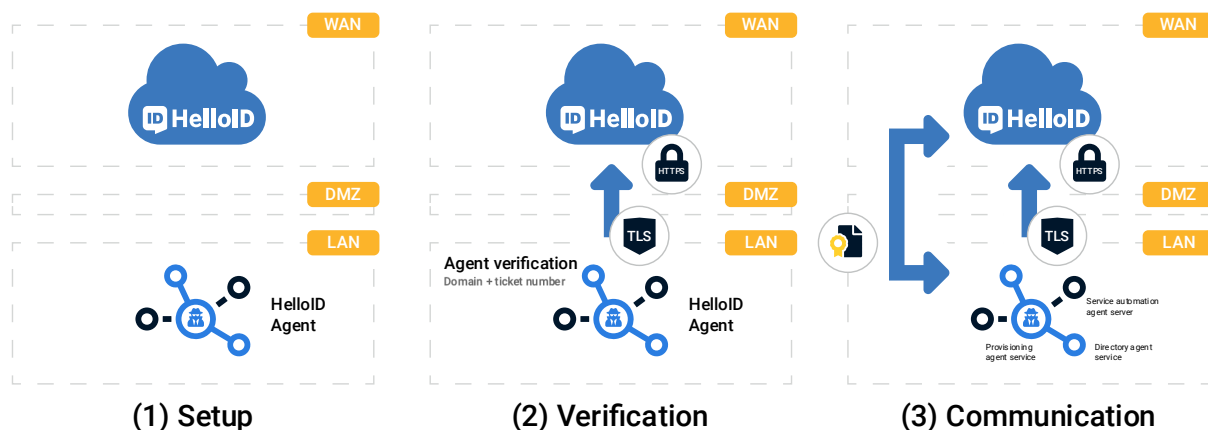
- Verificación de token antes de que tenga lugar cualquier comunicación.
- Comunicación sobre HTTPS con cifrado TLS 1.2.
- Y autenticación basada en certificado para todos los “endpoints”.

Para consultar requerimientos técnicos y procedimientos de instalación del Agente, ir a docs.helloid.com

Instalación, verificación y comunicación del Agente

Inicialmente el portal de HelloID se entrega sin Agente. La configuración de defecto de HelloID es cloud-to-cloud. El Agente solo se instala si HelloID necesita interactuar con recursos locales. (por ejemplo: carpetas compartidas, Active Directory, Exchange, aplicaciones corporativas on-premise, etc...)

El proceso de puesta en marcha en 3 pasos garantiza un canal de comunicación seguro entre HelloID y el Agente:



Configuración

El primer paso es [instalar](#) el Agente en un servidor de la red. Se puede instalar en cualquier servidor del dominio con acceso HTTPS a HelloID. En general, debería ser un servidor que no sea controlador de dominio para evitar conflicto con directivas de seguridad local. Los servicios del Agente se ejecutarán con una cuenta de dominio con derechos suficientes y necesarios para realizar las acciones en los sistemas de la red.

Verificación

A continuación aseguramos que su portal HelloID confíe únicamente con las instancias correctas del Agente. Durante la instalación del Agente, HelloID genera un número de ticket OTP. Este número sólo puede utilizarse una vez y dentro de los 10 minutos a partir de su creación. El Administrador de HelloID introduce este número durante la instalación del Agente. Se genera un certificado compartido basado en la combinación del OTP, la URL del portal y el GUID del Agente. Después, este certificado valida cada intento de comunicación entre el Agente y el portal de HelloID. Si el certificado no coincide, o el GUID del Agente ha cambiado, no es posible la comunicación. Si el certificado o el Agente se copia o mueve, la confianza se revoca de forma inmediata.

Este proceso de verificación sólo puede ser ejecutado por los Administradores de HelloID con permiso para añadir Agentes desde el panel de control de HelloID. Para máxima seguridad, no se permite ningún otro escenario.

Comunicación

Después de la verificación, el portal HelloID y el Agente pueden comunicar. El Agente es pasivo, sólo ejecuta acciones solicitadas por el portal HelloID y no puede enviar comandos al portal. Cuando el Agente responde a una solicitud, el portal HelloID verifica la dirección IP origen. Si no coincide con la IP utilizada durante la verificación, el comando se rechaza y la confianza se revoca de inmediato. No es necesario abrir ningún puerto especial del cortafuego. El Agente se comunica a través del puerto estándar TCP 443. Si su organización tiene un filtro URL, aquí tiene la lista de las URLs que tiene que permitir a los servidores que ejecutan el Agente: [HelloID whitelist domain](#).

Los servicios del Agente

El Agente incluye tres servicios Windows distintos: uno por cada módulo de HelloID (Provisioning, Service Automation, y Access Management). Cada servicio puede ser ejecutado con su propia cuenta de servicio con derechos distintos dependiendo de los requisitos de su compañía.

Access Management

El servicio del módulo AM (HelloID Directory Agent) utiliza HTTPS con “long polling”. Cada solicitud permanece abierta durante 30 segundos. Durante este intervalo, el servicio responde cada cinco segundos con cinco procesos “polling” simultáneos. La mayoría de las solicitudes tienen un tiempo de respuesta inferior a un segundo. Todas las comunicaciones están cifradas con los certificados HelloID vía el protocolo mínimo TLS 1.2. Cada solicitud se verifica basándose en el certificado y el GUID del Agente. Esto asegura que la comunicación sea inmediatamente cancelada si se elimina el Agente desde el panel de control de HelloID. Este servicio está optimizado para la estabilidad.



Provisioning

The Provisioning service uses secure **WebSockets** to maintain open, near real-time communication with HelloID. An initial HTTPS request to the HelloID portal is upgraded to a secure WebSocket. The WebSocket is recycled every three hours, and has a 60-second heartbeat to check whether the connection should remain open. All communication is encrypted with via HelloID certificates via TLS 1.2. Each request is verified based on the Agent certificate and GUID. This service is optimized for near real-time communication, stability, and bulk request performance.

El servicio de Provisioning utiliza **WebSockets** para mantener un canal de comunicación abierto, prácticamente, en tiempo real con el portal HelloID. La solicitud HTTPS inicial al portal HelloID se actualiza en un **WebSocket** seguro. El **WebSocket** se recicla cada tres horas, y tiene un heartbeat cada 60 segundos para verificar si la conexión permanece abierta. Todas las comunicaciones se cifran con los certificados HelloID vía el protocolo mínimo TLS 1.2. Cada solicitud se verifica basándose en el certificado y el GUID del Agente. Este servicio está optimizado para una comunicación en tiempo real, estable y un tiempo de respuesta rápido para solicitudes masivas.

Service Automation

El servicio SA (HelloID SA Agent) comparte las características de seguridad del servicio de Provisioning. Está optimizado para una rápida respuesta a fin de que los usuarios finales tengan una agradable experiencia en el uso de los formularios HelloID.

TOOLS4E SOUTH EUROPE

Dirección: Calle Ramon Turró 169
08005 BARCELONA
ESPAÑA

General : +34 933 93 92 98

Email: sesales@tools4ever.com

