TOOLS4EVER
IDENTITY GOVERNANCE & ADMINISTRATION

Security White Paper

HelloID Agent

Table of Contents

Introduction

HelloID is a cloud-based Identity Management (IDaaS) platform. It facilitates access control (SSO and MFA) and provisions user accounts in IT applications and systems.

If your company is 100% cloud-based, HelloID operates without any on-premise components. But for organizations that still have a local data center, HelloID offers an optional on-premise **Agent**.

Agent is a set of lightweight Windows services installed inside your organization's network. They allow communication with HelloID. In other words, Agent is a "broker" that exchanges data and performs on-premise actions. This includes load balancing, failover, and monitoring.

This document explains the security measures built into Agent, including:

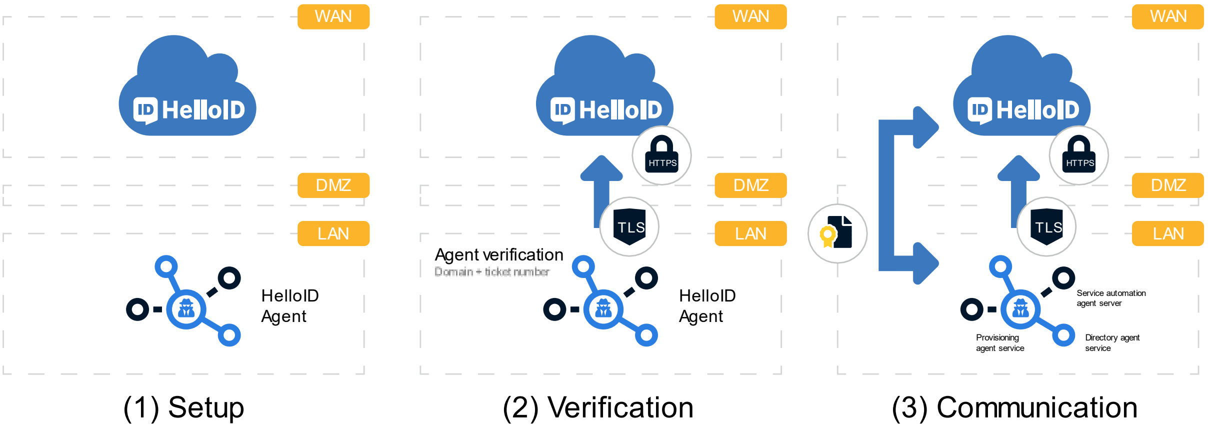
- Token verification before any communication takes place;
- Communication over HTTPS with TLS 1.2 encryption;
- And certificate authentication for all endpoints.

For Agent technical requirements and installation procedures, refer to docs.helloid.com. For more resources including our security whitepaper and Deloitte penetration testing guarantees, visit www.tools4ever.com/resources.

Agent setup, verification and communication

The HelloID portal is initially deployed without an Agent. HelloID's default configuration is purely cloud-to-cloud. Agent is only installed if HelloID must interface with local resources (e.g., filesystem, Active Directory, Exchange).

A 3-step setup process ensures a secure communication path between HelloID and Agent:



(1) Setup (2) Verification (3) Communication

Setup

The first step is to install Agent on a network server. This can be any server in the domain with HTTPS access to HelloID. Typically, it should be a server that is not a domain controller, to avoid conflicts with local security policies. Agent's services will run on a domain account with local admin rights.

Verification

Next, we ensure that your HelloID portal trusts only the correct instance of Agent. During Agent installation, HelloID generates an OTP ticket number. This number can only be used once, and only within 10 minutes of its creation. The HelloID Administrator provides this number to the Agent installer. A shared certificate is generated based on a combination of the OTP, the portal URL, and the Agent GUID. Subsequently, this certificate validates every communication attempt between HelloID and Agent. If the certificate does not match, or the Agent GUID has changed, communication is impossible. If the certificate or Agent is copied or moved, trust is immediately revoked.

This verification procedure can only be performed by HelloID Administrators with permission to add Agents in the HelloID admin dashboard. For maximum security, no other scenario is allowed.

Communication

After verification, the HelloID portal and the Agent can communicate. The HelloID Agent is passive and one-way. It only performs actions requested by the HelloID portal, and cannot send commands to the portal. When Agent responds to a request, HelloID checks the originating IP address. If it does not match the IP used during verification, the command is rejected and trust is immediately revoked. No special firewall port opening or DMZ configuration is required. Agent communicates through the standard TCP port 443.

Agent services

Agent comprises three separate Windows services — one for each HelloID module (Provisioning, Service Automation, and Access Management). Each service can be run under its own account, with differential security settings according to your organization's requirements.

Access Management

The AM service uses HTTPS with **long polling**. Each request stays open for 30 seconds. During this interval, the service responds every five seconds, with five processes polling simultaneously. Most requests are answered in less than one second. All communication is encrypted with via HelloID certificates via TLS 1.2. Each request is verified based on the Agent certificate and GUID. This ensures that communication is immediately halted if Agent is removed in the HelloID admin dashboard. This service is optimized for stability.

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.

Service Automation

The SA service shares the security characteristics of the Provisioning service. It is optimized for quick response time, to make HelloID Forms a snappy experience for end users.