





# Windows Login Agent Introduction

Securing legacy technologies within an organisation's IT infrastructure is a critical yet often overlooked component of cybersecurity. In this whitepaper, we will be exploring the topic in-depth, focusing our analysis onto the innovative Windows Login Agent, a powerful tool designed to enforce Multi-Factor Authentication (MFA) for technologies that are traditionally more challenging to safeguard, such as the Remote Desktop Protocol (RDP) and Physical Console access for Windows Servers and Desktops.

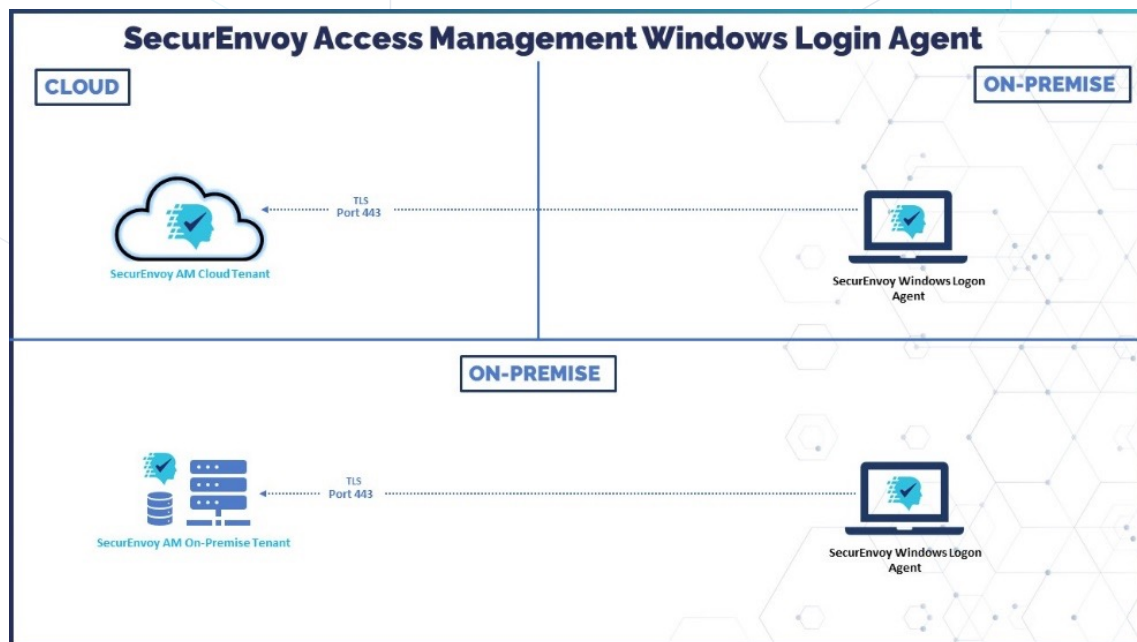
Despite the rapid shift towards cloud-based applications and services, a substantial portion of enterprise operations remains tethered to legacy systems. These systems, while reliable and essential, often lack the modern security features necessary to defend against current cyber threats. As regulatory bodies and cybersecurity upholders of their responsibility to protect data and systems find themselves at a crossroads - raising the question of how to bring indispensable, yet dated, technologies under the protective umbrella of contemporary cybersecurity standards.

The SecurEnvoy Windows Login Agent is a testament to innovation in this realm, bridging the gap between the inherent vulnerabilities of legacy systems and the stringent security protocols necessitated by today's threat landscape. By deploying this agent, organisations can achieve a higher level of security compliance, not merely as a reactionary measure, but as a proactive step towards a more secure and resilient IT environment.

## SecurEnvoy Windows Login Agent Solution Summary

The SecurEnvoy Windows Login Agent is a tool that can be centrally deployed and managed via Windows Servers and Desktops, in both physical and virtual environments.

The Agent can be set up to enforce multi-factor authentication (MFA) at point of login for user access, based on a user group. For example, Administrator Accounts for Remote Desktop Access to Windows Servers can be configured to require MFA.



## Deployment Options

The SecurEnvoy Windows Login Agent can be installed on a single machine or distributed across multiple machines as the preferred deployment method. It can be installed on a single machine or distributed across multiple machines as the preferred deployment method. It can be installed on a single machine or distributed across multiple machines as the preferred deployment method.

For more information on how to install the SecurEnvoy Windows Login Agent, see the SecurEnvoy Windows Login Agent installation guide. This approach is particularly useful for large-scale deployments, ensuring consistent and secure access across the network.

## System Requirements for SecurEnvoy Windows Login Agent

The SecurEnvoy Windows Login Agent (WLA) is extremely lightweight and will run on any hardware specification that meets the minimum requirements for Windows OS.

The following are the recommended minimum requirements to support the SecurEnvoy Windows Login Agent (WLA):

- Processor: 1 gigahertz (GHz) or faster processor
- RAM: 1 gigabyte

## Agent Configuration Options

### Central Management

Within the SecurEnvoy Access Management graphical user interface (GUI), accessible in Administrator Mode, the configuration interface for the SecurEnvoy Windows Login Agent can be customised for each individual machine or applied collectively through the 'Bulk Setup' option.

The 'Bulk Setup' option allows for the configuration of multiple agents across all agents within a selected domain, with the additional option to include all the sub-domains as well as individual machines. This ensures consistent and secure access across the network.

### Device Name

This feature allows for more descriptive or standardised naming conventions, facilitating easier identification and management of devices. The default naming convention is 'DeviceName-IP-Port'. This can be modified through the 'Device Name' field in the configuration interface.

The default device name can be modified through the configuration interface. Simply navigate to the 'Device Name' field in the configuration interface, and you will find the option to edit the 'Device Name'.

### Granular Protection Configuration

The SecurEnvoy Windows Login Agent enhances security by integrating multi-factor authentication (MFA) for both direct Console access and Remote Desktop (RDP) sessions, or for either one independently, based on organisational needs. This added layer of protection is easily activated through a user-friendly interface.

Administrators can enable MFA for the desired access point—Console or RDP or both—simply by adjusting the relevant toggle switch in the agent's settings. This intuitive control mechanism allows for quick and flexible configuration of security settings. For more information on how to configure MFA, see the SecurEnvoy Windows Login Agent configuration guide.

## Emergency Access

To ensure uninterrupted access in scenarios where the Windows Login Agent is unable to establish a connection with the Access Management console, Emergency User accounts can be configured. These emergency accounts can either be local machine accounts or domain user accounts, offering flexibility in various network environments.

The process of adding these accounts is straightforward. Administrators need to register the emergency accounts through the Login Agent console. This step is crucial for enabling the functionality of these accounts.

For effective disaster recovery, it is essential to ensure that emergency access is available while the machine is offline. This is achieved by caching the IP address of the Access Management tenant in the local cache. This proactive measure enhances the system's resilience and ensures continuous access, thus maintaining productivity and operational availability.

## Restricted Group Access

To control access through the Login Agent, the SecurEnvoy Access Management system allows administrators to restrict access to a specific group. This setting ensures that only members of the designated group are authenticated, while all others are denied access, thus reinforcing security by precisely managing user authentication permissions.

Enhanced access control for the Windows Login Agent can be achieved through the implementation of the conditional access policy engine. This feature enables the creation of policies that restrict access based on specific criteria such as user group membership, device capability, and administrator access. This ensures compliance with organisational policies.

## Last Logged-In User Mode

In environments where information security policies restrict the display of the last logged-in user's details, the Windows Login Agent offers a configurable option. This allows administrators to tailor the prompt behaviour according to organisational needs. You can choose to either display the last logged-in user information or omit it. The Login Agent aligns with various security protocols, providing a balance between user convenience and adherence to stringent security policies.

## Offline Access

Users can securely log in to their console using multi-factor authentication (MFA) even when there is no internet connectivity. This is facilitated through the use of Software and Hardware OTP (One-Time Password) Tokens. This functionality guarantees consistent access while upholding security protocols, ensuring operational continuity.

# User Experience

## Supported Authentication Methods

The Windows Login Agent supports the following authenticators:

Method	Supported
Soft Token (OTP) – iOS, Android	Online + Offline
Soft Token (PUSH) – iOS, Android	Online + Offline
Hardware Token (OTP) – Keyfob, Card	Online + Offline
Yubikey USB Token	Online
FIDO2	Online*
SMS OTP	Online
Email OTP	Online
Static Code	Online

\* FIDO2 is only supported via its SMS or Email backup – Online support is scheduled in roadmap.

If the default authentication method is not available, the system is designed to wait until a user is prompted to enter a 6-digit OTP (One-Time Password) displayed in the iOS/Android app.

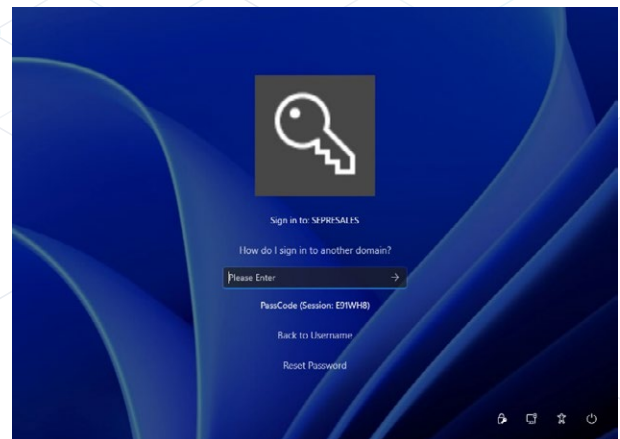
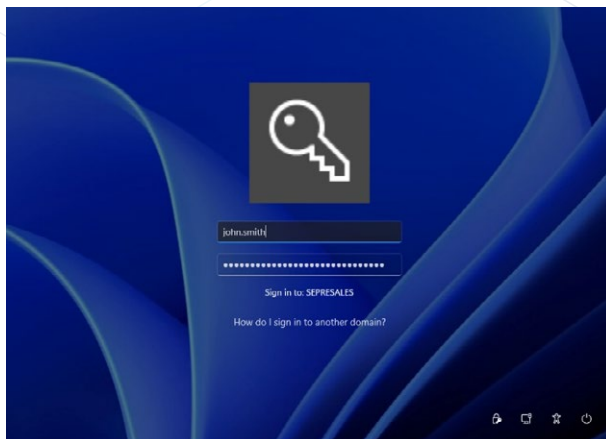
For enhanced security, a built-in 2FA (Two-Factor Authentication) is provided. This dual-layer protection is designed to meet the highest security requirements.

## Physical Console Access

The Windows Login Agent is compatible with and can be deployed to secure the following versions:

- Windows 10
- Windows Server 2012
- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2019
- Windows Server 2022

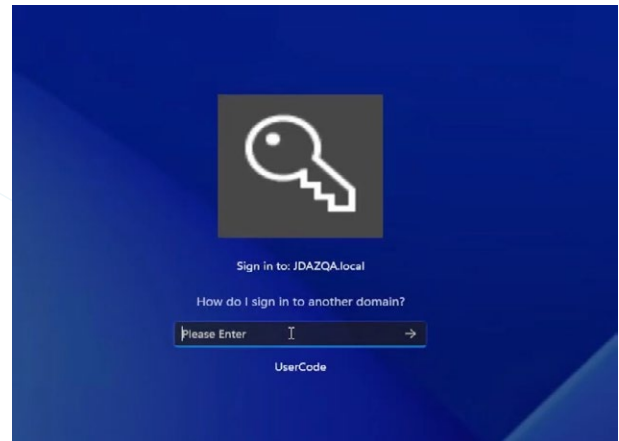
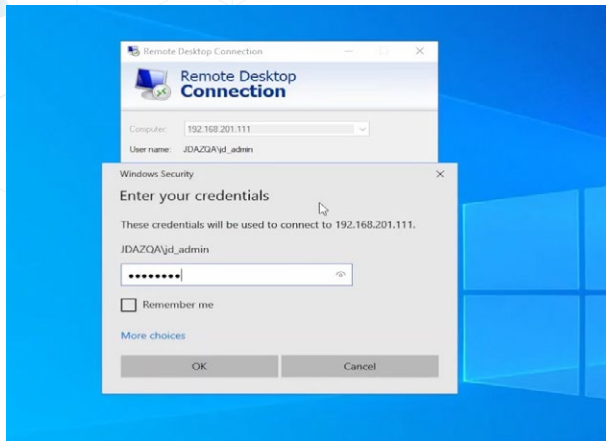
Once deployed, it provides a secure environment for the user to access the standard credential provider.



The user will be asked for their UserID, Domain Password, then prompted for the 2nd factor.

## Remote Desktop (RDP)

When the Windows Login Agent is integrated with Remote Desktop (RDP), the user experience closely mirrors that of a physical console login, as described earlier. Users begin by entering their UserID and Password in the usual manner. Following this initial step, users are then prompted to provide their chosen second factor for authentication, ensuring a seamless yet secure login process.



## Self-Service Password Reset (SSPR)

The integration of the Windows Login Agent (WLA) with physical consoles enhances security by enabling users to securely reset their password. If a user forgets their password while using the WLA, they can initiate the process by entering their UserID, then clicking the 'reset password' prompt. This action sends a push notification to the user's mobile device via a push notification service. Upon receiving the notification, the user can click a link to a mobile app. This app allows them immediate access to log in. Additionally, for heightened security, this password reset function can be geographically restricted, ensuring that users can only perform the reset when they are within a predefined, trusted location, thereby preventing password theft by eavesdroppers.

## Augmenting Microsoft Entra ID

For many organisations that have adopted the Microsoft eco-system for managing user identities, this will serve the majority of business use-cases. However, for organisations who still operate some legacy technologies there will remain some gaps where the implementation of MFA is either not possible, or limited and awkward. This is where SecurEnvoy can be added to the existing Microsoft environment to either enhance or plug authentication gaps with physical console and virtual RDP sessions, for example.

**To seamlessly add SecurEnvoy Windows Login Agent to Microsoft Entra ID, just 6 simple steps are required:**

1. Choose your desired implementation: SaaS, Private Cloud, On-premise
2. Synchronise the target 'Group' of 'Users' from Entra ID to SecurEnvoy Access Management Platform
3. Create the SecurEnvoy Windows Login Agent MSI and push the package to the desired machines via Microsoft Group Policy Management Console (GPMC)
4. Enrol users to SecurEnvoy Access Management Platform with MFA
5. Enable protection of machines on single-machine or bulk setup options within the Access Management Platform.
6. Test Authentication and assign additional security implementations such as Conditional Access, Group Authentication.

The installation of SecurEnvoy Access Management and integration of the Windows Login Agent into an existing Microsoft Entra ID ecosystem can typically be completed in less than 60 minutes.

## Conclusion

SecurEnvoy provides a comprehensive Access Management solution, designed for versatile deployment scenarios. This solution is capable of functioning as a complete, stand-alone Access Management system or can be seamlessly integrated with Microsoft Entra ID. Such integration enhances an existing Microsoft ecosystem, enabling organisations to adopt a layered security strategy.

This approach offers significant benefits, particularly in managing users by segmenting them into a distinct user repository. Additionally, it addresses legacy integration challenges, ensuring a more secure and cohesive access management solution. Organisations can tailor their security infrastructure to meet their needs while maintaining ease of use and integration.



✉ [support@securenvoy.com](mailto:support@securenvoy.com)

🌐 [securenvoy.com](https://securenvoy.com)

in [linkedin.com/company/securenvoy](https://linkedin.com/company/securenvoy)

X [twitter.com/securenvoy](https://twitter.com/securenvoy)