White Paper

Securing Legacy Technologies

with SecurEnvoy Windows Logon Agent

SecurEnvoy
A Shearwater Group plc Company

Contents

Windows Logon 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 Logon 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.

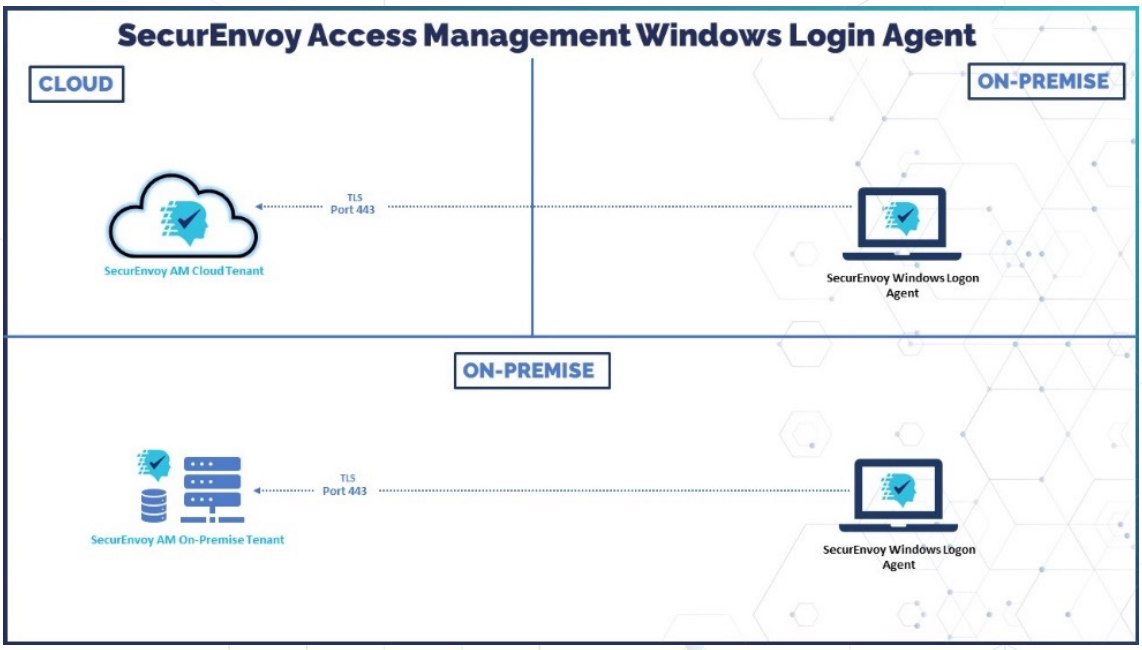
Despite the rapid shift towards cloud-based applications and services, a substantial portion of enterprise operations remains tethered to legacy systems. These systems, while reliable and essential, often lack the modern security features necessary to defend against current cyber threats. As regulatory bodies and cyber insurance policies tighten their requirements for security measures, organisations 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 Logon 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 Logon Agent Solution Summary

The SecurEnvoy Windows Logon 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 logon for user access, based on a user group. For example, Administrator Accounts for Remote Desktop Access to Windows Servers can be configured to mandate MFA prior to granting administrative access.



Deployment Options

The deployment of the Windows Logon Agent offers flexibility, catering to both individual and bulk installation needs. It can be directly installed on a single machine or distributed across multiple machines via the Group Policy Management Console (GPMC), utilising an MSI (Microsoft Installer) file for remote installation.

For a more streamlined and unobtrusive deployment, the 'wlaagent-setup.exe' can be pre-configured using an MSI Editor. This pre-configuration process allows the inclusion of the necessary settings for the SecurEnvoy Access Management tenant. As a result, the agent can be silently installed and configured, minimising disruption and the need for manual intervention during the installation process. This approach is particularly beneficial for large-scale deployments, ensuring a seamless and efficient rollout of the Windows Logon Agent across the network.

System Requirements for SecurEnvoy Windows Logon Agent

The SecurEnvoy Windows Logon Agent (WLA) is extremely lightweight and will run on any hardware specification that is capable of running Windows OS.

The following are the recommended minimum requirements to support the SecurEnvoy Windows Logon 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, there is a convenient feature for centrally configuring the Windows Logon Agent. This configuration can be customised for each individual machine or applied collectively through the 'Bulk Setup' option.

The 'Bulk Setup' functionality simplifies the process of configuring multiple agents. It allows administrators to uniformly apply settings across all agents within a selected domain, with the additional option to include all related sub-domains. This approach is particularly beneficial for comprehensive deployments or for ensuring consistent settings across numerous machines, streamlining the management of configurations and enhancing overall operational efficiency in maintaining security standards across the network.

Device Name

This feature allows for more descriptive or standardised naming conventions, facilitating easier identification and management of devices within the Access Management system. This straightforward process ensures that device names align with your organisation's naming protocols or specific identification requirements, improving overall system organisation and efficiency.

The default 'Device Name' can be modified through the Access Management Console. Simply navigate to the 'Setup' section and access the 'Logon Agent' configuration area. In this section, you will find the option to edit the 'Device Name'

Granular Protection Configuration

The SecurEnvoy Windows Logon 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 protocols. Once enabled, MFA requires users to provide additional verification beyond their standard login credentials, significantly bolstering the security of both local and remote access points.

Emergency Access

To ensure uninterrupted access in scenarios where the Windows Logon Agent is unable to establish a connection with the Access Management tenant, it is recommended to configure Primary and Secondary Emergency User accounts. 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 via the Logon Agent configuration section within the Access Management administration console. This step is crucial for enabling the functionality of these accounts.

For effective utilisation, it is essential that users log in with their designated emergency user account while the machine is connected to the network. This action allows for the caching of the user profile on the machine. The cached profile is a critical component that facilitates offline access, ensuring users can log in even when the machine is not connected to the Access Management tenant. This proactive measure enhances the system's resilience and ensures continuous access, thus maintaining productivity and operational efficiency in various connectivity scenarios.

Restricted Group Access

To control access through the Logon Agent, the SecurEnvoy Access Management system allows administrators to restrict authentication to specific user groups via its central configuration. For example, access can be limited to only those in the 'Administrator' 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 Logon 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 time of day, geographic location, and device status. This capability enables administrators to fine-tune access permissions, ensuring a higher level of security and 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 at the login prompt, the SecurEnvoy Windows Logon Agent offers adaptable settings to comply with such requirements. Through the central configuration GUI, administrators have the flexibility to tailor the login prompt behaviour according to organisational needs. You can choose to either display the last logged-in user information, conceal it, or defer to the Windows Default configuration setting. This feature ensures that the Logon 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 connection or if the Access Management tenant is temporarily unavailable. This offline access is facilitated once a user has authenticated in an online state. The system supports offline MFA with both Software and Hardware OTP (One-Time Password) Tokens. This functionality guarantees consistent access while upholding robust security protocols, effectively mitigating any disruptions caused by connectivity challenges.

User Experience

Supported Authentication Methods

The Windows Logon 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 a smartphone soft token utilising push notifications, the system is designed to automatically switch to an alternative method when the user's device is offline. In such cases, the user will be prompted to enter a 6-digit OTP (One-Time Password) displayed in the iOS/Android app.

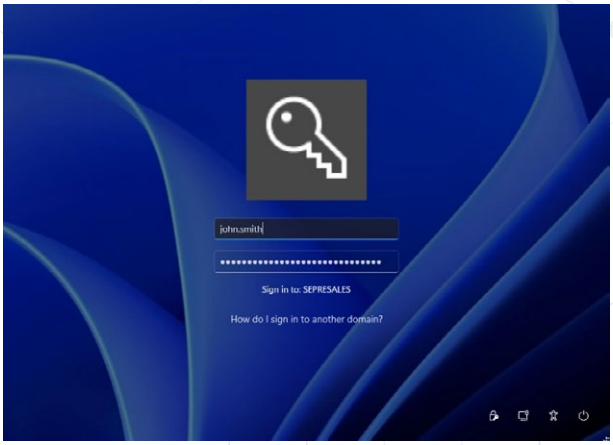
For enhanced security, both the push notification and the 6-digit OTP can be safeguarded with the phone's built-in security features, such as a PIN or biometric authentication (like fingerprint or facial recognition). This dual-layer protection ensures secure access while providing flexibility in varying network conditions.

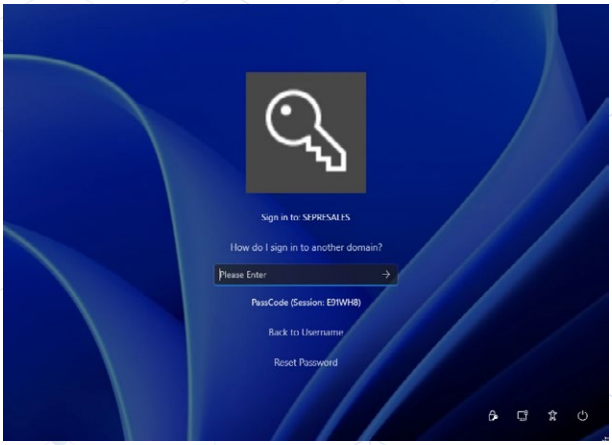
Physical Console Access

The Windows Logon 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, the WLA will provide the user with a familiar logon experience, with the first part being the standard credential provider:

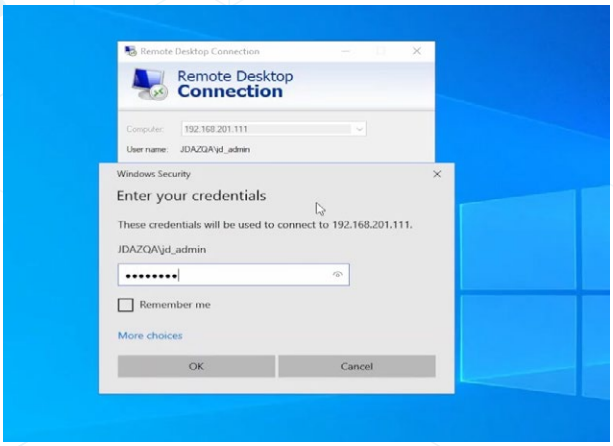


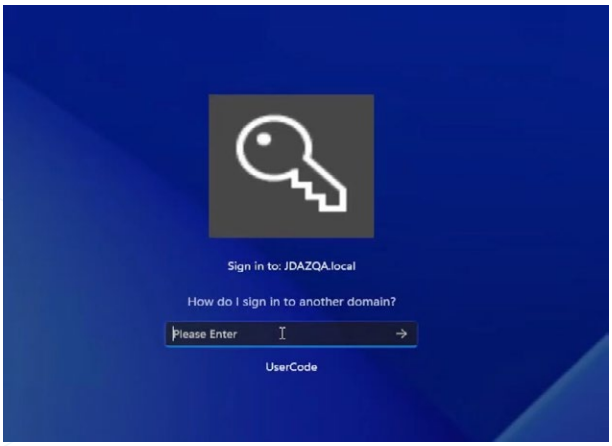


The user will be asked for their UserID, Domain Password, then prompted for the 2nd factor.

Remote Desktop (RDP)

When the Windows Logon 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 Logon 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. Upon accepting the authentication request via the push notification, the user can then set a new password directly within the mobile app. This updated password 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 enhancing the safety and integrity of the password reset process.

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 Logon 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 Logon 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 access for third-party and non-workforce users by segmenting them into a distinct user repository. Additionally, it addresses legacy integration challenges, ensuring a more secure and cohesive access management framework. This flexibility allows organisations to tailor their security infrastructure to meet specific needs, reinforcing protection while maintaining ease of use and integration.

support@securenvoy.com
securenvoy.com
linkedin.com/company/securenvoy
twitter.com/securenvoy

SecurEnvoy
A Shearwater Group plc Company