How secure is SSO Plugin?

And why our customer list include military, governments & financial services.

Simplify access without sacrificing security. The JSS SSO Plugin provides the highest standard of security and protection, compliant with FIPS 140-2 certificates, using AES256 algorithms for the encryption of data and integration to Microsoft Active Directories.
Because the product completely conforms to the BMC SSO framework and whitepaper, it utilises the same BMC API. Therefore, all network traffic can be encrypted with 256-bit AES CBC through the "BMC Premium Security" module. Details can be found in the BMC Remedy Encryption Security Guide on the BMC website.

Deutsche Bank

FORTIS

Federal Aviation Administration

International Monetary Fund

SwissLife

LOCKHEED MARTIN

UniCredit Bulbank

SSO Plugin never stores users passwords and replays or injects.

There are products on the market that will advertise they are SSO compliant applications. These products will record the domain password locally on the users desktop and then monitor the screen for a login prompt and reply and inject those keys into the destination application. Therefore presenting the appearance of SSO when in fact such products are known to have been reverse engineered to obtain those stored passwords. SSO Plugin™ does not follow such a design and instead uses the global standard and recommended integration layer libraries.

SSO Plugin conforms to the BMC SSO framework and encryption.

Because the product completely conforms to the BMC SSO framework and whitepaper, it utilises the same BMC API. Therefore, all network traffic is encrypted. Customers can further upgrade the encryption level from BMC to **256-bit AES CBC** through the "Premium Security" module. Details can be found in the BMC Remedy Encryption Security Guide on the BMC Website.

SSO Plugin utilises the same Windows logon protocols as your desktops

SSO Plugin support the two most popular and secure logon protocols used within the Microsoft domain. **NTLMv2** and **Kerberos**. Both are commonly used within any Microsoft network when our desktops login to our domains.

With the addition of rotating keys, no two logon requests are the same.

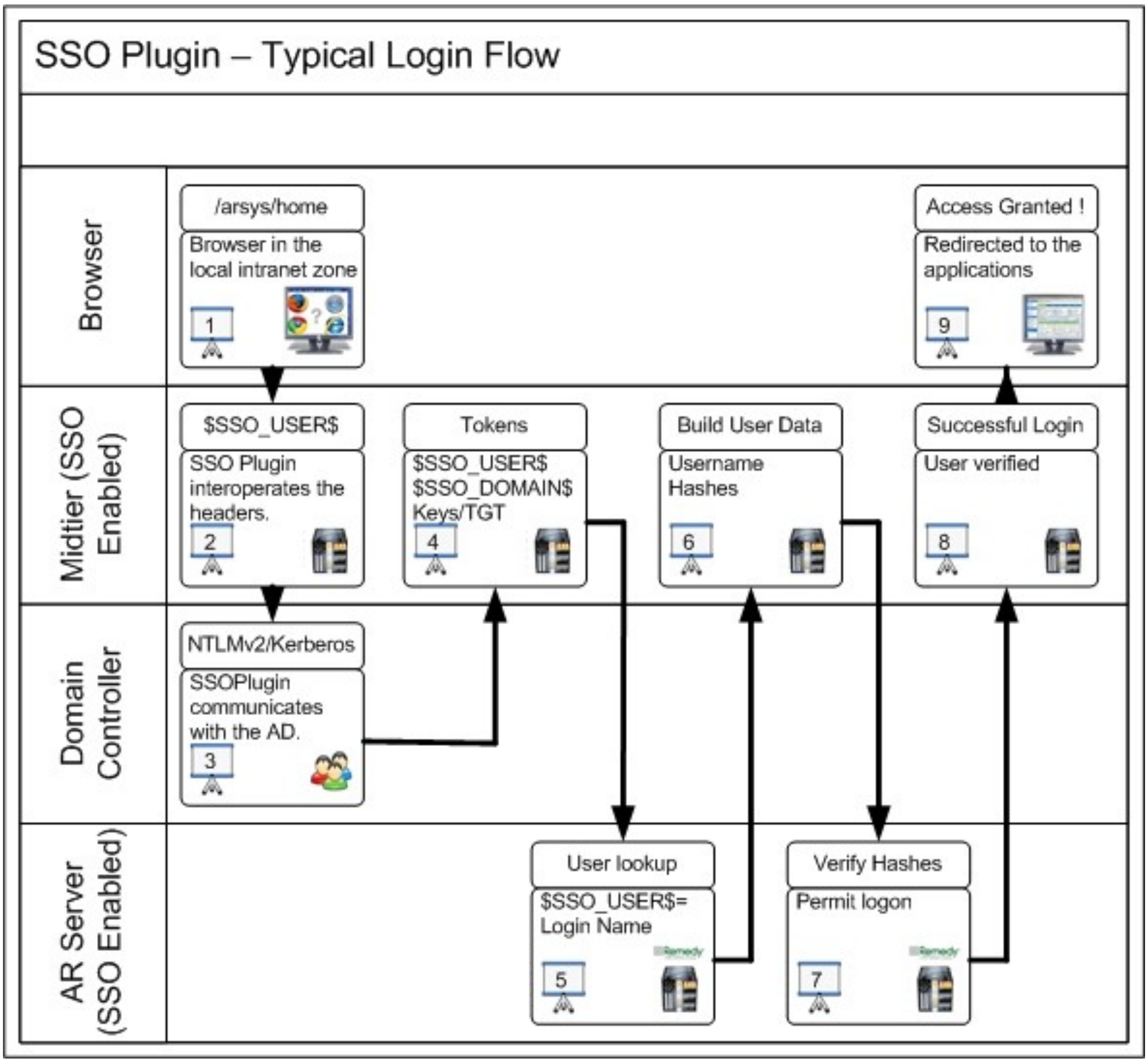
A feature designed by our security team, not available in any other SSO application, means that no two login data is ever the same. User data is accompanied by a one way hash which prevents someone installing their own client and trying to impersonate a trusted Mid Tier or Windows User Tool and its users.

Trusted Mid Tier verification at the AR Server level.

A configured list of Mid Tier IP addresses are stored in the SSO Plugin configuration. The IP address of the Mid Tier is embedded into the data packet of the communication, preventing spoofing, which is then verified at the AR Server level. If found not to be in the list, authentication is rejected.

Typical authentication flow diagram

The following diagram represents the typical configuration of the SSO Plugin deployed in a customer environment.



1. The browser, in the local intranet zone, makes a request to the Mid Tier. This includes header information such as the domain user. Unless the customer Mid Tier is using SSL, this communication is plain text.
2. SSO Plugin gathers the header information and depending on the configured Windows protocol, will communicate to the active directory controller and verify the user. This communication is using the Microsoft NTLMv2 or Kerberos standard.
3. The active directory controller will participate in a number of challenge / response communications.
4. If the active directory has signalled the user is genuine, tokens are created and SSO Plugin performs a lookup to the AR System User table to confirm the user exists. Features such as aliasing can help identify the user. This communication is using the BMC Remedy API and therefore using the same encryption the system uses. Standard is 56-bit DES.
5. If a valid user is found, the data is returned to the SSO Plugin.
6. The SSO Plugin builds the username and hash detail to send to the SSO AREA Plugin configured on the AR Servers. This communication is using the BMC Remedy API and therefore using the same encryption the system uses. Standard is 56-bit DES.
7. The SSO AREA Plugin verifies the data came from a trusted SSO enabled Mid Tier. Then continues to verify the username hash and token.
8. If the above data is valid, the Mid Tier is allowed to proceed with this user.
9. User is redirected to the application. Securely identified using SSO Plugin