Syssero® Solution Packet

Updating x509 Public Key for SSO in Workday

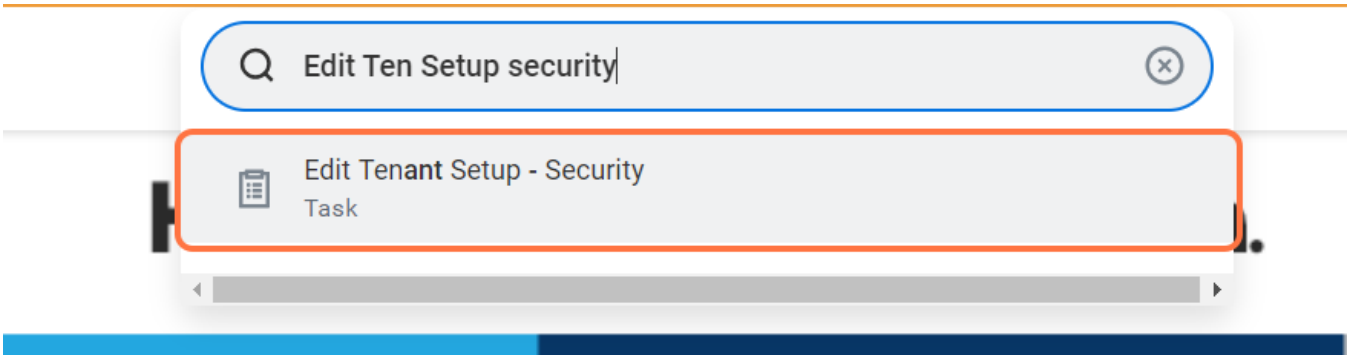
Solution Overview

An x509 public key is a tool used in digital security to help verify and trust the identities of users and systems. In the context of Single Sign-On (SSO), when a user logs into a service like Workday, the SSO provider creates an authentication token that proves the user's identity. This token is signed with the provider's private key. The x509 public key acts like a lock that can confirm this token's signature, ensuring it was indeed issued by the SSO provider and has not been altered.

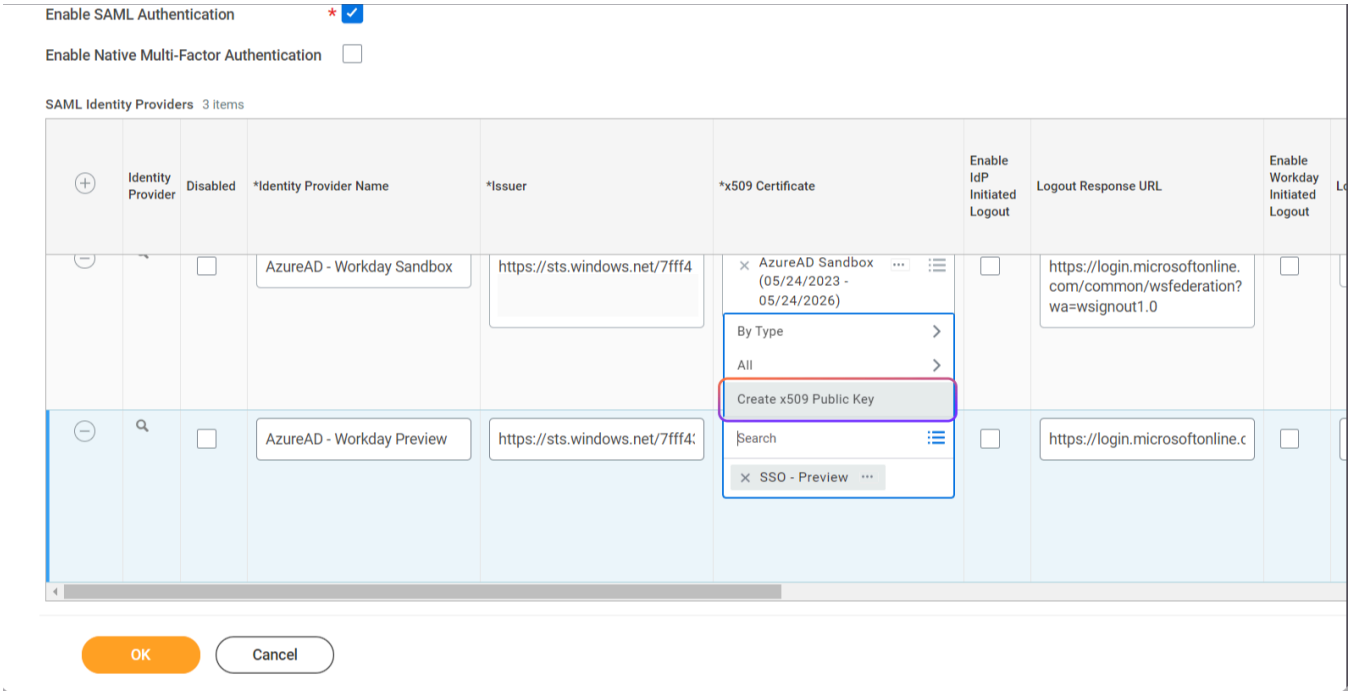
This solution will guide you through the essential steps for configuring, updating, and maintaining the x509 public key, a critical component for verifying user identities during the authentication process. You will gain a clear understanding of the procedures to follow when managing these keys, enabling you to uphold the integrity and security of your organization's authentication systems.

Step 1. Open the valid x509 Certificate in Base64 format in Notepad. This text will be copied/pasted into the new x509 key in Workday.

Step 2. In the Workday Production tenant, navigate to the "Edit Tenant Setup - Security" task.

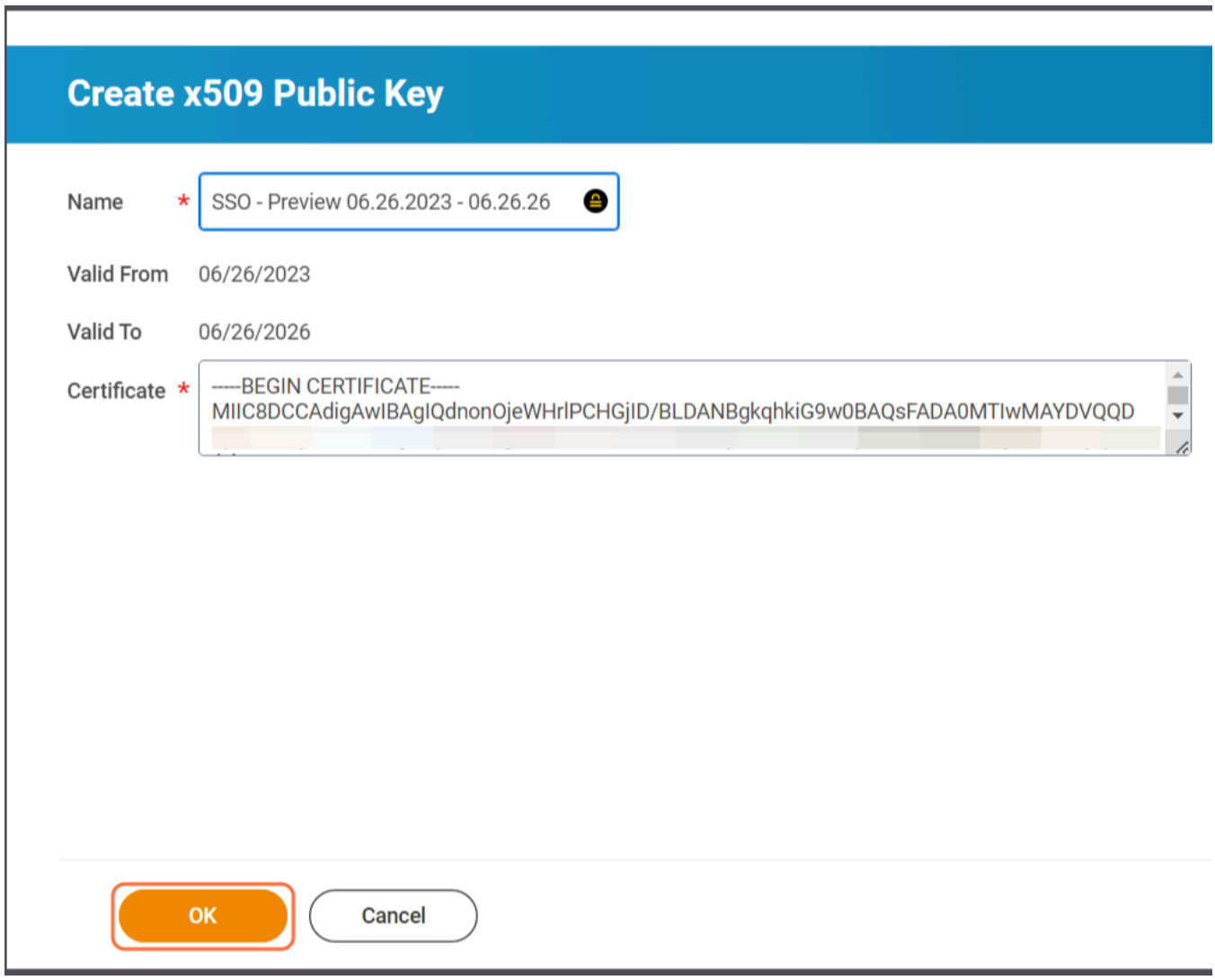


Step 3. In the "SAML Identity Providers" grid, locate the row that corresponds with the tenant that needs updating. In the "x509 Certificate" column of that row, click in the field where the current key is located and then select "Create x509 Public Key" from the menu.

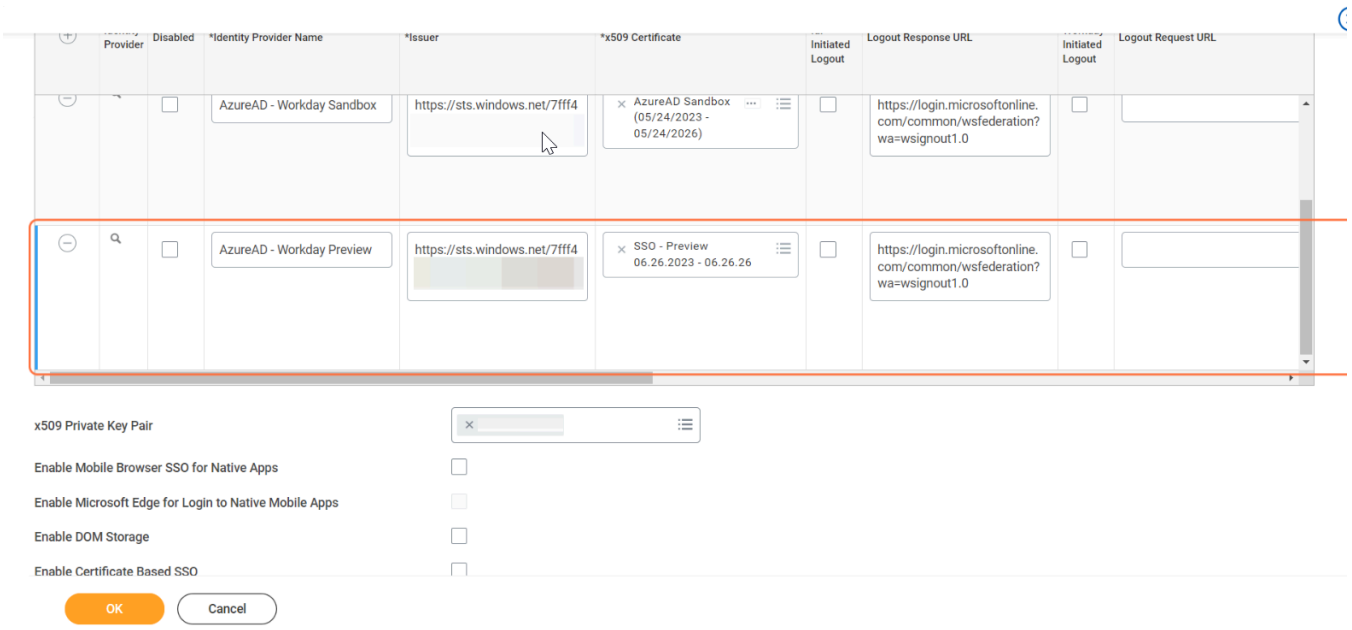


Step 4. Enter a name for the new key that is unique to the updated certificate.

- Copy the entire certificate text previously opened in Notepad and paste into the "Certificate" field.
- The "Valid From" and "To" dates will automatically populate when the new certificate is pasted from Notepad.
- Click OK to save the new x509 Key.



Step 5. Validate that the previous, expired key has been replaced with the newly created x509 Public Key in the x509 Certificate column of the correct row. Lastly, click ok to save all changes!



Step 6. If updating the x509 Key for a non-Production tenant (i.e. - Sandbox, Preview, Implementation), REPEAT STEPS 2-6 IN THE CORRESPONDING TENANT FOR IMMEDIATE ACCESS. The x509 Key/SSO certificate has been successfully updated.

Conclusion

The effective management of the x509 public key is vital for ensuring secure authentication processes within Single Sign-On configurations. Regular updates and diligent monitoring of expiration dates not only safeguard user access but also uphold the integrity of data exchanges between service providers and identity providers. By prioritizing these practices, organizations can foster a secure environment, enabling seamless operations within platforms like Workday and beyond. Staying proactive in this area will mitigate risks and reinforce trust in the technology systems that support business functions.