



Secure and reliable channel for your customers to access your web applications

Benefits

- Offer your customers a highly secure and reliable channel to access your applications and services
- Increase your customer reach by facilitating adoption among SWIFTNet customers
- Customers can use their existing SWIFTNet infrastructure for single window access to multiple services
- User-authentication service centrally managed by SWIFT
- Straightforward integration into your web-applications

SWIFT WebAccess

Offer your customers secure and reliable access to your web applications over SWIFTNet

In today's highly competitive environment, financial institutions across the world are differentiating themselves by offering interactive financial services to their customers via web portals. A variety of options exist for providers to connect customers to their services, with internet or proprietary channels as common solutions.

Yet, with cyber-threats an ever present risk, the internet may not measure up to the security and reliability demanded by mission-critical applications. On the other hand, proprietary channels require dedicated infrastructure set-up costs for each channel added, and require customers to use a variety of processes and tools, all of which may have implications on the resources needed to implement and maintain.

Our solution

With SWIFT WebAccess, you can offer your customers a highly secure and reliable screen-based channel to access your web applications and services – using customers' existing SWIFTNet infrastructure.

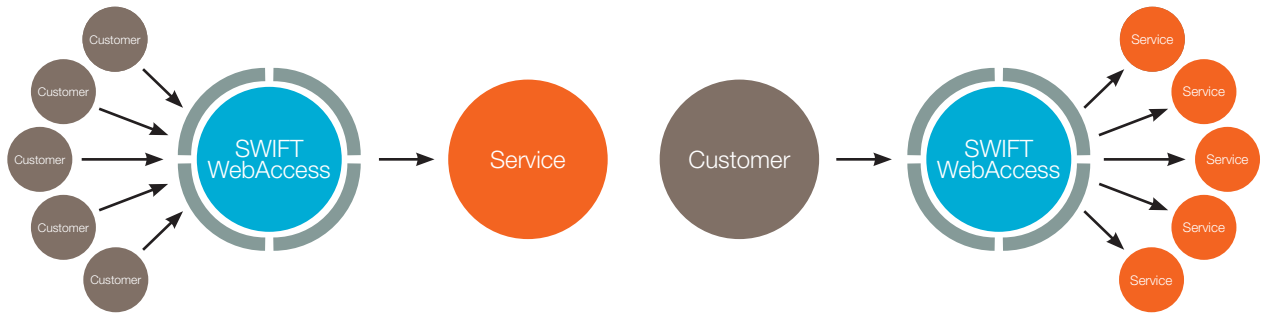
From a business perspective, SWIFT WebAccess offers a winning solution for you and your customers: you can increase your client reach by facilitating adoption among SWIFTNet customers (over 10,800+ financial institutions and corporations in 200+ countries); and your customers benefit from a single channel for accessing multiple services, all based upon their current SWIFTNet infrastructure.

Benefits for you

SWIFT WebAccess enables you to offer your web applications to all SWIFTNet users via a secure channel centrally managed by SWIFT. SWIFT operates the user authentication service centrally, allowing you to focus your resources on adding value to your services. Nevertheless, via a managed closed user group, you remain in full control of the institutions that can access your application.

Benefits for your customers

By using their existing SWIFTNet infrastructure, customers do not need to set up and manage dedicated connectivity (VPN), or other security mechanisms; and they further benefit from all the security and reliability of SWIFTNet. WebAccess also reduces user complexity by enabling customers to access multiple applications using a single authentication method – enabling a simple, harmonised user experience.



▲ Benefits for service providers and customers in using SWIFT WebAccess

SWIFT WebAccess builds upon our previous interactive service, Browse. WebAccess is distinct from Browse as it offers a SWIFT managed centralised authentication service (detailed above), which does not necessitate deep integration of the SWIFT security framework into your web applications.

Key features

- A secure and reliable channel to access your customers
Your customers can connect over the SWIFT-managed MV SIPN network, providing them with infrastructure resilience and multi-layered session-based integrity and confidentiality protection. Their users are strongly authenticated with individual SWIFTNet PKI certificates stored in hardware (HSMs or personal tokens).
- Increase customer reach
By using customers' existing infrastructure, WebAccess greatly facilitates adoption of your services among SWIFTNet customers, enabling you to increase your customer reach across the all SWIFT community.
- User access centrally managed
User access to your applications is handled through a service centrally managed by SWIFT. You control which institutions are authorized to access your applications through a managed closed user group. Your customers control which users are authorised to access your applications within their institution via Role-based access control (RBAC).

WebAccess ensures that access to your application is only possible by authorised users from authorised institutions – users need to successfully authenticate using

their individual SWIFTNet PKI certificate. WebAccess constantly screens your application from unwanted access.

- Non-repudiation service
Service providers can optionally request non-repudiation confirmation over WebAccess for end users to authorise critical transactions. WebAccess displays the transaction information sent by the service provider over a confirmation screen for review by the end-user. The end-user provides their confirmation by signing the transaction using their personal certificate, which ensures non-repudiation and traceability at the end-user level. SWIFT stores the signed transaction centrally for 124 days and can act as trusted third-party between the service provider and the end-customer.

- Simple to integrate
WebAccess implementation is based on open standards (for example, SAML 2.0), and does not require the use of proprietary protocols. There is no need for deep security integration in the application as user access is centrally managed.

Costs

The costs include a monthly usage fee, which depends on the number of your customers using WebAccess, as well as a per transaction fee if the service uses the secure transaction feature. Factors such as expected throughput may also impact on costs. SWIFT also offers a developer toolkit license and service packages to help integrate the solution into your business web application. Please contact your SWIFT account manager for pricing information.

For more information, please visit: the [SWIFT WebAccess webpage](#) or contact your SWIFT account manager

Product features

- Channel security: MV-SIPN & HTTPS – Screen-based channel with the security and reliability of SWIFTNet, offering multi-layered encryption and integrity protection
- User-level security: SWIFTNet PKI – Strong user authentication based on SWIFTNet PKI certificates stored in hardware (HSM box or personal token)
- Central user access validation: Centrally managed user access – Applications screened from unauthorized access
- Community: Closed User Group – You control which institutions are authorized to access your application
- Access Control: Role-based access control (RBAC) – Only users authorized by their institution can access your application
- Transparent resilience: Single URL – Users use a single URL to reach your application, SWIFT automatically connects user to your first available web server

Optional features

- Transaction confirmation: Non-repudiation service – SWIFT provides a complete non-repudiation service for critical transactions, enabling auditing at user level (with SWIFT as a trusted third-party)
- Application roles: RBAC – Centrally stored user roles can be provided for service providers to customize the functionality within the application
- Load distribution: Session distribution – you can define traffic distribution across data centres, thereby spreading the load
- Flexibility of access: Internet support – you can enable users access over the internet