LSEG Workspace | Entra

Frequently Asked Questions

LSEG DATA & ANALYTICS

Contents

About this document

This document provides answers to questions that commonly arise when customers:

- First encounter Microsoft Entra, and
- Prepare to configure the use of Entra for LSEG Workspace authentication.

Intended readership

This document is intended for LSEG customers that intend to use LSEG Workspace for HERE Core, which requires Entra authentication. The roles for which this document is of interest are:

- Identity Administrators
- IT Administrators
- Workspace Administrators

Additional resources

You can:

- Request further assistance with the points discussed in this FAQ, contact Support.
- Find more detailed technical information about Entra configuration in the Administrator Guide.

Workspace documentation

For general technical information about LSEG Workspace, see the Workspace technical documentation site. You can also provide feedback on this and other Workspace technical content, by contacting DocFeedback@lseg.com.

Entra fundamentals

How is Workspace authentication changing?

In March 2025, LSEG released a Customer Identity and Access Management (CIAM) solution that integrates our customer corporate identity management system with your corporate identity. That is, it provides integration between LSEG and your organisation's Entra. This mode of integration, known as SCIM, is the industry standard for integrating identity and its scope extends beyond just single-sign-on for authentication. It provides the capability for our customers to automate provisioning of users and license, thereby reducing their operational overhead.

Several customers have since adopted this solution due to the benefits it provides, in terms of:

- Security
- Compliance
- Operational overhead
- User experience

📌 Our original LSEG Workspace platform (formerly *Refinitiv Workspace*) continues to use Forgerock for authentication.

What is Microsoft Entra?

In short, Microsoft Entra could be described as *Microsoft Active Directory on the cloud*. It is a comprehensive suite of identity and access management solutions, provided by Microsoft. A significant portion of our customers use Entra to:

- Manage their Windows user identities
- Secure access, and
- Protect sensitive data.

It includes services like Azure Active Directory and Microsoft Identity Manager.

What is SCIM?

System for Cross-domain Identity Management (SCIM) is an established industry standard for organisations to integrate user identities to automate management of users and provisioning entitlements in real-time. To find more information about SCIM, see Microsoft FAQs on SCIM.

How can I check whether my organisation is using Entra?

If you have Microsoft Office 365, you are likely to have Entra. Your administrators in IT, ServiceDesk or Microsoft Support would be able to clarify if you use Entra to manage your corporate identity.

What if my company does not use Entra?

LSEG offers other single sign on solutions for linking your user login credentials to LSEG products through their corporate identity system. For further information, contact your LSEG Customer Implementation team.

For Entra, we use an internal identity portal, will integrating LSEG CIAM cause issues?

Yes. If you use your own portal to map your corporate identities to Entra, this integration will not be suitable for you. However, we offer other solutions that allow you to link the login IDs of your users to LSEG Workspace through their corporate identity. For further information, contact your LSEG Customer Implementation team.

What are the benefits of using Entra to login to Workspace?

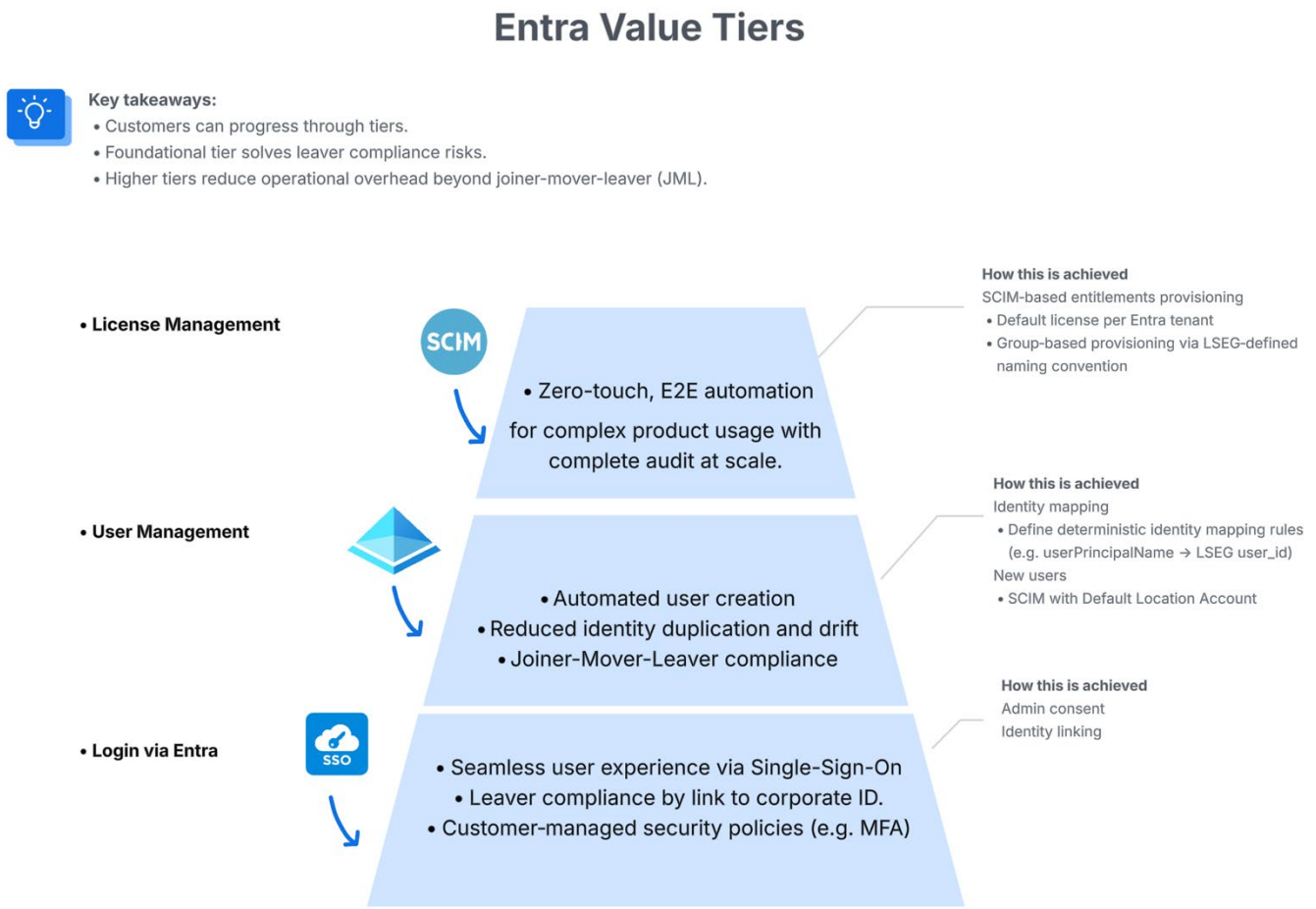
By integrating with LSEG through your Entra tenancy, you have complete control over the credentials used to access LSEG Workspace. There are also optional add-ons that reduce operational overheads further (see below). The benefits include:

Enhanced security	Workspace authentication is routed through your IT systems. This means that security policies and access controls can be consistently enforced within your organisation. This solves joiner and leaver compliance, out of the box.

Reduced costs	Reduces the administrative overhead associated with managing multiple sets of user credentials and accounts.
Improved user experience	By enabling single sign on, users will experience seamless access to various applications; including LSEG Workspace.
Reduced password fatigue	Users often struggle to remember numerous passwords for different applications. Through identity federation, users can log in once to access both their Windows environment and LSEG Workspace.
Improved interoperability	Promotes interoperability by providing a standard protocol for authentication and authorisation. This allows different systems and applications to work together.

What are the optional add-ons in the Entra integration?

Optionally, you may allow LSEG to receive automated updates from their Entra configuration through SCIM, an industry standard technology. On receipt of these updates, LSEG can manage your organisation's users and their licenses within the LSEG ecosystem. This is illustrated in the image below.



Where can I learn more about LSEG's Entra authentication strategy?

For more information, contact your LSEG Account team.

User experience

What will the new login page look like?

When you are setup to authenticate through Entra, you are prompted to enter your usual corporate credentials – email address and password, for example. However, not only will this single sign on provide you with access to your corporate Windows desktop environment, but also to LSEG Workspace.

The exception to this process is if you have already authenticated elsewhere, in which case access to Workspace will be seamless.

Can I still change my password?

Yes, you can still change your corporate password. However, once you are setup to log into Workspace through your corporate identity, LSEG does not play any role in storing or resetting the password for your corporate account.

Workspace provides a seamless single sign on based on your corporate identity. So, resetting your corporate password is done using your existing IT processes.

Will other products be impacted by this change?

At present, Entra authentication provides seamless login to Workspace and LSEG's support and training portals. We are in the process of expanding the number of products in the LSEG product suite that support Entra, which will allow you to experience all of your touchpoints seamlessly using your corporate identity.

If I am running Workspace and FX Trading, will my password stay the same?

Currently, FX Trading and FXall standalone applications retain their existing login experience, using the login credentials issued by LSEG.

License administration

How is the initial user mapping between Entra and LSEG performed?

Initial user mapping can occur in several ways depending on the onboarding method.

SCIM	When SCIM provisioning is enabled[1], mapping is determined by the attribute-mapping rules configured in your Entra tenant (for example, mapping userPrincipalName to the LSEG user identifier).
Self-service mapping	Existing users can be linked through a self-service identity linking flow or through admin-managed identity linking

Using Entra, how do I remove licenses from users?

If your users are SCIM-provisioned, when the corresponding users are deprovisioned or removed from groups in your Entra tenant, their licenses are removed from LSEG systems automatically. For further information, see the Workspace | Entra - Administrator Guide.

License pool management at Location Account level in LSEG remains unchanged - Entra onboarding does not alter how you assign or remove licenses from your overall contract entitlement. If you are integrated with LSEG through SCIM, when a user is removed from your Entra configuration, a SCIM event is sent to LSEG's systems. This results in the user's license being returned to the pool of available licenses for the customer.

What happens if we over-provision users in Entra?

Let us assume that automatic license provisioning is configured and a finite number of licenses are available in your license pool. If licenses are available in your license pool, any new users you add are created in the LSEG system. If new users are received through SCIM after the license pool is exhausted, their user records are created in our system, however, a license is not assigned.

You can, of course, use the existing LSEG process, through our license management tools or Sales/Operations contacts, to manage your licenses. License management includes activities such as:

- Adding a license
- Assigning licenses to users
- Viewing license entitlements

Does Entra integration help to prevent unauthorised access?

Yes, Entra allows you to enforce conditional access policies, such as:

- Device trust
- Location-based rules
- Compliant device requirements, and
- MFA enforcement

These controls are applied before a user reaches LSEG systems, ensuring compliant usage and reducing the risk of unauthorized data access. Many customers leverage Entra as their primary control plane for secure access.

For further information about these capabilities, refer to the Microsoft Entra Conditional Access site.

[1] SCIM integration must be enabled for automated provisioning of users to function.

Network access

The new identity and authentication service is cloud-hosted and does not use static IP addresses.

⚠ It is expected that customers will adopt the correct setup, in accordance with the specific requirements of their own organisations, to authenticate their end users into their corporate Entra tenants. As a result, Entra authentication and related domains are outside scope of this document.

How do I gain access using the Internet?

If you whitelist access to the public Internet, you will need to permit the following list of Fully Qualified Domain Names (FQDNs) [2].

FQDN1	Protocol/Port	New domain	Delivery	Description
openfin.co	HTTPS, 443		WWW	Download HERE Core Runtime (RVM) and upgrades
lseg.com	HTTPS, 443	token.workspace.lseg.com login.workspace.lseg.com workspace.lseg.com api.workspace.lseg.com	WWW	Authorization security token issuance and refresh
All existing WWW domains [3]	HTTPS, 443 WSS, 443 [4]	*.Refinitiv.com *.refinitiv.net	WWW	Application access

How do I gain access using private networks?

To access new Azure service endpoints, customers using a private network must whitelist the following new IP addresses, in addition to the previously communicated IP ranges, which will impact Delivery Direct, FCN and CMC users.

- 159.43.248.0/23 [AMERS]
- 159.43.240.0/23, 159.43.244.0/23 [EMEA]
- 159.43.227.0/24 [APAC]

These new IPs are part of the larger IP subnet - 159.43.192.0/18 - which was communicated in previous networking documents. LSEG recommends that customers allow connections to the wider, larger IP subnet.

LSEG Workspace leverages Internet access for connecting to the new security/authorisation token services and for HERE Core Runtime upgrades itself. Accordingly, you should ensure that your network is configured to allow the below domains:

FQDN1	Protocol/Port	New domain	Delivery	Description
lseg.biz	HTTPS 443	login.workspace.lseg.biz	Private Network	Application access
All existing private domains [3]	HTTPS, 443 WSS, 443 [4]	*.Refinitiv.biz *.refinitiv.net	Private Network	Application access

Is Entra available over a private line or direct fibre connection?

No. Entra is a cloud identity service delivered over the public internet and does not support direct private connectivity, such as leased lines or private peering. This is by design, as Entra must be reachable globally by all managed devices and applications. You should ensure that your security policies allow outbound connectivity to Entra's published endpoints.

---

[2] Any existing whitelisted domains LSEG has previously communicated should not be removed.
[3] For further information, refer to configuration and administration guides, found in the Workspace technical guides site.
[4] For market data streaming.

Compliance

Is SCIM provisioning between Entra and LSEG DORA-compliant?

LSEG's implementation of SCIM is compliant with DORA-aligned principles, such as:

- Identity governance
- Least privilege
- Secure API communication

Final DORA compliance always depends on your configuration of Entra and how you implement access governance. Influencing factors include:

- Conditional access
- MFA
- Device compliance

SCIM itself follows Microsoft's provisioning standards, which meet modern regulatory expectations.

Could an Azure or Entra outage impact our access to LSEG services?

Your authentication workflow will rely on your Microsoft Entra tenant, which acts as your corporate identity provider. Entra is a globally redundant, highly available solution provided by Microsoft. If Entra experiences a global outage, your users may encounter issues in accessing any of your corporate IT systems that are secured through Entra. By extension, in such a scenario, your users may temporarily be unable to sign into LSEG products, such as Workspace for HERE Core.

Entra’s uptime and service history can be tracked by choosing **Microsoft Entra ID (formerly Azure AD)** in the product dropdown, through the public Microsoft status page:

https://azure.status.microsoft/en-us/status/history/.

LSEG product compatibility

How does Real-Time access change with Entra onboarding?

With Entra onboarding, Workspace can respect your Entra device identity, ensuring Real-Time market data is only accessed from a single device at a time by authenticated identity. Device identity controls are part of Entra's Conditional Access framework.

For Entra, if we use an internal identity portal, will integrating with LSEG cause issues?

No. If your internal identity system ultimately federates users into Entra, LSEG sees the Entra-validated user object and treats it as authoritative.

SCIM provisioning and authentication depend only on what is present inside your Entra tenant, regardless of how identities arrive there. As long as your portal continues synchronizing identities into Entra correctly, your integration with LSEG will work normally. For further information, refer to the Microsoft Entra federated identity documentation.

If we have separate DACS identities, will those federate through Entra or SCIM?

No. DACS identities are not part of the Entra-to-LSEG identity federation path and cannot be SCIM-provisioned. If you have questions about unifying or altering your DACS user model, we recommend discussing this with the LSEG product team, as impacts vary by product set.

What happens in LSEG when a user is deactivated in Entra?

If a user is deactivated in your Entra, they will lose access to LSEG Workspace instantly. Additionally, If SCIM integration is configured and a user is disabled or removed in Entra, SCIM sends a deprovisioning event to LSEG [5]. If you have configured automated license management, their licenses are removed and returned to your license pool.

[5] Automatic deprovisioning is only available with a SCIM implementation.