

Ivanti Unified Access Licensing

For Ivanti Network Security VPN and ZTNA Products

Overview

- Centralized and automated license management in the Neurons cloud platform
- Includes Ivanti Connect Secure VPN, Ivanti Neurons for Secure Access and Ivanti Neurons for Zero Trust Access
- Named user licensing
- ISA-V gateway platform licensing included
- Supports both ISA and PSA model VPN gateways

Product Description

Ivanti Unified Access Licensing (UAL) is a named user licensing mode that is attached to the Neurons platform for Ivanti Connect Secure VPN, Ivanti Neurons for Secure Access gateway cloud management and Ivanti Neurons for Zero Trust Access. UAL allows for unlimited deployment of virtual ISA VPN and ZTNA gateways managed by the Neurons platform. With UAL, all user and gateway licensing is managed by the Neurons platform, meaning admins no longer need to manually install licensing on each of their gateways or operate an Ivanti Connect Secure license server as part of their deployment.

What's included in Unified Access Licensing?

Ivanti Unified Access Licensing includes subscriptions to Ivanti Connect Secure VPN, Ivanti Neurons for Secure Access and Ivanti Neurons for Zero Trust Access.

With UAL, all licensing is centralized and automated inside of the Neurons platform. This provides administrators the freedom to quickly stand up, scale, or decommission VPN or ZTNA gateways on-demand with ease, in the cloud or as a virtual machine, without ever having to worry about installing or managing licenses.

What are the advantages of Unified Access Licensing over Concurrent User Licensing?

Unified Access Licensing is a named user license. This means each user is assigned their own dedicated license the first time they sign in, which is then tracked inside of their associated Neurons instance. Any time a user signs into a device in the deployment, that user will be authorized against the UAL named user list for the organization.

Ivanti Unified Access Licensing bridges the gap between traditional VPN and zero trust network access. With UAL and the Ivanti Secure Access Client, an organization can transition to zero-trust network access at its own pace, deploying VPN or ZTNA gateways flexibly as needed, and set up applications in Ivanti Neurons for ZTA when ready. Improve operational efficiency with greatly reduced management overhead, centralize VPN gateway management, enjoy user behavioral analytics and risk scoring, and future-safe security investments.

With Ivanti Unified Access Licensing, administrators have the freedom to immediately deploy both VPN and ZTNA gateways whenever and wherever they need them. As gateway platform licensing is included with UAL, the administrator can deploy whatever size gateways they need for the given task. New gateways only need be attached to the customer Neurons instance as part of initial set-up; admins will not need to install or configure any further licensing on the device as it will be all managed automatically inside of Neurons.

How does Neurons track UAL users and named licenses?

The management of UAL named users are handled separately between Ivanti Neurons for Secure Access and Ivanti Neurons for Zero Trust Access. Both maintain their own list of assigned named user licenses, and how the user licenses are assigned and freed up differ between the services.

For Ivanti Neurons for Zero Trust Access, the user's last activity is tracked by their login. If a user has not logged into Ivanti Neurons for ZTA for the past 90 days, then the user's named license is automatically released and made available for reassignment to a new user. The now license-less user will need to re-register with Ivanti Neurons for ZTA to be added back to the UAL database.

With Ivanti Neurons for Secure Access, the first time the Ivanti Neurons for Secure Access instance sees activity from a user, it will map an associated user account within Ivanti Neurons for Secure Access. This user account is associated to the named user license and does not expire. This mapping will remain assigned until the user account is removed from Ivanti Neurons for Secure Access. When the user account is removed, the named user license mapping is also removed, immediately freeing up the named user license for a new user to claim.

Coexistence between PSA / ISA with UAL

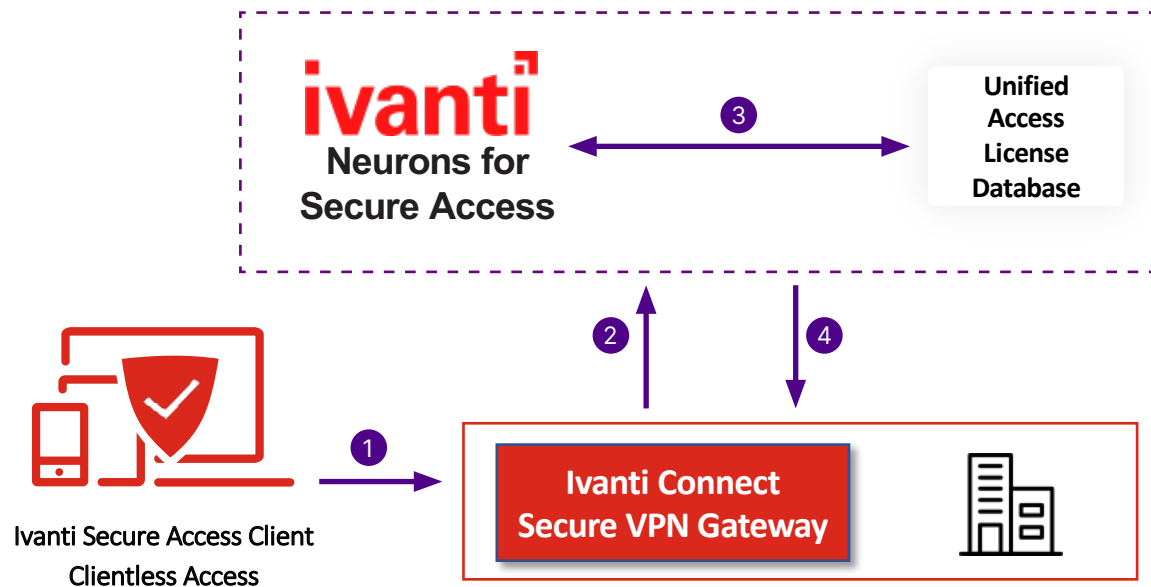
Ivanti Unified Access Licensing works with both ISA and PSA series gateways, so existing customers can easily migrate their PSA deployments over to the Ivanti Unified Access License model. Both PSA and ISA series gateways can be centrally managed by Ivanti Neurons for Secure Access, meaning existing PSA deployments can fully take advantage of centralized configuration and automated licensing without having to replace their gateways.

What is the upgrade path for PSA series gateways?

To enable Ivanti Neurons for Secure Access cloud management on a PSA series gateway, the gateway must be updated with the Neurons-enabled version of the PSA code available for download from within the Neurons instance. Once the update is complete, the PSA series gateway can then be attached to a Neurons instance and be managed fully from the Neurons cloud.

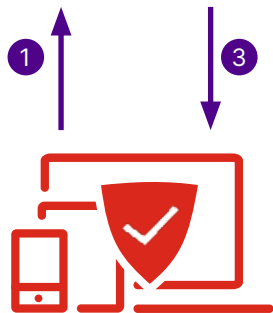
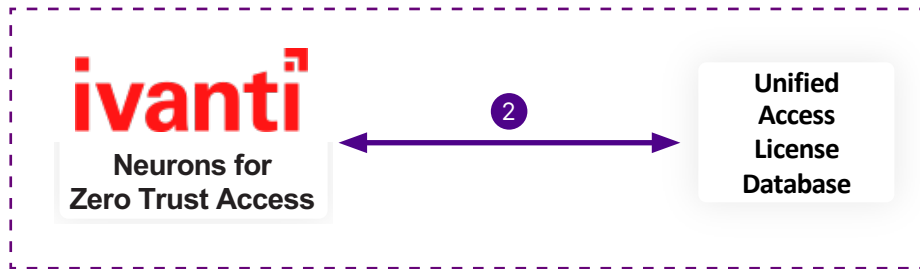


Ivanti Neurons for Secure Access Unified Access Licensing Diagram



- 1 A user connects to an Ivanti Neurons for Secure Access managed ICS gateway via the Ivanti Secure Access Client or clientless through the gateway User Portal.
- 2 Neurons-managed ICS Gateway checks local license cache for an existing user/license pairing. If a license pairing is found, then user is allowed to continue with realm/role assignment. If the user is not found in the local gateway cache, the gateway then queries Ivanti Neurons for Secure Access for user/license lookup.
- 3 Ivanti Neurons for Secure Access queries the UAL database for the user license pairing. If no user pairing is found and a free license is available, then a new user license pairing will be created. **NOTE** – If no free UAL licenses are available and no existing user license pairing exists, then user login will be denied by the ICS Gateway
- 4 Ivanti Neurons for Secure Access returns user/license pairing to ICS Gateway, which will cache the user license pairing locally for future logins.

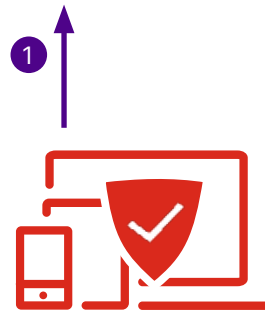
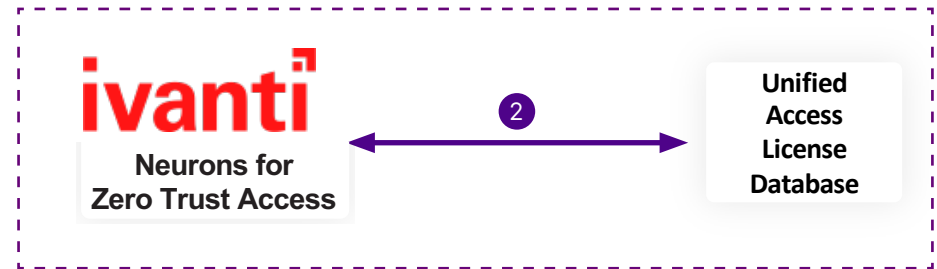
Ivanti Neurons for Zero Trust Access Unified Access Licensing Diagram for **new** ZTNA users



Ivanti Secure Access Client

- 1 New user logs in to a new laptop for the first time and registers with Ivanti Neurons for Zero Trust Access
- 2 Ivanti Neurons for Zero Trust Access assigns the new user a license if a free license is available. If no free license available in the UAL database, then user registration will be blocked, and user will be prevented from registering with Ivanti Neurons for Zero Trust Access.
- 3 Ivanti Neurons for Zero Trust Access will continue registration process for the user, including automatic client configuration.

Ivanti Neurons for Zero Trust Access Unified Access Licensing Diagram for **existing** ZTNA users



Ivanti Secure Access Client

- 1 Existing user logs into Ivanti Neurons for Zero Trust Access from the Ivanti Secure Access Client
- 2 Ivanti Neurons for Zero Trust Access confirms the user is still registered and assigned a license in the UAL database and continues with app assignment process. If the user is no longer assigned a license in the UAL database, user will be blocked from login and must re-register with Ivanti Neurons for Zero Trust Access.

NOTE – Ivanti Neurons for Zero Trust Access user license pairings expire after 90 days of no login from the user.

Benefits of Ivanti Unified Access Licensing

Benefit	Description
Consolidated remote access, gateway management and ZTNA licensing	Simplify your secure access deployment with a single SKU that combines VPN, cloud gateway management and advanced user analytics and zero trust network access for corporate applications.
Enjoy a seamless ZTNA migration	Thanks to the unified Ivanti Secure Access Client, existing ICS VPN users will not need to rip and replace their Ivanti endpoints, meaning no disruption to regular VPN users while rolling out Ivanti Neurons for Zero Trust Access.
No more sizing and licensing challenges when deploying new gateways	Platform licenses are automatically included with any new Neurons for ZTA or ICS gateway deployed, ensuring gateways will always be “right-sized” for the job. With centralized user management inside of Neurons, never worry about applying licenses to gateways or license servers again.
A single UI for managing your entire VPN and ZTA deployment	With Ivanti Neurons, manage all your ICS and ZTA gateways from a single pane of glass including full configuration and lifecycle management, multi-gateway/cluster management and configuration templates for VPN gateways.
Identify and control risky user behavior before it becomes a problem.	With UEBA and advanced user behavioral analytics, identify risky or anomalous user, device and application usage for both ZTA and VPN users in the environment
Reduce the number of Ivanti appliances to manage	Unified Access Licensing automates all user and platform licensing within the Neurons cloud, meaning organizations no longer need to maintain and manage an Ivanti License Server in their deployment.
Identify shadow-IT and risky user applications	Identify shadow-IT and track user application usage for both ICS VPN and Neurons for ZTA users. Create application policies based on application discovery findings and stop risky apps from becoming a threat.
Enjoy included advanced features that other providers charge separate licensing for	Unified Access Licensing includes SSL VPN, clientless access for VPN users, the Ivanti Secure Access Client which features Host Checker, custom endpoint scripting, Ivanti Neurons for Risk-Based Vulnerability Management (RBVM) Vulnerability Risk Rating (VRR) scoring for ZTA, and the freedom to deploy as many gateways as needed, when needed, without having to worry about user or platform licensing.



About Ivanti

Ivanti makes the Everywhere Workplace possible. In the Everywhere Workplace, employees use myriad devices to access IT networks, applications and data to stay productive as they work from anywhere. The Ivanti automation platform connects the company's industry-leading unified endpoint management, zero trust security and enterprise service management solutions, providing a single pane of glass for enterprises to self-heal and self-secure devices, and self-service end users. More than 40,000 customers, including 96 of the Fortune 100, have chosen Ivanti to discover, manage, secure and service their IT assets from cloud to edge, and deliver excellent end user experiences for employees, wherever and however they work. For more information, visit [ivanti.com](https://www.ivanti.com)

The Ivanti logo consists of the word "ivanti" in a bold, lowercase, sans-serif font. The letter "i" is red, while the remaining letters "vanti" are black. A small registered trademark symbol (®) is located at the top right of the letter "i".

ivanti

A vertical bar on the right side of the page, transitioning from red at the top to orange at the bottom.

[ivanti.com](https://www.ivanti.com)

1 800 982 2130

sales@ivanti.com