Ivanti Connect Secure (ICS):
Next-Gen Security and Scalability: Modern OS, Advanced Protection, and Seamless Zero Trust Migration

Overview

Ivanti Connect Secure (ICS) 25.x provides a modern, reliable solution for secure enterprise connectivity and zero trust migration. Built on Oracle Linux 9.x with OS, ICS offers improved scalability and performance for distributed environments. Advanced security measures, including SELinux and integrated WAF, actively prevent unauthorized access and ensure sensitive data remains protected. Automated policy enforcement and granular privilege controls protect against lateral movement. Built-in security analytics and threat defense improve visibility and speed incident response. ICS 25.x delivers reliable, unified secure access tailored for today's dynamic business environments.

Ivanti Connect Secure (ICS) 25.x introduces a modernized and secure foundation for remote access with significant advancements in both system architecture and protection features. Built on Oracle Linux 9.2 operating system with a robust 64-bit user space and Oracle Linux 5.14 kernel, ICS 25.x benefits from improved performance, scalability, and reliability, supporting enterprise-grade workloads and efficient management of larger files and datasets. The upgraded UEFI BIOS, GPT partitioning, and EXT4 file system further enhance stability, compatibility, and resilience against memory-based attacks.

Security is deeply embedded; SELinux is enabled and runs in enforcement mode by default, providing rigorous system hardening, continuous monitoring, and minimized attack surface through strong policy-based enforcement. Root Privilege Avoidance is implemented to ensure that processes adhere to the Principle of Least Privilege, limiting blast radius and opportunities for lateral movement within networks.

ICS 25.x extends secure boot integrity to additional filesystems, reinforcing the boot sequence against malicious code and ensuring a clean system image after factory resets.

Key management is strengthened via unique, randomized keys for each deployment and Trusted Platform Module (TPM) integration, which secures credentials and sensitive data, and protects data-at-rest with disk encryption. The web server architecture transitions to a NGINX-based platform featuring a built-in Web Application Firewall (WAF), improving visibility into application traffic, enhancing security incident analytics, and defending against web-based threats through custom rule sets. These features collectively reinforce Ivanti's value proposition by supporting seamless zero trust migration, bridging traditional VPNs to future-ready secure access, and enabling unified, secure connectivity for distributed applications and users.

Ivanti Secure Access Client

Ivanti Connect Secure includes the Ivanti Secure Access Client, a dynamic, multiservice network client for mobile and personal computing devices. Ivanti Secure Access Clients are easy to deploy, enabling users to quickly "click and connect" from any device, anywhere.

The Ivanti Secure Access Client supports per-app VPN, on-demand VPN connectivity, always-on and lockdown modes.The Ivanti Secure Access Client also supports full tunnel and FQDN or IP/network-based split tunnel connectivity.

The Ivanti Secure Access Client securely connects users to networks, both data center and cloud. Wrapped in a user-friendly package, the Ivanti Secure Access Client dynamically enables the appropriate network and security services on users' endpoints. With Ivanti, the connection just works, helping deliver the productivity promised by mobile devices.

The Ivanti Secure Access Client on desktop delivers dynamic access control, seamlessly switching between remote (SSL VPN) and local (NAC) access control services on user devices. It also enables comprehensive endpoint security posture assessment for mobile and desktop computing devices, and quarantine and remediation if necessary.

Ivanti Security Appliance

The Ivanti Security Appliance (ISA) is the new generation of Ivanti appliance offerings. ISA series appliances are purpose-built for speed and security and can scale to match any organization's needs, from SMB to enterprise. ISA series appliances can be deployed to the data center or cloud as virtual appliances and are also available as fixed-configuration rack-mounted hardware.

Architecture and Key Components

Ivanti Connect Secure is available on Ivanti Security Appliance (ISA) as hardware or as a virtual appliance as noted below.

Ivanti Security Appliance (ISA) Series

- ISA 6000 Appliance: Fixed configuration, 1U rack-mounted appliance supports up to 2,500 concurrent users.
- ISA 8000 Appliance: Fixed configuration, 1U rack-mounted appliance supports up to 25,000 concurrent users in stand-alone mode and up to 45,000 concurrent users in cluster mode subject to traffic types.
- Virtual Appliances (ISA-V Series): VMware ESXi, KVM, Microsoft Hyper-V, Nutanix, Microsoft Azure, Amazon Web Services and Google Cloud Platform.
- Virtual Appliances (ISA-V Series) include:
  - ISA4000-V: supports up to 250 users.
  - ISA6000-V: supports up to 2,500 users.
  - ISA8000-V: supports up to 25,000 users. Ivanti Connect Secure (ICS).

Ivanti Connect Secure (ICS) Security Standards and Certifications

Ivanti Connect Secure (ICS) adheres to National Institute of Standards and Technology (NIST) Federal Information Processing Standards (FIPS) and National Information Assurance Partnership (NIAP) standards to ensure the security and interoperability of systems and products, and to protect the confidentiality, integrity and availability of data.

Ivanti Connect Secure (ICS)	NIST / FIPS: Certified by using openSSL.org's FIPS provider/module in ICS 22.6R2 or later.
Ivanti Secure Access Client (ISAC) for Windows	NIST / FIPS: 22.7R2 or later based on openSSL.org Cert #4282.
ISAC for macOS	NIST / FIPS: 22.7R2 or later based on openSSL.org Cert #4282.
ISAC Mobile – iOS, Android	NIST / FIPS: SafeLogic based Cert #1938.

Features in 25.x

Ivanti Connect Secure (ICS)

Feature	Benefit
Oracle Linux 9 OS **Whitepaper:** The Role of Operating Systems in IT and Security Strategy	■ Greater memory support: 64-bit OS can address more memory (RAM), enabling Connect Secure to handle larger datasets and more simultaneous users ■ Increased security: 64-bit user space enhances protection against memory-based attacks ■ Improved performance: Applications can leverage 64-bit processing power, resulting in faster data processing, higher throughput, and better overall performance ■ Enhanced scalability: Supports larger database sizes, more connections, and resource-intensive applications, making it suitable for enterprise-scale workloads ■ Futureproofing and compatibility: Newer Oracle features and software updates are optimized for 64-bit platforms, ensuring ongoing compatibility and support for a wide variety of 3rd party software libraries
SELinux	■ Provides fine-grained, mandatory access control that dramatically limits potential damage from compromised applications or processes, even if such processes run as root. Enabled in enforcement mode by default in ICS.
NGINX with integrated Web Application Firewall (WAF) configuration for ICS gateways	■ Inspects and stops Layer 7 (application) attacks over HTTP traffic terminating on Connect Secure gateways ■ Prevents attacks such as SQL injection, cross-site scripting (XSS), and other web exploits ■ Minimizes attack surface
Key Management - Unique, randomized keys for every gateway - Utilizes TPM/vTPM (Trusted Platform Module) implementation for robust key management	■ Enhances security by minimizing risk of breach ■ Reduces impact of key compromise ■ Prevents sensitive data leakage / compromise ■ Elevates security posture
Secure Boot / Factory Reset - Provides enhanced integrity checks at boot time to thwart low level malware persistence - Ensures integrity of critical file systems remains intact during factory reset for ISA hardware devices and VMs running ICS software images - Incorporates Trusted Platform Module (TPM)	■ Protects integrity of boot process by verifying an established chain of trust ■ Extends chain of trust validations to additional file systems, further safeguarding their integrity ■ Prevents loading of low-level malicious code from boot partitions ■ Prevents attacker persistence at low level files systems ■ Enhances security by reducing risk of compromise

Features in 25.x - Ivanti Connect Secure (ICS)

Feature	Benefit
Secure Boot / Factory Reset – Virtual Appliances - Ensures only trusted and verified code runs at startup with secure boot implementation for virtual appliances. - Validates firmware and OS integrity during boot - Utilizes vTPM (virtual Trusted Platform Module)	■ Virtual appliances include all hardware appliance secure boot and factory reset features, plus... ■ Safeguards systems from tampering, unauthorized changes, or malware injection ■ Ensures trusted execution across virtual appliances
Root Privilege Avoidance (NRP) - System processes are denied full administrator rights by default, and are run with the least privileges required, for example, as unprivileged or dedicated service accounts	■ Limits access to only the required files and system resources ■ Limits attack surface ■ Reduces risks and limits potential harm
Debug Web Server Logs	■ Provide debug severity codes for web-related events
Multi-factor Authentication (MFA)	■ Requires users to provide two or more independent methods of verification to access an account or system ■ Enhances security by making it much harder for unauthorized users to gain access, even if they have obtained a password

Features in 25.x - Ivanti Secure Access Client (ISAC)

Feature	Benefit
Desktop and Mobile Platform Support	■ Desktop – Windows (Intel x86 and ARM), macOS (Intel and ARM) M1/M2/M3/M4, Linux ■ Mobile – iOS, Android, Android App on ChromeOS
Fully Qualified Domain Name (FQDN) Split Tunneling - Enables users to securely access specific resources over VPN (based on domain names, not just IP addresses) - Allows other internet traffic to route directly (outside the VPN)	■ Improves network efficiency and resource utilization ■ Reduces VPN bandwidth usage ■ Enhances user experience by routing only necessary traffic through the secure tunnel
Fast Identity Online (FIDO) - Latest standard: FIDO2	■ Provides more secure and friendly authentication without passwords ■ Utilizes passkeys, biometrics, PINs

Features in 25.x - Neurons for Secure Access (nSA)

Feature	Benefit
Run External Integrity Checker Tool (ICT) - Scans from nSA to single or multiple gateways with a single click - Security utility designed to verify the integrity of key files and system components - Detects unauthorized changes, corruption, or tampering	■ Aids in identifying potential compromises or anomalies by comparing files against known good baselines ■ Enables faster response to threats and maintaining system trustworthiness ■ Provides an alert if there is an anomaly in the executed ICT on a gateway ■ Enables admins to select a version-specific ICT package, execute against one or multiple ICS gateways, and view the results on the same page where the ICT is executed
Advanced HTML5 Feature license Management	■ Managing HTML feature licenses brings cost, legal, security, and operational benefits ■ Enables organizations to control and audit the web technologies available to users or developers.
Alerts and Notification Enhancements	■ Email-based alerts provide ICS gateway status

Features and Benefits

Feature	Description
Layer 3 VPN	■ Dual-transport (SSL + Encapsulating Security Payload) full Layer 3 VPN connectivity with granular access control. ■ "Always-on VPN with Lockdown Mode" and "VPN Only Access" modes for Compliance (VPN connection automatically connects/disconnects based on user's location). ■ Machine-based VPN with ability to step up to user-based authentication after user log-in. ■ "On Demand VPN" and "Per App VPN" for seamless and secure end-user experience.
Layer 4 VPN	■ Client/server proxy application that tunnels traffic from specific applications to specific destinations. ■ The Windows version of the Secure Application Manager (PSAM) enables secure traffic to individual client/server applications and application servers. ■ The Java version of the Secure Application Manager (JSAM) provides support for static TCP port client/server applications.
Conditional Access	■ Validates and verifies devices and users via a set of automated policies to protect networks and data. Each access attempt is evaluated dynamically and controlled in real time based on the policies in effect.
Advanced User Portal (Layer 7/Clientless VPN)	■ Secures clientless access from any HTML5-capable browser to published and/or user-added applications and links. ■ Dynamically generated based on user role. ■ RDP/VNC/SSH access with Advanced HTML5. ■ Web rewriter and web proxy built in. ■ Multi-portal support (e.g., SSO portal for employees, 2FA portal for contractors). ■ Support for Windows Terminal Services, VDI (Citrix, VMware) and File Browsing.
Optimized end-user experience	■ Smooth roaming from remote access to local LAN access (Ivanti Policy Secure). ■ Single Sign On (SSO) for rapid, secure access from remote or on-site locations (via integration with Ivanti Connect Secure and Ivanti Policy Secure).
Stateful endpoint integrity and assessment	■ Assesses and remediates end-user devices prior to authentication with easy policy definitions. ■ Windows, MacOS, Apple iOS and Android.

Features and Benefits (continued)

Feature	Description
Flexible launch options (standalone client, browser-based launch)	■ Users can easily launch SSL VPN via their web browser or directly from their devices. ■ Auto Connect feature allows devices to automatically connect to VPN, either when the machine starts or user logs on. ■ VPN on demand feature leverages OS capabilities for auto triggering VPN seamlessly in the background when an approved application needs corporate access.
Supports Cloud Secure Solution	■ Blend cloud and data-center access into a seamless user experience for next-generation workers. ■ Add compliance rules for hybrid DC access.
Pre-configuration options (Windows and Mac only)	■ Administrators can preconfigure a deployment with a list of gateways for end users to choose.
Authentication options	■ Adaptive Authentication using dynamic, multi-factor authentication using several user attributes. ■ Administrators can deploy Ivanti for remote user authentication using a wide array of authentication mechanisms, including biometric authentication support with Windows Hello for Business, hardware token, smart card, soft token, Google Authenticator, one-time passwords and certificate authentication. ■ Administrators can send AAA traffic via a desired interface (internal / external / management) for delegating user authentication to an Identity Provider. ■ OAuth/OpenID Connect support allows integration with any standard OpenID Provider like Google, OKTA, Azure AD, etc., while connecting to Connect Secure (acting as Relying Party).
VDI support	■ Ivanti supports the latest versions of VMware Horizon and Citrix XenApp / XenDesktop.
Granular SSL Cipher Configuration	■ Enables the administrator to select specific ciphers over those pre-configured for highly secure compliance.
REST API	■ A comprehensive REST-based API for programmatic access to the appliances.
Secure Boot with Trusted Platform Module (TPM)	■ Enhanced integrity checks at boot time to thwart low-level malware persistence ■ Utilizes unique and random encryption key at instance level ■ Hardware appliances have integrated TPM chip ■ Virtual appliances use virtual TPM from underlying cloud/hypervisor platform

Rich Access Privilege Management Capabilities

Feature	Description	Benefit
Dynamic role mapping with custom expressions	■ Combines network, device and session attributes to determine which types of access are allowed. ■ A dynamic combination of attributes on a per-session basis can be used to make the role-mapping decision. ■ Through MDM integration, fetches device attributes and applies policy decisions appropriately before granting access.	■ Enables the administrator to provision by purpose for each unique session.
Support for RSA Authentication Manager	■ RSA Authentication Manager risk-based authentication.	■ Provides another authentication layer option.
Standards-based built-in Time-based One-Time Password (TOTP)	■ Enables multi-factor authentication using smartphones.	■ Leverages smartphones to roll out a cost-effective and self-service two-factor authentication mechanism, where one-time passcodes are generated by a mobile app.
Multiple sessions per user	■ Allows remote users to launch multiple remote-access sessions.	■ Enables remote users to have multiple authenticated sessions open at the same time, such as when accessing VPN from a laptop and a smartphone simultaneously.
User record synchronization	■ Supports synchronization of user records such as user bookmarks across different Ivanti Appliances.	■ Ensures a consistent experience for users who often travel from one region to another and therefore need to connect to different Ivanti Appliances running Ivanti Connect Secure.
Mobile-friendly SSL VPN login pages	■ Provides predefined HTML pages that are customized for mobile devices, including Apple iPhone, iPad and Google Android.	■ Provides mobile device users with a simplified and enhanced user experience and web pages customized for their device types.
Integration with strong authentication and identity and access management (IAM) platforms	■ Ability to support SecurID, Security Assertion Markup Language (SAML) including standards-based SAML v2.0 support and public key infrastructure (PKI)/digital certificates. ■ OAuth/OpenID Connect Support.	■ Leverages existing corporate authentication methods to simplify administration.

Ease of Administration

Feature	Description	Benefit
Neurons for Secure Access	■ Optional centralized management, analytics and reporting platform for Ivanti Connect Secure deployments. ■ Full configuration management, one-click upgrades, centralized logging, custom reporting and troubleshooting. ■ "Lift and shift" configurations through configuration templates and multi-node configuration management.	■ Centralized configuration and gateway lifestyle management saves time and money. ■ Enhanced behavioral analytics identify and automatically act on risky user behavior before it becomes a problem. ■ Simplifies management of multi-node or global deployments.
Mobile Device Management (MDM) integration	■ Enables consolidated reporting and dashboards for simplified management. ■ Leverages MDM attributes for more intelligent and centralized policy creation. ■ Facilitates transparent "no touch" MDM-based deployment of Ivanti Clients to iOS and Android devices.	■ Extends MDM investments to gain comprehensive endpoint visibility and support additional mobile use cases.
Bridge Certification Authority (BCA) support	■ Bridge CA is a PKI extension that cross-certifies anchors (Root CAs). ■ Supports federated PKI deployments with client certificate authentication. ■ Enables customers to configure policy extensions in the admin UI, to be enforced during certificate validation.	■ Enables customers who use advanced PKI deployments to deploy Ivanti Appliances to perform strict standards-compliant certificate validation before allowing data and applications to be shared among organizations and users.
Multiple hostname support	■ Ability to host different virtual extranet websites from a single appliance.	■ Eliminates the cost of incremental servers. ■ Provides a transparent user experience with differentiated entry URLs. ■ Eases management overhead.
Customizable user interface	■ Creation of completely customized sign-on pages.	■ Provides an individualized look for specified roles, streamlining the user experience.

Flexible Single Sign-On (SSO) Capabilities

Feature	Description	Benefit
SAML single sign-on for cloud and web applications access	■ SAML 2.0-based SSO to a variety of web applications, including many of today's most popular Software as a Service (SaaS) applications. ■ Includes SSO functionality, even when connecting via an Ivanti Connect Secure Layer 3 VPN tunnel. ■ Ivanti Connect Secure supports deployments as both a SAML Identity Provider (IdP) and as a SAML Service Provider (SP).	■ Single sign-on to a user's web and cloud-based applications, simplifying the user connectivity experience.
Kerberos Constrained Delegation	■ Support for Kerberos Constrained Delegation (KCD) protocol. ■ Enforces KCD for Exchange Active Sync traffic, requiring client certificates, trusted CA certificates and proper delegation policies for authentication.	■ Eliminates the need for companies to manage static passwords, reducing administration time and costs.
Kerberos SSO and NT LAN Manager (NTLMv2) support	■ Ivanti Connect Secure will automatically authenticate remote users via Kerberos or NTLMv2 using user credentials.	■ Simplifies the user experience by eliminating their need to enter credentials multiple times to access different applications.
Password management integration	■ Standards-based interface for extensive integration with password policies in directory stores (LDAP, AD and others).	■ Leverages existing servers to authenticate users. ■ Users can manage passwords directly through the Ivanti Connect Secure interface.
Web-based SSO basic authentication and NTLM	■ Enables users to access other applications or resources protected by another access management system without re-entering login credentials.	■ Alleviates the need for users to enter and maintain multiple sets of credentials for web-based and Microsoft applications.
Web-based SSO forms-based, header variable-based, SAML-based	■ Ability to pass username, credentials and other customer-defined attributes to the authentication forms of other products and as header variables.	■ Enhances user productivity and provides a customized experience.
OAuth/OpenID Connect	■ OAuth/OpenID Connect support allows integration with any standard OpenID Providers like Google, Okta, Azure AD, etc., while connecting to Connect Secure (acting as Relying Party).	■ Integrate into existing OAuth deployments for easy user ID federation.

Provision by Purpose

Feature	Description	Benefit
Ivanti Secure Access Client	■ Unified, integrated, remote access client that can also provide LAN access control and dynamic VPN features to remote users.	■ Ivanti Secure Access Client replaces the need to deploy and maintain multiple, separate clients for different functionalities such as VPN and LAN access control. End users simply "click and connect" the connection they need.
Clientless core web access	■ Secure access to different types of web-based applications, including today's most common applications such as Outlook Web Access, SharePoint and many others. ■ Remote Desktop Protocol (RDP) access in Ivanti Connect Secure can be delivered over HTML5, via third-party RDP.	■ Provides the most easily accessible form of application and resource access from a variety of end-user devices with extremely granular security control options. ■ Completely clientless approach using only a web browser.
IKEv2 support for mobile devices	■ Enables remote users to connect from any mobile device that supports Internet Key Exchange (IKEv2) VPN connectivity. ■ Administrator can enable strict certificate or username/password authentication for access via IKEv2.	■ Full L3 VPN support for new devices that support IKEv2 but for which a client is not yet available.
Virtual Desktop infrastructure (VDI) support	■ Allows interoperability with VMware View Manager and Citrix Xen Desktop.	■ Provides remote users seamless access to their virtual desktops hosted on Vmware and Citrix servers.
Zero Touch Provisioning	■ Deploy ICS using OpenStack KVM, VMWare, Hyper V and cloud (GCP, Azure, AWS). ■ Obtain initial configuration from local DHCP server without manual data entry. ■ Configure and manage via REST API.	■ Enhances admin productivity and provides a customized experience.
ActiveSync Proxy	■ Provides secure access connectivity (strong encryption + certificate authentication) from mobile devices (such as iOS or Android) to the Exchange Server via proxy, with no client software installation. Enables up to 5,000 simultaneous sessions.	■ Enables customers to allow many users (including employees, contractors and partners) to access corporate resources through mobile phones via ActiveSync.
Secure Application Manager (SAM)	■ A lightweight application download enabling access to client/server applications.	■ Enables access to client/server applications using just a web browser. Also provides native access to terminal server applications without the need for a preinstalled client.

About Ivanti

Ivanti is an enterprise software company that aprovides a comprehensive IT and security cloud-based platform. Ivanti provides software solutions that scale with our customers' needs to help enable IT and Security to improve operational efficiency while reducing costs and proactively reducing security risk. The Ivanti Neurons platform is cloud-native and is designed as a foundation of unified and reusable services and tools for consistent visibility, scalability and secure solution delivery. Over 34,000 customers, including 85 of the Fortune 100, have chosen Ivanti to meet challenges head-on with its end-to-end solutions. At Ivanti, we strive to create an environment where all perspectives are heard, respected and valued and we are committed to a more sustainable future for our customers, partners, employees and the planet. For more information, visit ivanti.com and follow @GoIvanti.

ivanti

For more information, or to contact Ivanti, please visit ivanti.com