

SINA® Workstation S

Mobil arbeiten, modern und sicher



Ihre Vorteile:

- » **2-Faktor-Authentisierung, Festplattenverschlüsselung und integriertes VPN**
- » **Paralleles Arbeiten in mehreren Windows- oder Linux-Arbeitsplätzen**
- » **Erweiterbar durch SINA Apps**
- » **Zentrale Management- und Remote-Administration**
- » **Zulassung für VS-NfD und VS-VERTRAULICH (offline)**

SINA Workstation S realisiert einen modernen und leistungsfähigen Arbeitsplatz, mit dem Sie sicher und gleichzeitig mobil unterwegs sein können. Die Sicherheitsplattform mit smartcardbasierter 2-Faktor-Authentisierung, Festplattenverschlüsselung und IPsec-gesicherter Kommunikation ist zugelassen für die Verarbeitung von Verschlusssachen.

Mit der SINA Workstation als Desktop, Notebook oder Tablet bewegen Sie sich jederzeit sicher und zugleich komfortabel in Ihrer vertrauten Arbeitsumgebung – online wie offline. Dabei haben Sie immer Zugriff auf Daten und Dokumente im Firmennetzwerk und können sämtliche Funktionen Ihrer gewohnten Anwendungen wie E-Mail und Textverarbeitung von jedem Ort der Welt aus nutzen. Mit dem Voice- und Video-Konferenzsystem sind Gespräche in Echtzeit – ohne separate Geräte möglich. Nach der PIN-Eingabe startet die SINA Workstation automatisch den Standardarbeitsplatz als Gastsystem. Die Unterschiede zum Arbeiten mit Ihrem bisherigen Windows-System sind marginal und für jeden Anwender intuitiv verständlich. Mit der SINA Workstation interagieren Sie einfach über die Statusleiste.

Sicherheitsarchitektur

Die SINA Workstation führt sogenannte Gastsysteme wie z. B. Windows oder Linux und deren Anwendungen in einer virtualisierten Umgebung aus. Dadurch werden Zugriffe auf Geräte und Schnittstellen, die das Gastsystem erkennt, unter der Kontrolle des SINA Sicherheitsbetriebssystems ausgeführt. Alle Festplattenzugriffe und Netzwerkverbindungen werden so automatisch und ohne weitere manuelle Interaktion des Anwenders von SINA verschlüsselt.

Zugriff auf die verschlüsselten Daten erhalten Nutzer nur mit einem PIN-geschützten SINA ID Token. Nach der PIN-Eingabe startet die SINA Workstation automatisch den Standardarbeitsplatz als Gastsystem.

Smartcardbasierte 2-Faktor-Authentisierung

Der SINA ID Token – entweder in Form einer Smartcard, eines USB-Tokens oder einer microSD-Karte – beinhaltet die initialen Konfigurationsdaten und Sicherheitsbeziehungen für die SINA Workstation. Er dient zudem als sicherer Speicher für kryptographische Schlüssel und Zertifikate.

Die Zugriffsrechte, d. h. welcher Nutzer mit seiner SINA Workstation auf welche Sicherheitsdomänen oder externen Schnittstellen zugreifen kann, können zentral über das SINA Management benutzer- und einstuftungsspezifisch vergeben werden.

Virtualisierung

Die Virtualisierungstechnik des SINA Sicherheitsbetriebssystems schottet die Gastsysteme vollständig ab. Ein paralleler Betrieb mehrerer Gastsysteme, die auch unterschiedlichen Sicherheitsdomänen zugewiesen sein können, macht es möglich, mit einem Gastsystem im internen VS-Netz zu arbeiten und gleichzeitig mit einem anderen System im Internet zu surfen – ohne dass die Gefahr besteht, das eigene Netz mit Schadsoftware zu kompromittieren.

Durch die Virtualisierung steht dem Gastsystem – unabhängig von der zugrundeliegenden Hardware – immer dasselbe virtuelle System zur Verfügung. Dadurch wird die Administration und der Austausch bzw. die Erneuerung von Hardware enorm vereinfacht. Die Virtualisierung ist

für den Desktopeinsatz optimiert und unterstützt beispielsweise gängige Audio- und Videogeräte.

Secure Label

Das Secure Label ist die Statusleiste der SINA Workstation und ist immer am oberen Bildschirmrand eingeblendet. Darüber können die wichtigsten Funktionen der SINA Workstation gesteuert werden, wie z. B. Umschalten zwischen Arbeitsplätzen, Starten eines neuen Arbeitsplatzes oder Verwalten von Netzwerkverbindungen.

ThinClients

Die SINA Workstation hat verschiedene Thin Clients integriert, um VPN-gesichert auf Terminal-Server zuzugreifen. Es werden verschiedene Industrieprotokolle wie Citrix ICA oder Microsofts RDP unterstützt.

VoIP-Telefonie-Session

Mit der VoIP-Session für SIP- und RTP-basierte IP-Telefonie ist ein VoIP-Telefonie-Client verfügbar. Eingehende Anrufe werden sowohl optisch im Secure Label angezeigt als auch akustisch signalisiert. Die VoIP-Session verfügt über eine intuitive Oberfläche, über die Standardfunktionen wie lokales und zentrales Telefonbuch sowie Anruflisten genutzt werden können.

SINA Apps

SINA Apps sind spezialisierte Gastssysteme mit festgelegten Aufgaben und erweitern die Einsatzmöglichkeiten der SINA Workstation. So sind mit den praktischen SINA Apps beispielsweise eine automatisierte Anmeldung an WLAN-Hotspots, der Start eines Video-Konferenzsystems oder anderer Kollaborationsanwendungen möglich. In Entwicklung sind auch ein Passwortresor und zusätzliche Thin Clients über SINA Apps für die SINA Workstation.

Zusätzliche Features

Mit Hilfe der Clipboard-Funktion können Daten (Text- & Bitmap-Grafiken) zwischen verschiedenen Arbeitsplätzen ausgetauscht werden – wenn es

der SINA Administrator konfigurativ erlaubt. Weiterhin bietet die SINA Workstation einen Energiesparmodus, um Akkulaufzeiten zu verbessern.

Zentrales Management / Remote Administration

Die Konfiguration der SINA Workstation im Netzwerk erfolgt zentral durch das SINA Management. Eine integrierte Public-Key-Infrastruktur (PKI) mit zugehörigem Benutzermanagement unterstützt wesentliche administrative Prozesse rund um den SINA ID Token, insbesondere dessen Personalisierung, die Generierung bzw. Aktualisierung von Schlüsseln und kryptographischen Parametern sowie die Verwaltung der zugehörigen PINs und PUKs.

Rechte können remote von einem SINA Administrator gewährt oder entzogen und die Konfiguration verändert werden. Für den einfachen Rollout und für die Fernadministration stehen leistungsstarke Anwendungen zur Verfügung, die in eigene Administrationsprozesse integriert werden können.

BSI-Zulassungen

Die vom BSI für die Verarbeitung, Speicherung und Übertragung von Verschlusssachen der Einstufungen VS-NUR FÜR DEN DIENSTGEBRAUCH zugelassenen SINA Workstations S adressieren nationale und internationale Sicherheitsnetze. Bei der SINA Workstation S sind sämtliche für den Schutz und den Betrieb des Clients erforderlichen Funktionalitäten in einer Hardwareplattform kompakt integriert.

Zulassungsrelevante Konstruktionsstände

SINA Workstation S	
Nationale Zulassungsgrade	vernetzt: VS-NFD offline: VS-VERTRAULICH*
Internationale Zulassungsgrade	vernetzt: NATO RESTRICTED; RESTREINT UE offline: NATO CONFIDENTIAL*; CONFIDENTIEL UE**/**
Softwareversion	3.3
Authentifizierungstoken	SINA Smartcard, SINA USB Token In den obigen Offline-Szenarien bspw. SINA mlDentity Token

Technische Daten

		SINA Workstation S X280	SINA Workstation S T480s	SINA Workstation S T580	SINA Workstation S M710q
Leistungsdaten					
Display	Größe, Typ	12.5" FHD IPS	14.0" FHD IPS	15.6" FHD IPS	23.8" (optional)
	Auflösung	1920 x 1080	1920 x 1080	1920 x 1080	1920 x 1080
CPU	Intel® Core™ Prozessor	i7-8550u	i7-8550u	i7-8550u	i7-6700t
Arbeitsspeicher		16 GB DDR4 SDRAM	24 GB DDR4 SDRAM	16 GB DDR4 SDRAM	16 GB (2x 8 GB) DDR4
Bootmedium	Solid State Disc	512 GB SSD	512 GB SSD	512 GB SSD	512 GB SSD
Schnittstellen					
USB 3.0	Standard	2x USB 3.0, 1x USB Type-C	2x USB 3.0, 1x USB Type-C	2x USB 3.0, 1x USB Type-C	6x USB
Smartcard-Leser	Für SINA Smartcards	■	■	■	in der Tastatur
Netzwerk	10/100/1000 Cu	■	■	■	■
		WLAN, Bluetooth, LTE	WLAN, Bluetooth, LTE	WLAN, Bluetooth, LTE	WLAN

Bezugsquellen

Behördenkunden in Deutschland können die SINA Komponenten aus dem Rahmenvertrag 5070 „Kryptogeräte der SINA Familie“ des Beschaffungsamtes des Bundesministeriums des Innern beziehen. Allen anderen nationalen und internationalen Kunden steht secunet gern zur Verfügung.

* Spezielle Anforderungen, z.B. hinsichtlich Abstrahlenschutz der verwendeten Hardware, entnehmen Sie bitte den VS-Zulassungsdokumenten.
** Gilt für den nationalen Gebrauch.

Weitere Informationen:
www.secunet.com/sina

secunet secunet Security Networks AG
Essen

Tel.: +49 201 5454 - 0
Fax: +49 201 5454 - 1000
E-Mail: info@secunet.com
www.secunet.com