opentext™

Data Sheet

Host Access Management and Security Server

Working alongside your OpenText™ Reflection, OpenText™ Rumba+ and OpenText™ InfoConnect software, Host Access Management and Security Server (MSS) streamlines and secures your host-access operation. Paired with your NetIQ Identity and Access Management (IAM) system, MSS seamlessly propagates changes to application settings and user-specific content—right now, from a central server, for immediate use by individuals or groups. Job satisfaction for you, stronger security for your host resources.

Product Highlights

Take Centralized Control

Secure host access management from your central console. Lock down hundreds (or thousands) of far-flung desktops with ease. Grant or deny access based on group or role via your IAM system. Apply changes quickly to align with business needs. Make post-install adjustments on the fly. Next time users launch a session, they'll receive the changes.

Use Strong Credentials to Bolster Security

With OpenText™ Host Access Management and Security Server (MSS), you can easily extend IAM security benefits to host systems. For example, use Active Directory or NetIQ eDirectory by OpenText™ to validate user credentials and grant access to host resources based on user/group definitions. Strengthen security with multifactor and certificate-based authentication. Minimize spoofing, man-in-the-middle attacks, and other network threats with PKI support, smart cards, and Kerberos. Securing your hosts is easier when you can leverage existing IT investments. As you integrate host access with IAM, you can replace weak, eight-character passwords with strong, complex ones. Implement best-fit multi-factor authentication (MFA) methods. Say goodbye to host passwords and automatically sign users on to their mainframe applications. It's safe, manageable, and economical with MSS.

Encrypt Data in Motion

MSS secures host data with SHA-256 digital signatures, AES 128/256, SSL/TLS, and cryptographic modules validated for FIPS 140-2—one of the U.S. government's top security standards. This high level of security protects your critical data and helps you keep pace with evolving regulatory standards.

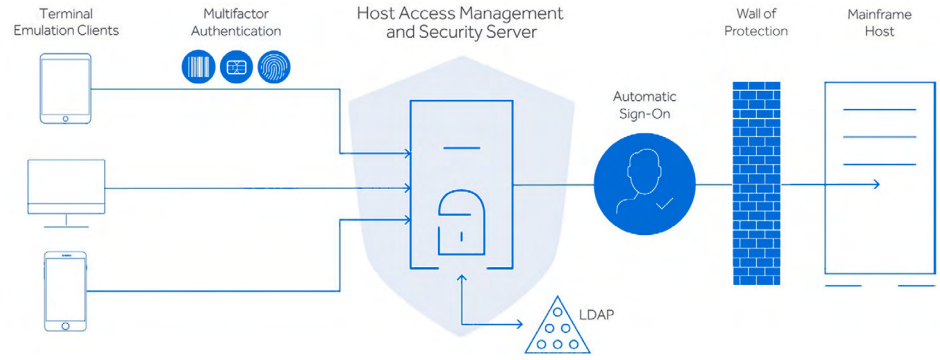
Know *Exactly* Who Is Accessing Your Critical Hosts

With MSS, you can log and monitor access to host resources from a centrally located metering server. You can create license pools to control access to sessions and hosts. You can also address specific needs with granular logging options—ensuring that you know who and when someone is accessing your critical host systems. Bottom line: Only authorized users and clients get in.

Quick View

- **New** Support for Kerberos Authentication for a Secure Windows SSO experience for the end user.
- **New** Support for TLS 1.3 in MSS and the MSS Security Proxy Add-on.
- Centrally manage certificates for IBM host systems.
- Strengthen security and streamline management by extending your identity and access management (IAM) system to host resources.
- Move from weak to strong multifactor authentication for your host resources.
- Transmit changes to security settings, application settings, and user-specific content from your central MSS console—making them immediately accessible to users.
- Use directory services, such as Active Directory, to authorize access to host applications—without changing your LDAP schema or data.

Connect with Us



MSS uses your IAM system to provide the strongest possible protection for host access and data. Ratchet up security with multifactor authentication. Get rid of mainframe passwords with automatic sign-on. Build a wall of security in front of your mainframe. Rest easy knowing your host systems are tightly locked down—no client or host changes necessary.

Reinforce Security with MSS Add-Ons

You'll gain additional critical functionality when you pair MSS with these products:

- **Security Proxy Add-On**—Security Proxy uses patented security technology to act as a proxy for terminal sessions. It provides token-based access control, routing encrypted host traffic to and from user workstations.
- **NetIQ Advanced Authentication Add-On**—NetIQ Advanced Authentication by OpenText™ provides a practical way to use multifactor authentication for authorizing access to your critical host systems. A range of authentication options gives you freedom to choose the best solution for your business.
- **Automated Sign-On for Mainframe Add-On**—Automated Sign-On for Mainframe uses your IAM system to automate sign-on to IBM 3270 applications. Connections are facilitated through the Digital Certificate Access Server (DCAS) on IBM mainframes, and users gain access using a single login. Say goodbye to your host password-management headaches.
- **PKI Automated Sign-On Add-On**—PKI Automated Sign-On enables secure, automated sign-on to enterprise applications. You can finally give these applications the security they deserve.
- **Terminal ID Management Add-On**—Terminal ID Management dynamically allocates terminal IDs based on username, DNS name, IP address, or address pool. It enables you to track ID usage and manage inactivity timeout values for specific users—conserving terminal ID resources and significantly reducing operating expenses.

When you team with MSS, everyone wins.

Learn more at
www.opentext.com

opentext™