Security white paper

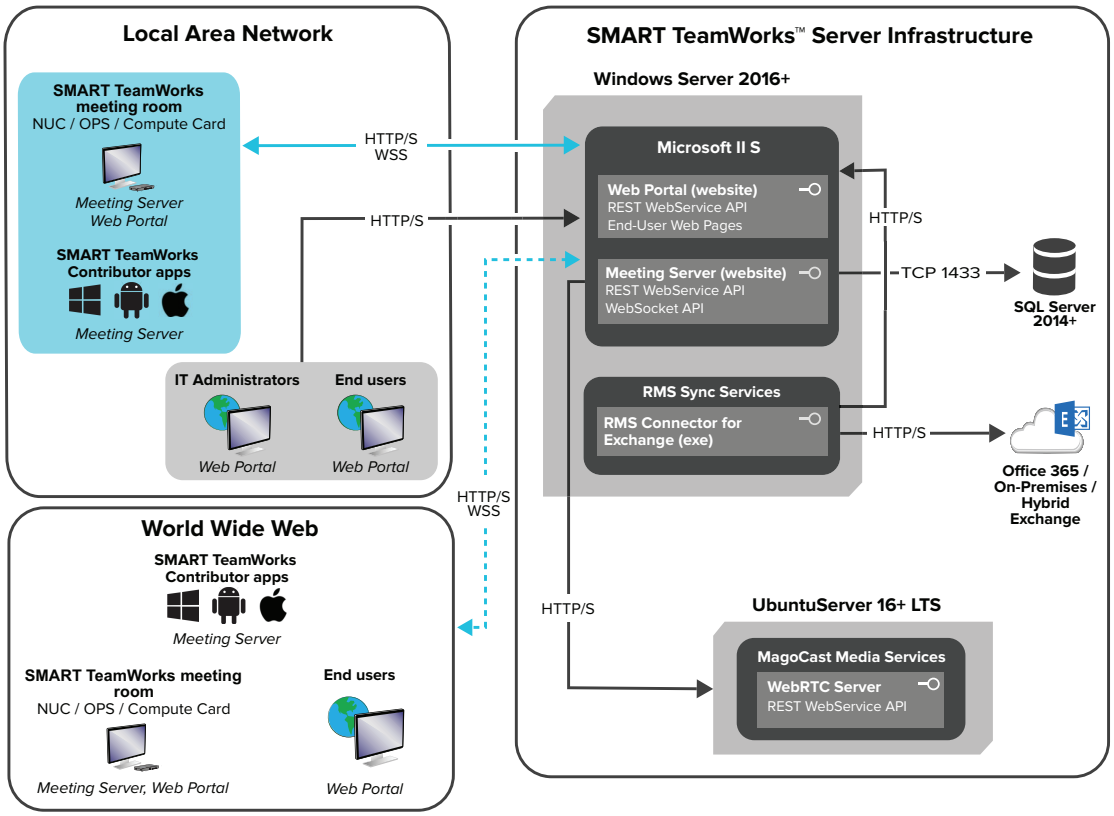
SMART TeamWorks™

Using SMART TeamWorks™, team members in various locations can work together in a real-time collaborative workspace as if they were in the same room. SMART TeamWorks provides video, voice, collaborative whiteboarding, wireless presentation, and document editing in a multi-page workspace.

Infrastructure

SMART TeamWorks Server uses a REST API provided by a back-end layer that is credential-secured over TLS 1.2, the successor protocol to the now-deprecated SSL protocol. Communication with the REST API and IIS services takes place over TLS (port 443) with 2048-bit asymmetric encryption and 256-bit symmetric encryption. SMART Board® interactive displays with SMART TeamWorks are authenticated on the servers using a four-step authentication process with SASL. Inbound and outbound data from the back-end layer is encrypted and transmitted with 2048-bit asymmetric encryption and 256-bit symmetric encryption using certificates from third-party credited authorities.

The back-end tier provides public services: REST API and IIS. Your organization can choose different back-end options for its deployment–on-premises or cloud-based (Microsoft® Azure®)–to provide a resilient, low latency and redundant back-end.



Although SMART TeamWorks Server supports HTTP connections (for internal lab and demo environments only), SMART strongly recommends the use of encrypted HTTPS over TLS 1.2 by default in a production environment.

SMART TeamWorks Server does not directly tunnel any service. Your organization can access only those resources that pass through the dedicated API interface after passing a double level of authentication.

SMART TeamWorks validates client inputs, verifying the presence of security tokens within the HTTP headers and checking the content of the client calls.

SMART TeamWorks implements strong custom authentication based on double security tokens. The first token is released at the first call and is mandatory for receiving the second token. The latest token is verified at the beginning of each client call.

SMART TeamWorks limits the authentication attempts a client can make within a time unit. SMART TeamWorks blocks potential attacker clients that exceed the limit.

SMART TeamWorks Server security

Separation of duties and “Least Privilege” security principles

“Least Privilege” security gives users only the minimum privileges needed for completing their daily tasks. To secure data and the system in general from potential damage, SMART TeamWorks Server identifies a comprehensive hierarchy of users and separate duties. SMART TeamWorks Server gives users separate IDs and only the permissions they require.

Role-based access control (RBAC)

SMART TeamWorks Server supports role-based access control (RBAC). Every meeting is managed by an owner who can control user permissions.

Purging policy for end user data (stateless configuration)

You can schedule a daily wipe of stored user data in a secured NFTS partition connected to the SMART TeamWorks Server architecture. End user data includes all meeting contents, IDs, PINs, and recap files.

Network security and firewall considerations

SMART TeamWorks client software requires internet access through these ports:

- TCP 80
- TCP 443
- UDP 53

If your organization is using layer 7 filtering or a proxy with protocol filtering on these ports, allow the following protocols:

- HTTP
- HTTPS
- DTLS
- DNS
- STUN
- TURN
- ICE

Proxy support

SMART TeamWorks supports the following proxies:

- HTTP proxy*
- SOCKS 5*
- Proxy auto-configuration (PAC) file*
- System proxy (Windows®)

Microsoft Azure deployment

Microsoft Azure data centers are geographically dispersed. The data centers comply with ISO/IEC 27001:2005, SOC 1, and SOC 2 and are CSA STAR certified.

Microsoft operates these data centers. Microsoft has decades of experience building enterprise software and runs some of the largest online services in the world.

On-premises deployment

TIP

On-premises deployment of SMART TeamWorks Server requires Microsoft IIS, Microsoft SQL Server®, and the NTFS file system.

SMART also recommends a layer 7 firewall to provide a high level of security and reduce exposure to zero day exploits.

*With or without authentication

SMART Board interactive displays with SMART TeamWorks security

SMART Board interactive displays with SMART TeamWorks are designed to be appliance-like, ensuring a consistent “walk-up” user experience without sacrificing security.

Security and lockdown

To allow the use of SMART Board interactive displays with SMART TeamWorks in communal spaces, such as meeting rooms, the custom operating system implements many of the security and lock-down features available in the Windows 10 operating system:

- UEFI secure boot
- User mode code integrity (UMCI) with Device Guard
- Application restriction policies using AppLocker®
- BitLocker® drive encryption
- Trusted Platform Module (TPM)
- Windows Defender
- User Account Control (UAC) for access to the Settings app

The custom operating system also offers these features to provide additional security:

- The custom shell and Start menu limit access to only meeting-related functions.
- The custom File Explorer grants access to only files and folders managed and set by your organization under **My Documents**, attached storage devices, or local-user mapped network drives.

Kiosk mode

The SMART TeamWorks user interface is designed specifically to support the large screens and touch features of SMART Board interactive displays. It doesn’t use the same shell as Windows 10 Enterprise operating system. SMART has removed a number of tools, such as the Command Prompt, Control Panel, and Registry Editor, to allow your organization to place SMART Board interactive displays with SMART TeamWorks in public without fear of tampering.

SMART TeamWorks is designed for use in communal spaces, such as meeting rooms. Unlike with Windows computers, anyone can walk up and use a SMART Board interactive display with SMART TeamWorks without signing in.

A local, auto signed-in, low-privilege user is always signed in to SMART TeamWorks.

Saving and browsing files during a session

By default, users can access only a limited set of folders on SMART TeamWorks during a session:

- **Meeting** (secure cache replicated during a session between clients)
- **Screenshots**
- **My Documents**

When users end a session in SMART TeamWorks, files attached to the meeting or added to the whiteboard session are deleted. If saving files is enabled by your organization, a user can save the file to a USB drive, email it, or disconnect the session from SMART TeamWorks Server if joined remotely.

Vigilant data safety

After each SMART TeamWorks session, data is wiped from the system to protect sensitive information. The next team to use the SMART Board interactive display has a blank session to start using.

Hard drive encryption

The SMART TeamWorks hard drive is encrypted by BitLocker. If someone removes the hard drive, they must provide the BitLocker key to re-enable the hard drive.

Ultrasonic pairing

Ultrasonic pairing is an optional method for transferring session connection credentials between the SMART Board interactive display and a contributor app on a mobile device. Configurable through SMART TeamWorks settings, it allows contributor apps to automatically join a session or to transfer a session initiated in the app to the interactive display.

Ultrasonic pairing works by broadcasting the meeting credentials (URL, meeting ID, and PIN) through an ultra-high frequency sound. It broadcasts in the 17.5 kHz to 20 kHz range.

For more information about ultrasonic pairing, see chirp.io/docs/data-over-sound-whitepaper.pdf.