AGAT mobileiron

SphereShield
Secure Skype For Business
Powered by MobileIron MDM

Background

Companies utilizing MobileIron face security challenges when deploying Skype for Business (SfB).
One significant threat is that the SfB app can be freely obtained and installed on any device. This allows any employee to install SfB on a personal device, outside MobileIron's control, and open a traffic channel into the company network bypassing MobileIron security controls. Such a device might be Jail-Broken or hacked and result in domain credentials theft and malicious traffic entering the network.
SkypeShield offers an integrated solution with MobileIron that allows organizations to verify that only devices that are managed by MobileIron and that are compliant with company security policy can use Skype for Business.

MAIN FEATURES

Restrict Skype for Business access to devices managed by MobileIron

- Restrict registration to MobileIron devices
- Conditional access based on MobileIron device security compliance settings
- Prevent access from jail broken or rooted devices
- Multi factor authentication based on MobileIron identity
- Optional no password SSO solution

In addition, the integration enables the organization to further secure the authentication process by using the MobileIron client's user identity as an additional authentication factor.

MobileIron Compliance Conditional Access

SkypeShield has developed a Mobile Device Management (MDM) Conditional Access Solution for Skype for Business, which is specifically designed to meet the security requirements of MobileIron MDM users.
SkypeShield's MDM conditional access solution verifies that only devices that are compliant with the company's security policy, as defined by MobileIron, can access the corporate network through Skype for Business.
SkypeShield's solution validates that devices are compliant with the settings defined by MobileIron.

If a device becomes non-compliant, all Skype for Business sessions are terminated automatically and access is immediately blocked.
So for example, Skype for Business access may be blocked to a device that has become jailbroken or rooted, or if the user has removed the device from MobileIron control.
During the sign-in process, and continuously thereafter, the solution verifies that the device is indeed listed as a valid device in the MobileIron core server and is not listed as Out Of Compliance.

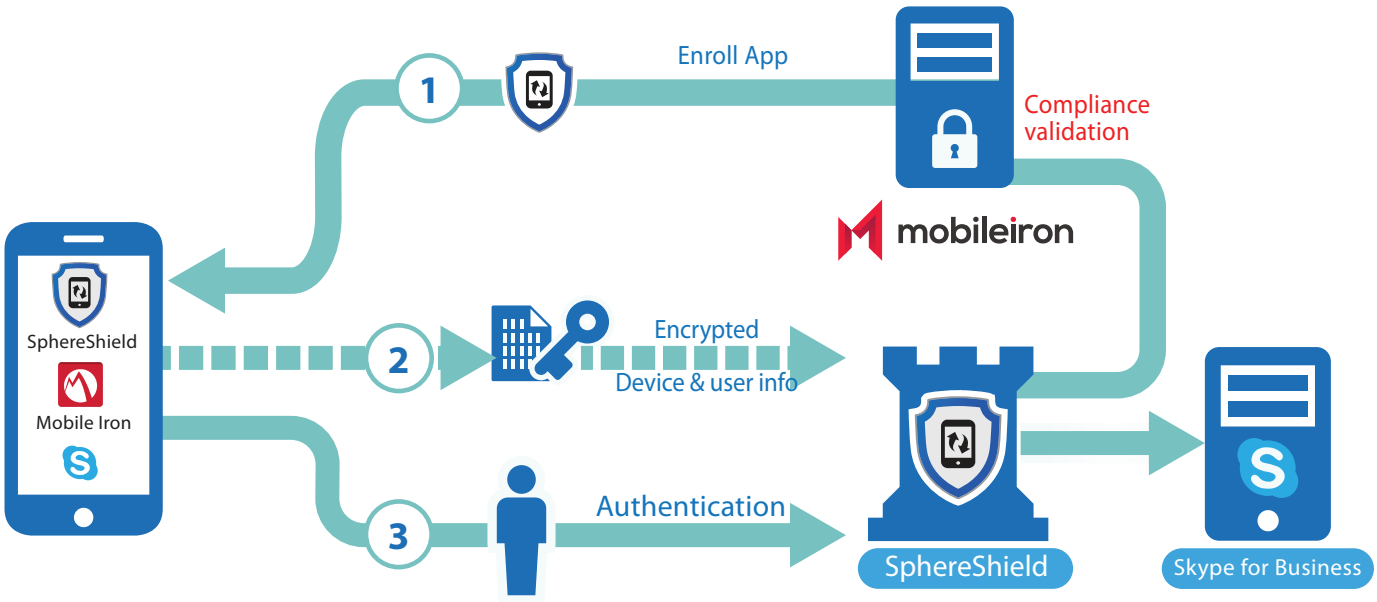
Leveraging MobileIron identity for secure authentication

SphereShield leverages MobileIron to securely identify the owner of the phone. Only a device that is registered on the MDM to a specific user can be used to sign in to that user's Skype for Business account.

This adds another security factor for the authentication, making the sign in process more secure while checking that the MDM identity match the Skype for Business user used for the specific device.

No Password authentication

By expanding the new integration developed with MDM, SkypeShield adds another security layer to the authentication process, by sending the user name from the MDM mobile device framework in parallel to the sign-in process. Based on this capability, SkypeShield offers a no-password authentication by trusting the MobileIron identity for the authentication.

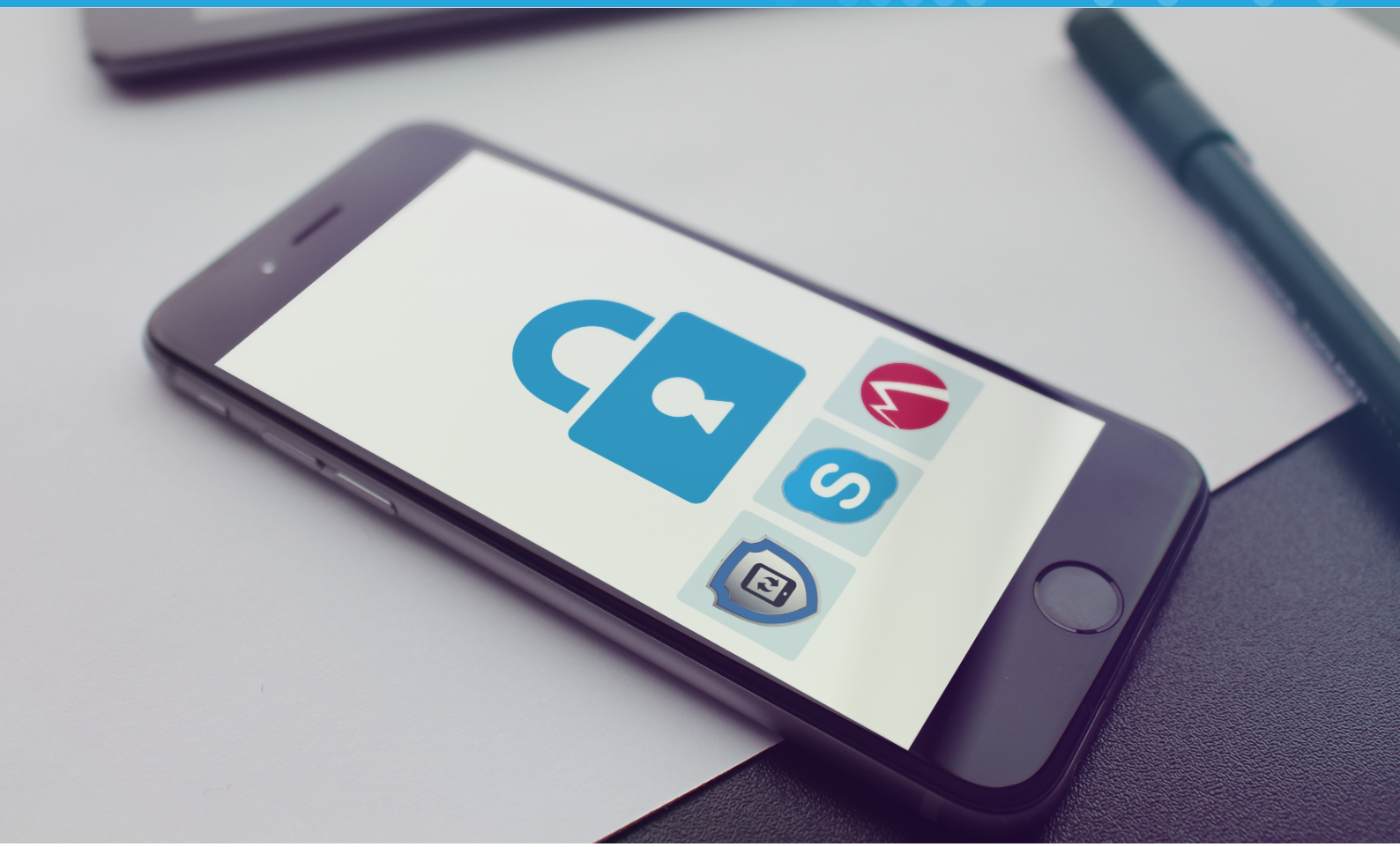


SphereShield Overview

SphereShield is an innovative solution that guarantees secure external Skype for Business (Lync) connectivity. SkypeShield allows users to safely connect to Microsoft Skype for Business servers from smartphone, tablets, desktop PCs and any other device outside the organization.
Connecting to the server using the Skype for Business client from external device poses several risks.
SkypeShield offers the following security features:

1. **MobileIron integration**
   Block access from devices that have become Out Of compliance or removed from MobiileIron control
   Read more
2. **Network protection**
   Protect against account lockout in DDoS attack. Device pre- authentication avoiding requests entering the organization's domain, unless coming from a registered device Read more
3. **Two Factor Authentication**
   TFA by TFA by requiring the device as the second factor in addition to credentials to Skype for Business & Exchange (EWS). Optionally can require 3three factor authentication based on VPN access / certificate. Read more
4. **Device Access Control**
   Restrict the usage of Skype for Business & Exchange only to registered devices. Several enrollment workflows, settings and web APIs are available to control the devices Read more
5. Active Directory credentials protection
   Avoid using and storing AD credentials on a device by defining dedicated Skype for Business-Lync credentials or by using RSA tokens.
   Read more
6. **Ethical wall**
   Solves ethical and compliance regulations, security and data protection issues by applying policies based on specific users, groups and domains/companies controlling activities such as IM, File transfer, Meeting, Audio, Video.
7. **Skype application Firewall**
   The firewall handles security threats related to guest and anonymous requests sent to the corporate network by performing data and protocol level Sanitization and rewriting-
   Read more
8. **DLP Engine**
   Apply content rules policies based on group membership with incident actions of block, mask or notify. Also supports commercial DLP integration with Symantec , ForcePoint (Websense), GTB and other vendors. Read more
9. **No password authentication**
   Allows to sign in without using password while trusting MDM identity
10. **Biometric authentication**
    Require fingerprint scan / Touch ID to sign into Skype for Business in addition or instead of password
11. * **Mobile smart card authentication**
    supports smart card authentication on mobile using Bluetooth readers (Gemlato , Feitian)
12. * **Secure meeting**
    Optionally require authentication from guests to verify participant identity
13. * **Authentication risk engine**
    Security alerts and action based on Geolocation information and behavior profiling

* *Coming soon*



SphereShield's client base consists of government offices, banks, insurance companies and large industrial global corporations, including Fortune 500 companies.

Please visit our sites at:

www.AGATSoftware.com

For more information
Contact us:
AGAT Software
Har-Hotzvim Hi-Tech Park
Jerusalem, Israel

Phone: +972-52-520-9860
info@agatsoftware.com

AGAT

Leading security for Skype for Business (Lync)