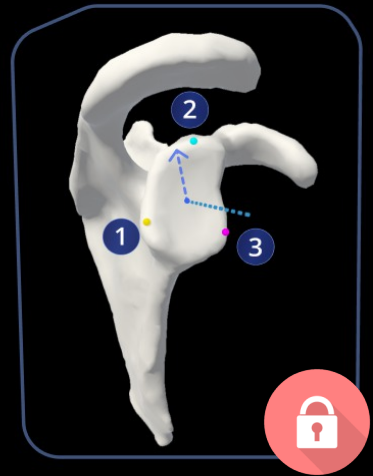
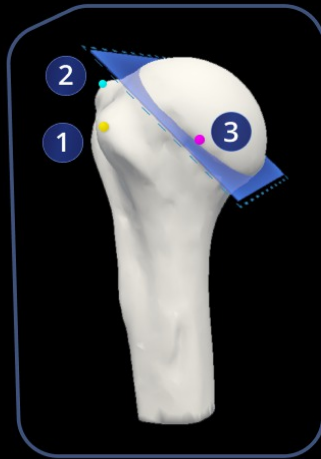




Signature™ Vision



Signature™ Vision

Mixed Reality Shoulder Navigation

Operator Instructions and Cybersecurity Considerations

Version 1.1, 2026-07-02

Table Of Contents

Table Of Contents.....	1
Terms and Abbreviations.....	3
Introduction.....	4
System Overview.....	5
SignatureOne Platform.....	6
USB Thumb Drive.....	6
OTS HMD.....	6
MDM Infrastructure.....	6
Provisioning Computer.....	6
WiFi Network.....	6
Crash Logging Service.....	6
Cybersecurity Considerations.....	7
Patient Data Protection.....	7
HMD Security Configuration.....	7
Network Requirements.....	9
Software Installation and Updates.....	10
Installation of Signature™ Vision.....	10
Updating Signature™ Vision.....	10
Device Management & Device Configuration Requirements.....	11
Configuration using MDM / MS InTune.....	11
Policy Settings.....	11
Sleep Settings (Optional).....	13
Configuration using Provisioning Profiles.....	15
Profile Settings.....	15
Sleep Settings (Optional).....	19
Provisioning Profile Installation.....	20
Servicing and Maintenance Tasks.....	21
Exporting and Deleting Log Files.....	23
Exporting Log Files.....	23
Delete Log Files from Device.....	23
Encryption Key Management.....	24
1. Generate Device Key Pair.....	25
2. Export Device Public Key.....	25
3. Import PMP Public Key.....	25
User-Defined Password / PIN.....	25
SBOM List.....	27
Regulatory Device Name.....	27
HMD Configuration Notice.....	28

Terms and Abbreviations

MDM	Mobile Device Management
Signature ONE	Signature ONE™ Planning Software of Zimmer Biomet used to create plans for Signature™ Vision
PMP	Personalized Medicine Portal. The portal to download the patient case files
Provisioning Profile	A Provisioning Profile contains device policies and operating system configurations.
Signature™ Vision	A mixed-reality navigation software used for shoulder arthroplasty
OTS	Off The Shelf
HMD	Head Mounted Display (OptiVu Tilt with HoloLens 2)
PHI	Protected Health Information
UI	User Interface
USB	Universal Serial Bus
SBOM	Software Bill of Material
Wi-Fi	Wireless Network

Introduction

This document is intended for operators responsible for managing Signature™ Vision devices and related infrastructure. It provides a system overview, outlines the network requirements for integrating the devices into an existing network infrastructure, detailed procedures for device management and provisioning, and offers instructions for essential servicing tasks. This includes the initial encryption key exchange required for Signature™ Vision to decrypt patient case files from Signature ONE/PMP.

The scope of this document excludes guidance on managing the OptiVu™ Shoulder Trackers and other instruments or tools.

System Overview

Signature™ Vision consists of multiple components. The following diagram illustrates the system from a cybersecurity perspective, highlighting all relevant components, which are described in detail in the sections below.

The diagram describes the two scenarios of provisioning (configuration profile and software deployment to the devices), using **MDM Infrastructure**, and **USB provisioning** (offline).

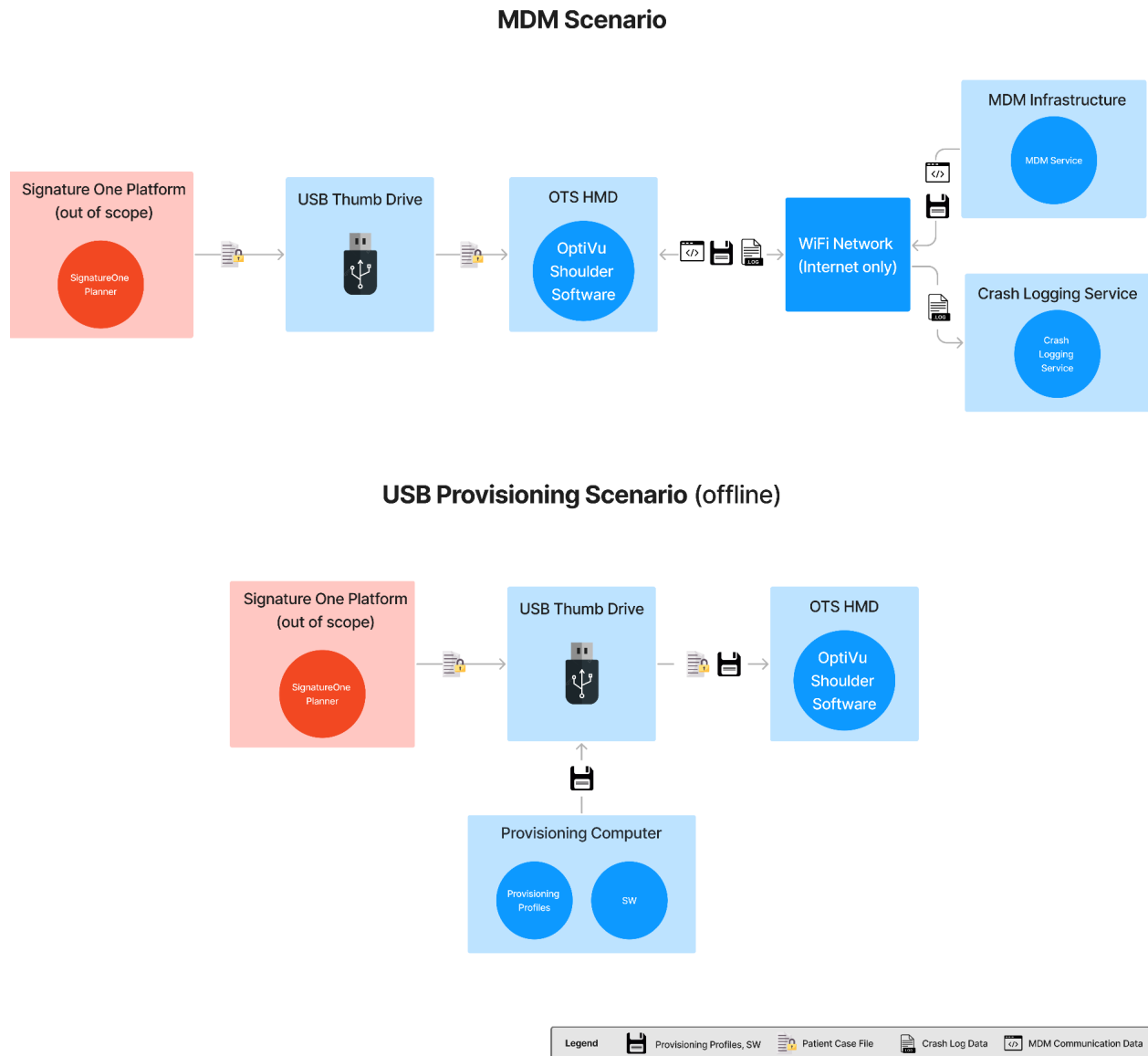


Figure 1: System Overview Diagram

SignatureOne Platform

The Signature ONE Planning tool is used to plan patient cases. Once a plan is approved by the surgeon, they can download the case to a USB thumb drive. Before download, the case gets encrypted with several layers of cryptographic keys and a user-defined password.

USB Thumb Drive

The USB-C thumb drive is used to transfer the downloaded patient case files to the HMD. In case of USB Provisioning, a USB thumb drive is used for deploying the SW and configuration profiles (not the same thumb drive).

OTS HMD

The Head Mounted Display (HMD), the OptiVu Tilt with HoloLens 2, is the device the surgeon wears during navigation. It imports the patient case files from the USB-C thumb drive. Using the Signature™ Vision software, the system supports the surgeon with navigation during shoulder arthroplasty.

MDM Infrastructure

The HMD devices can be managed using a Mobile Device Management (MDM) solution. We recommend using Microsoft Intune (cloud-based, deployment to the HMD via Wi-Fi).

The MDM distributes software updates, manages user logins, and enforces security policies.

Provisioning Computer

If no Mobile Device Management (MDM) solution is employed to deploy the software and device configurations, the HMD can be provisioned using provisioning profiles that are deployed on a USB thumb drive. The computer used to create these provisioning profiles and copy the USB thumb drive is known as the Provisioning Computer.

WiFi Network

In the MDM-managed device scenario, the HMD needs to be connected to a Wi-Fi network to receive software updates and device configuration through the Mobile Device Management (MDM) solution. Only connect the HMD to a secure Wi-Fi network that features either WPA2 or WPA3 wireless security protocols.

The HMD does not need to access the hospital network directly. An isolated connection to the internet is sufficient (see section [Network Requirements](#)).

However, the Signature™ Vision software can run completely offline using USB provisioning.

Crash Logging Service

In case of software crashes, the Signature™ Vision software generates a crash report that is sent to a crash logging service for maintenance. The data sent to the crash logging service do not contain any PHI. In case the device is used offline, the crash reports are cached locally and sent once a connection to the crash logging service is established. If the device is never joined to a network connection, the crash logs are retained to maintain storage space.

Cybersecurity Considerations

As shown in the System Overview diagram above, Signature™ Vision comprises a limited number of components. From a cybersecurity perspective, it is crucial to ensure that no patient data, including potential Protected Health Information (PHI), is exposed by the device or network. Additionally, measures must be taken to minimize the system's attack surface against potential malicious actors.

Patient Data Protection

The HMD and USB thumb drive for patient data used for the system should be stored in a secure location with access restricted to authorized personnel only. Additionally, all patient cases are encrypted with multiple layers of cryptography. This includes asymmetric encryption based on shared keys, as well as symmetric encryption using a user-defined password.

The patient case files are downloaded from the PMP portal and encrypted. The files get transferred via a USB storage device to the HMD. The Signature™ Vision application then copies the files to the local device storage. The Signature™ Vision application allows for storing 20 patient case files on the device. The user needs to manually remove cases no longer needed.

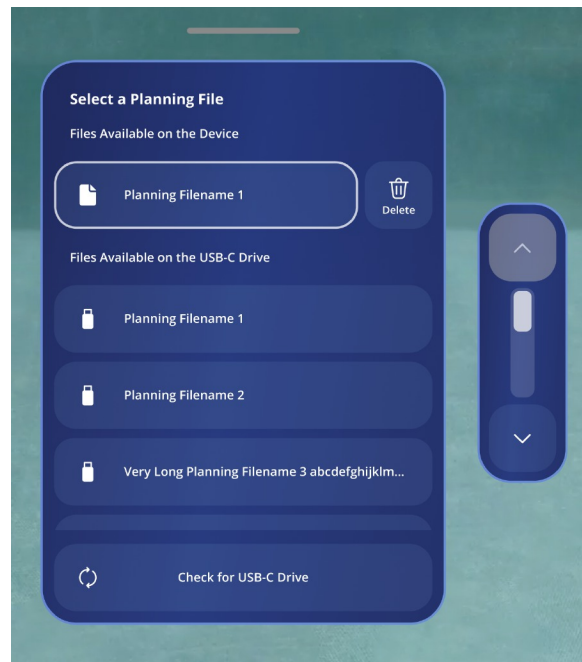


Figure 2: Planning File Selection seen on HMD

The Signature™ Vision application does not alter patient case files nor transmit them to any external server or service.

HMD Security Configuration

The Head-Mounted Display (HMD) must be configured to enforce specific security policies. This can be achieved using a Mobile Device Management (MDM) solution or USB provisioning profiles. These policies include disabling the HMD's ability to take pictures or record videos, restricting microphone and camera use to the Signature™ Vision application only, and running the Signature™ Vision application in Single Kiosk mode.

Refer to the [Device Management](#) section for a comprehensive list of mandatory policies applicable to all HMD devices.

When performing device management using local provisioning profiles, the USB thumb drive containing the provisioning profiles should be stored in a secure location with access restricted to authorized personnel only. The PC used to create the provisioning profiles shall be protected with a strong password.

When performing device management using a cloud-based MDM, ensure that access to the MDM is protected with a strong password and two-factor authentication.

Network Requirements

The Signature™ Vision device does not require network connectivity during routine operation, as patient case data are transferred via a USB-C thumb drive. However, Wi-Fi connectivity is necessary for device maintenance to enable software updates and configuration management in case the HMD is managed by an MDM solution.

To facilitate updates and configurations, certain service endpoints must be accessible. The following table assumes that Microsoft Intune is used for device management.

Access to the crash logging service endpoint is optional but recommended. When enabled, crash report data will be sent to sentry.io to support maintenance and SW crash investigation.

The following table lists all required endpoints for each HMD.

Service	Description	Required	Endpoint Domain	Ports
Microsoft Intune MDM	MDM solution managing the devices, including the distribution of software updates.	Yes	*.manage.microsoft.com	80, 443 (in/out)
Crash Logging Service	Service to receive crash reports for maintenance	No	*.sentry.io	80, 443 (in/out)

Network operators should configure firewall rules accordingly.

When devices are provisioned using USB profiles, software updates are handled by returning the hardware to the distributor. This approach allows the devices to function in a fully offline capacity, requiring no network connectivity.

Software Installation and Updates

Signature™ Vision operates on managed HMD devices, which is achieved using either:

1. Via **Microsoft Intune**: please refer to Microsoft's documentation:
<https://learn.microsoft.com/en-us/mem/intune/>
2. Via **Provisioning Packages**, please refer to
<https://learn.microsoft.com/en-us/windows/configuration/provisioning-packages/provisioning-packages>

Installation of Signature™ Vision

The Signature™ Vision application is deployed through an MDM solution or provisioning profiles transferred to the HMD via a USB thumb drive. For instructions on distributing and installing the application, please consult your MDM provider's documentation or the provisioning packages documentation from Microsoft mentioned above.

After the initial installation, manual setup tasks must be completed by a field service engineer or technician. These tasks include generating initial encryption keys and conducting the initial exchange of public keys between the device and the PMP portal to enable decryption of protected patient case files. Refer to the [Servicing and Maintenance Tasks](#) section, specifically [Encryption Key Management](#), for more details.

Updating Signature™ Vision

The Signature™ Vision application is updated via the MDM solution or by returning the device to the distributor. Refer to the MDM provider's documentation for update procedures when using an MDM solution.

Please note that initially generated private/public keys are retained during updates. However, **if the software is uninstalled before a new version is installed, or the device has been re-flashed, the key pairs must be re-generated and exchanged between PMP and the device.** See the [Servicing and Maintenance Tasks](#) section, specifically [Encryption Key Management](#), for more details.

Device Management & Device Configuration Requirements

The HMDs must be configured to ensure that Signature™ Vision can be used safely and securely in the operating room. Operators are required to implement the specified configurations and policies to minimize unintended use, prevent data leakage (including Protected Health Information, or PHI), and mitigate cybersecurity risks.

The following tables outline the policies that must be applied and pushed to all HMD devices running Signature™ Vision, configured either via Microsoft Intune or when generating the provisioning profile for the HMD.

Configuration using MDM / MS Intune

Employing a Mobile Device Management (MDM) solution, such as Microsoft Intune, facilitates the centralized administration of HMD hardware. Key capabilities include executing remote data erasure, deploying over-the-air software updates, and ensuring the persistent enforcement of security policies and device configurations.

For the deployment of Signature™ Vision via an MDM infrastructure, onboard the hardware following the provider's protocols or consult with your designated integration partner. During the profile creation phase, it is mandatory to incorporate all security policies specified in the following sections.

Policy Settings

User Authentication

The OTS HMD must be configured to force users to log in each time they use the device.

Policy CSP	/DeviceLock/ DevicePasswordEnabled
Value	0 (enabled)

Disable Bluetooth

The OTS HMD must be configured to disable Bluetooth connections.

Policy CSP	/Connectivity/ AllowBluetooth
Value	2 (disable)

Policy CSP	/Bluetooth/ AllowDiscoverableMode
Value	0 (disable)

Disable Camera for Other Applications, Disable Taking Pictures and Videos

The OTS HMD must be configured to prevent applications other than Signature™ Vision from accessing the camera and disabling the recording of videos and taking pictures on the HMD.

Policy CSP	/Privacy/ LetAppsAccessCamera
Value	2 (force deny)

Policy CSP	/Privacy/ LetAppsAccessCamera_ForceAllowTheseApps
Process	SignatureVision_pzq3xp76mxafg

Disable the Microphone for Other Applications

The OTS HMD must be configured to prevent other applications than Signature™ Vision from accessing the microphone.

This cannot be achieved without disabling voice commands, but it is covered by enabling Single App Kiosk mode. See below. Force allowing Signature™ Vision will ensure that the user prompt for microphone permission is skipped.

Policy CSP	/Privacy/ LetAppsAccessMicrophone_ForceAllowTheseApps
Process	SignatureVision_pzq3xp76mxafg

Disable Gaze Input for Other Applications

The OTS HMD must be configured to prevent other applications other than Signature™ Vision from accessing gaze input.

Policy CSP	/Privacy/ LetAppsAccessGazeInput
Value	2 (force deny)

Policy CSP	/Privacy/ LetAppsAccessGazeInput_ForceDenyTheseApps
Process	SignatureVision_pzq3xp76mxafg

Disable USB Connections

The OTS HMD must be configured to disable the usage of the HMD as a USB client.

Policy CSP	/Connectivity/ AllowUSBConnection
Value	0 (disable)

Disable Developer Mode and the Device Portal

The OTS HMD must be configured to disable Developer Mode and the Device Portal.

Policy CSP	/ApplicationManagement/ AllowDeveloperUnlock
Value	0 (disable)

Disable Installation and Removal of Other Applications

The OTS HMD must be configured to disable the ability to install and remove other apps by the user.

This is covered by enabling Single App Kiosk mode.

Policy CSP	/ApplicationManagement/ AllowAllTrustedApps
Value	0 (Explicit deny)

Enable Kiosk Mode

The OTS HMD must be configured to run Signature™ Vision in Kiosk Mode.

Configuration	Kiosk Mode
Process	SignatureVision_pzq3xp76mxafg

Trust Signing Certificate

The OTS HMD must be configured to trust the Signing Certificate of Signature™ Vision.

Configuration	Trusted Certificate (Computer Certificate Store - Root)
Certificate	[Will be provided by the distributor]

Sleep Settings (Optional)

Operating in Single App Kiosk Mode implies that power-cycling the device or entering sleep mode will trigger an application restart. Since restarting the Signature™ Vision software necessitates re-performing the anatomical registration, it is recommended to configure the sleep mode timeout to a minimum of 30 minutes if on battery, and one hour if plugged in. Note that this setting results in continuous battery consumption while the HMD is not in use. Consequently, it is strongly advised to connect the hardware to a charger during surgical procedures whenever it is not being worn.

Configuration	Administrative Templates/System/Power/ Sleep Settings/Specify the system sleep timeout (on battery)
Value	Enabled, 1800

Configuration	Administrative Templates/System/Power/ Sleep Settings/Specify the system sleep timeout (plugged in)
Value	Enabled, 3600

Configuration using Provisioning Profiles

If no Mobile Device Management (MDM) solution is employed, the HMD can be provisioned using profiles deployed via a USB thumb drive. While these profiles are primarily intended for the initial setup of the hardware, the activation of Single App Kiosk Mode effectively prevents users from modifying system configurations or removing the established policies.

The provisioning profile (PPKG) is generated using the Windows Configuration Designer software on a compatible workstation. To ensure the device is configured correctly, implement the specific policy settings detailed in the following sections.

Profile Settings

User Authentication

The OTS HMD must be configured to force users to log in each time they use the device.

Policy CSP	Runtime settings/Policies/DeviceLock/ DevicePasswordEnabled
Value	Not Enabled

Disable Bluetooth

The OTS HMD must be configured to disable Bluetooth connections.

Policy CSP	Runtime settings/Policies/Connectivity/ AllowBluetooth
Value	No

Policy CSP	Runtime settings/Policies/Bluetooth/ AllowDiscoverableMode
Value	No

Disable Camera for Other Applications, Disable Taking Pictures and Videos

The OTS HMD must be configured to prevent applications other than Signature™ Vision from accessing the camera and disabling the recording of videos and taking pictures on the HMD.

Policy CSP	Runtime settings/Policies/Privacy/ LetAppsAccessCamera
Value	Force Deny

Policy CSP	Runtime settings/Policies/Privacy/ LetAppsAccessCamera_ForceAllowTheseApps
-------------------	---

Process	SignatureVision_pzq3xp76mxafg
----------------	-------------------------------

Disable the Microphone for Other Applications

The OTS HMD must be configured to prevent other applications than Signature™ Vision from accessing the microphone.

This cannot be achieved without disabling voice commands, but it is covered by enabling single app Kiosk mode. See below. Force allowing Signature™ Vision will ensure that the user prompt for microphone permission is skipped.

Policy CSP	Runtime settings/Policies/Privacy/ LetAppsAccessMicrophone_ForceAllowTheseApps
Process	SignatureVision_pzq3xp76mxafg

Disable Gaze Input for Other Applications

The OTS HMD must be configured to prevent other applications other than Signature™ Vision from accessing gaze input.

Policy CSP	Runtime settings/Policies/Privacy/ LetAppsAccessGazeInput
Value	Force Deny

Policy CSP	Runtime settings/Policies/Privacy/ LetAppsAccessGazeInput_ForceAllowTheseApps
Process	SignatureVision_pzq3xp76mxafg

Disable USB Connections

The OTS HMD must be configured to disable the usage of the HMD as a USB client.

Policy CSP	Runtime settings/Policies/Connectivity/ AllowUSBConnection
Value	No

Disable Developer Mode and the Device Portal

The OTS HMD must be configured to disable Developer Mode and the Device Portal.

Policy CSP	Runtime settings/Policies/ApplicationManagement/ AllowDeveloperUnlock
-------------------	--

Value	No
--------------	----

Disable Installation and Removal of Other Applications

The OTS HMD must be configured to disable the ability to install and remove other apps by the user.

This can not be achieved using provisioning profiles, but is covered by enabling single Kiosk mode. See below.

Enable Kiosk Mode

The OTS HMD must be configured to run Signature™ Vision in Kiosk Mode.

Configuration	Runtime settings/AssignedAccess/ AssignedAccessSettings
Process	<code>{"Account": "SignatureVision", "AUMID": "SignatureVision_pzq3xp76mxafg!App"}</code>

To run Signature Vision in Single App Kiosk Mode, the application needs to be installed using provisioning profiles, and a local user needs to be created. See sections [App Installation](#) and [User Account](#).

Trust Signing Certificate

The OTS HMD must be configured to trust the Signing Certificate of Signature™ Vision.

Configuration	Runtime settings/Certificates/ RootCertificates (Computer Certificate Store - Root)
Certificate	[Will be provided by the manufacturer]

App Installation

The app is installed using provisioning profiles. The following needs to be configured:

Configuration	Runtime settings/UniversalAppInstall/ UserContextApp/PackageFamilyName
Value	SignatureVision_pzq3xp76mxafg

Configuration	Runtime settings/UniversalAppInstall/ UserContextApp/SignatureVision_pzq3xp76mxafg/ApplicationFile
----------------------	---

Value	[Upload .appx]
--------------	----------------

Configuration	Runtime settings/UniversalAppInstall/ UserContextApp/SignatureVision_pzq3xp76mxafg/DependencyAppxFiles
Value	[Upload VCLibs .appx]

The SignatureVision and VCLibs .appx files will be provided by the manufacturer.

User Account

This is configured in provisioning profiles. A local user is created.

Configuration	Runtime settings/Accounts/ Users/UserName
Value	SignatureVision

The user profile that has been created must have a password assigned to it.

Configuration	Runtime settings/Accounts/ Users/SignatureVision/Password
Value	[Define a secure password]

First Experience Settings (Optional)

These configuration options make setting up the device simpler by skipping some steps in the *First Experience* dialogs.

Configuration	Runtime settings/ FirstExperience/HoloLens/PreferredLanguage
Value	en-US

Configuration	Runtime settings/ FirstExperience/HoloLens/SkipCalibration
Value	TRUE

Configuration	Runtime settings/ FirstExperience/HoloLens/SkipTraining
Value	TRUE

Configuration	Runtime settings/ FirstExperience/HoloLens/SkipWiFi
Value	TRUE

Sleep Settings (Optional)

Operating in Single App Kiosk Mode implies that power-cycling the device or entering sleep mode will trigger an application restart. Since restarting the Signature™ Vision software necessitates re-performing the anatomical registration, it is recommended to configure the sleep mode timeout to a minimum of 30 minutes if on battery, and one hour if plugged in. Note that this setting results in continuous battery consumption while the HMD is not in use. Consequently, it is strongly advised to connect the hardware to a charger during surgical procedures whenever it is not being worn.

Configuration	Runtime settings/ Policies/Power/DisplayOffTimeoutOnBattery
Value	<enabled/> <data id="EnterVideoDCPowerDownTimeOut" value="1800"/>

Configuration	Runtime settings/ Policies/Power/DisplayOffTimeoutPluggedIn
Value	<enabled/> <data id="EnterVideoACPowerDownTimeOut" value="1800"/>

Configuration	Runtime settings/ Policies/Power/StandbyTimeoutOnBattery
Value	<enabled/> <data id="EnterDCStandbyTimeOut" value="1800"/>

Configuration	Runtime settings/ Policies/Power/StandbyTimeoutPluggedIn
----------------------	---

Value	<pre><enabled/> <data id="EnterACStandbyTimeout" value="1800"/></pre>
--------------	---

Provisioning Profile Installation

For the deployment of both the provisioning profile and the application, performing a device re-flash is the recommended procedure.

Instructions for this process can be found in the *Clean-reflash the device* documentation available at <https://learn.microsoft.com/en-us/hololens/hololens-recovery#clean-reflash-the-device>.

Transfer the PPKG file to a formatted USB storage device. Following the re-flash, insert the drive into the HMD's USB-C port once the hummingbird appears. Proceed by confirming the profile installation or allowing the system to proceed automatically after the timeout.

Ensure the setup concludes without error. After the subsequent restart, advance through the configuration wizard until the Signature™ Vision software initializes.

At this stage, the hardware is prepared for operation with Signature™ Vision.

Servicing and Maintenance Tasks

Signature™ Vision offers a user interface for servicing and maintenance tasks. The UI is available in the *About* screen of Signature™ Vision, which can be opened through the hand menu.

To access the *Maintenance Tasks* screen, open the Hand Menu by looking at the palm of your hand, then tap the *About* button.

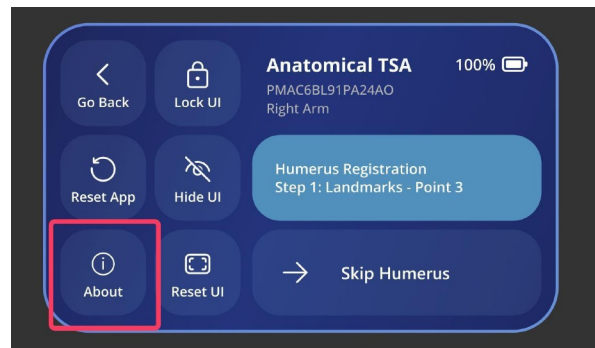


Figure 3: Signature™ Vision Hand Menu

In the *About* panel, tap the *Maintenance Tasks* button.

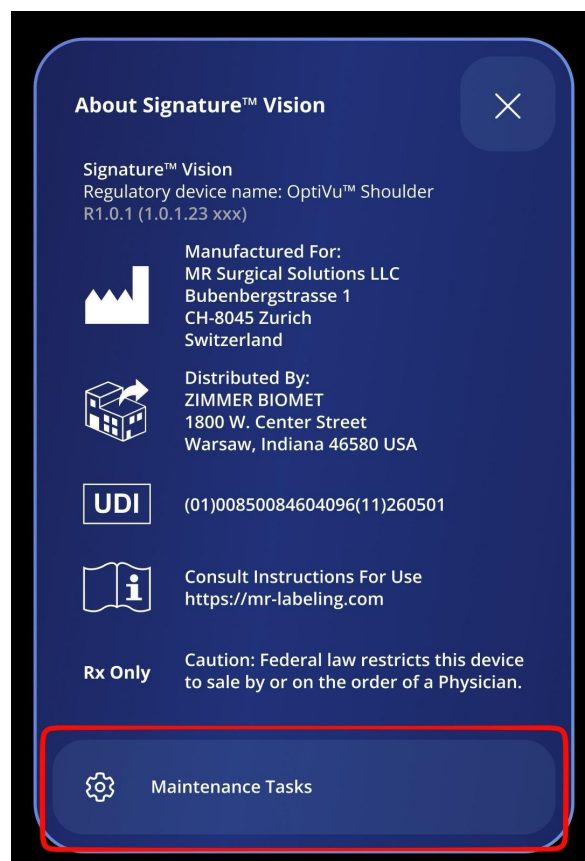


Figure 4: Signature™ Vision “About” panel (accessed from Hand Menu)

The *Maintenance Tasks* screen offers two features that are described in more detail in the upcoming sections.

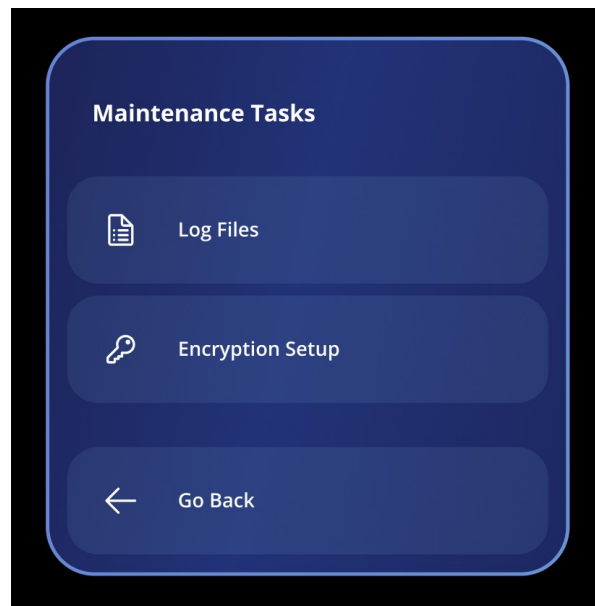


Figure 5: Signature™ Vision Maintenance Tasks Menu

Exporting and Deleting Log Files

Signature™ Vision provides technicians with options to export internal application log files to a USB-C thumb drive and to delete log files from the device's internal storage.

The internal log files contain valuable information for software maintenance, along with usage logs that assist in investigating software issues.

The *Log Files* options are accessible under *Maintenance Tasks > Log Files*.

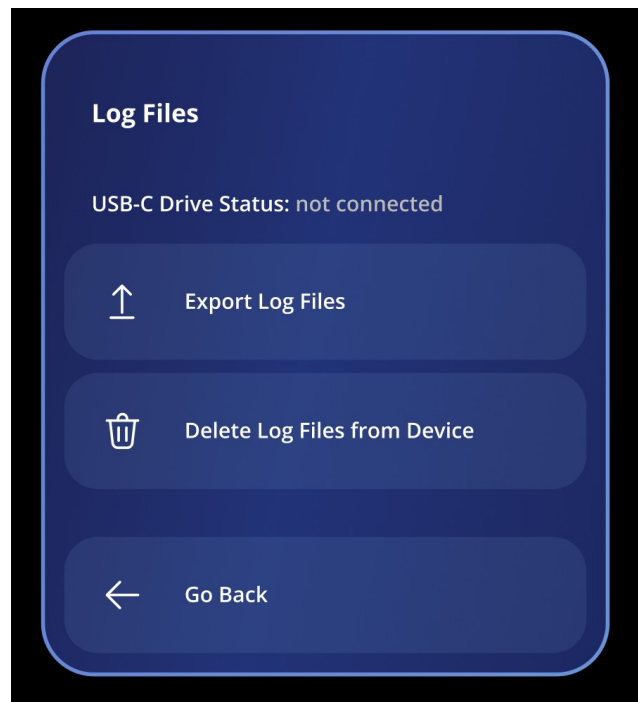


Figure 8: Signature™ Vision Log Files Menu

Exporting Log Files

The software retains the most recent 2,000 log files and automatically deletes older files to prevent the device's internal storage from filling up.

To export log files, connect a USB-C storage device to the HMD and tap the *Export Log Files* button. This action copies the internal log files to the USB-C thumb drive without removing them from the HMD.

Delete Log Files from Device

Tap the *Delete Log Files from Device* button to remove all the internal log files. Note that the log file of the current application session remains on the device after executing this command.

Encryption Key Management

All patient case files are encrypted with multiple layers of cryptography. This includes private/public key encryption, as well as encryption using a user password. The decryption implementation of Signature™ Vision has been adopted from the existing implementation at Zimmer Biomet.

An initial public key exchange needs to be performed to allow Zimmer Biomet employees, or more specifically the PMP portal, to encrypt the patient case files for Signature™ Vision. The PMP portal needs a copy of each public key of each Signature™ Vision device, and each Signature™ Vision device needs a copy of the PMP's public key.

This initial exchange of public keys between the device(s) and the PMP happens in an initial setup step performed by a field service engineer or technician after the installation of Signature™ Vision.

The application offers a *Maintenance Menu*, accessible on the *About* screen. Tap the *Encryption Setup* button to enter the *Encryption Setup* menu:

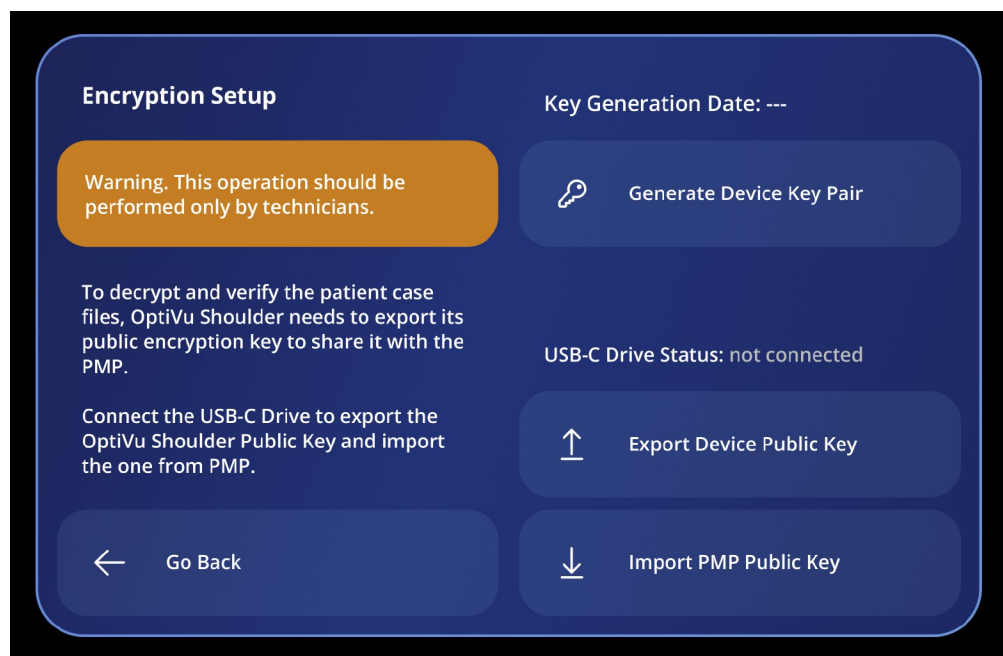


Figure 6: Signature™ Vision Encryption Setup Menu

The encryption setup screen offers the following features:

1. Generate Device Key Pair
2. Export Device Public Key
3. Import PMP Public Key

The files are imported and exported to/from the USB storage device. Connect a USB-C storage device to the HMD before using one of the export/import features. Do not use a thumb drive with USB-A connected to a USB-A-to-C adapter. The OptiVu Tilt with HoloLens 2 supports USB drives formatted in exFAT and FAT32.

1. Generate Device Key Pair

Tap the Generate Device Key Pair button to generate a new private/public key pair for the device in use. After key generation has been completed, the Export Device Public Key button gets enabled. The UI will show the date of the key generation. The private key gets stored securely on the device, and the public key needs to be exported and shared with PMP.

2. Export Device Public Key

Make sure you have a USB-C storage device connected to the HMD to allow exporting the public key. Tap the Export Device Public Key button to copy the device's public key to the USB storage device.

After successfully exporting the public key, import the key to the PMP portal.

3. Import PMP Public Key

To allow decryption of the patient case files, the Signature™ Vision application needs a copy of the PMP's public key. Copy the PMP's public key to the USB-C storage device.

The filename of the public key must be exactly as the following: *pmp_certificate.pem*

Tap the Import PMP Public Key button to copy the PMP's public key to the device.

User-Defined Password / PIN

When downloading a patient case file from PMP, the user needs to define a password to additionally protect the patient case file. This password needs to be typed in within the UI of the Signature™ Vision application when opening a case.

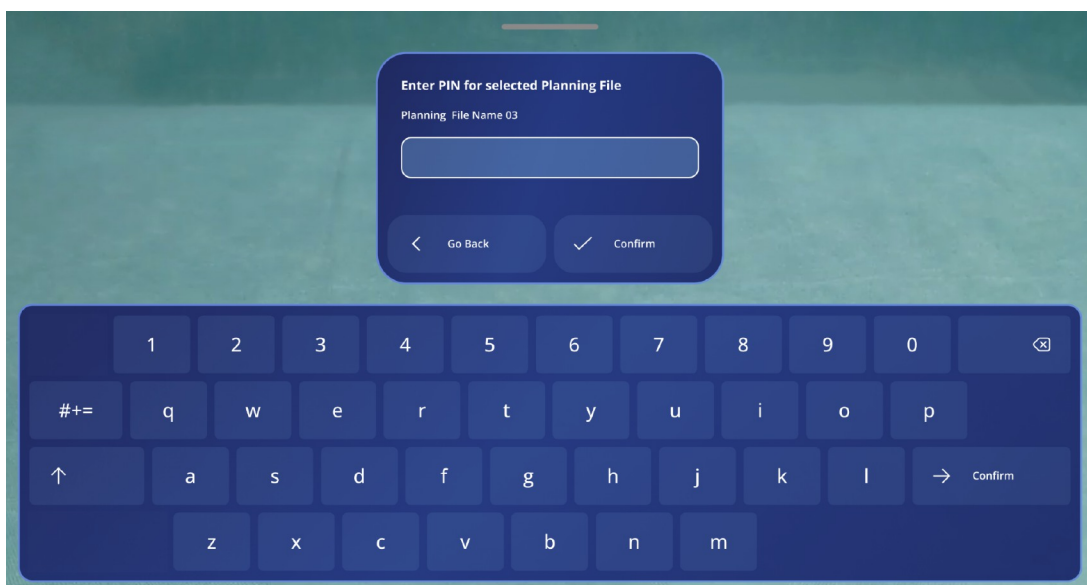


Figure 7: Signature™ Vision PIN Entry Screen

In case the user forgets the password, the case needs to be re-encrypted and re-downloaded using the PMP portal.

SBOM List

The following table lists the Software Bill of Material (SBOM) used in the Signature™ Vision SW.

Supplier Name	Component Name	Version of the Component
ALGLIB Project (Bochkanov Sergey Anatolyevich)	Alglib	3.13.0
Rafael Muñoz Salinas	ArUco	3.0.7
OpenCV Team	OpenCV	3.4
Microsoft	Mixed Reality Toolkit 3	3.2.1
Parentelement LLC / Newtonsoft	Newtonsoft Json	13.0.102
Modest Tree Media	Extenject	9.2.1
Sentry	Sentry-Unity	2.0.2
Yoshifumi Kawai / neuecc	UniRX	7.1.0
Unity Technologies	Unity 3D	2022.3.32
Unity Technologies	Text Mesh Pro	3.0.9
Open Source	Serilog	3.0.1
Andreas Atteneder	GLTFast	6.2.0
Microsoft	Windows 11 Holographic	24H1
Legion of the Bouncy Castle Inc.	Bouncy Castle	2.4.0

Regulatory Device Name

The FDA-cleared medical device officially designated as OptiVu™ Shoulder is commercially distributed under the marketing name Signature™ Vision by Zimmer Biomet.

HMD Configuration Notice

For inclusion with the OptiVu™ Shoulder / Signature Vision HMD package

Controlled Source Notice: This standalone insert page is controlled as part of the current approved revision of this Signature™ Vision Mixed Reality Navigation - Operator Instructions and Cybersecurity Considerations document. Print this page only after the HMD has been configured according to this procedure.

This Head-Mounted Display (HMD), OptiVu Tilt with HoloLens 2, has been configured for use with Signature™ Vision according to the applicable device configuration requirements.

Before using the device, review the current Signature™ Vision User Manual.

User manual location: <https://mr-labeling.com>

If the HMD has been re-flashed, reset, or the Signature™ Vision software has been uninstalled and reinstalled, configuration and encryption key setup may need to be performed again before use.

Note: This notice is intended to identify HMD configuration status and provide the location of the Signature™ Vision User Manual. It does not replace the User Manual.