PARITYMEDICAL

NHS Approved Framework Supplier

Tech Devices - Link 4 Framework Agreement (Lot 2)
Contract References
NHS SBS: 10515
NOE CPC: NOE.0633 / 2024/S 000-027266

ONYX VENUS 224 / 244 BIOS AND EC DEPLOYMENT PROCEDURE

Customer Deployment Guide

1. PURPOSE

This guide provides instructions for preparing a USB flash drive and manually deploying approved BIOS and Embedded Controller (EC) firmware updates to ONYX Venus 224 / 244 and Venus 224P / 244P systems.

The procedure is intended for suitably trained and authorised personnel and must be completed individually on each target system.

IMPORTANT:

BIOS and EC firmware updates carry a risk of system failure if interrupted or performed incorrectly. Ensure the system remains connected to a stable power source throughout the update process.

Do NOT remove power or forcibly restart the system while firmware is being programmed.

Use only the firmware files and utilities supplied with the approved update package.

2. USB FLASH DRIVE PREPARATION

2.1 USB DRIVE REQUIREMENTS

Use a suitable USB 2.0 or greater flash drive with a minimum capacity of 1 GB for the supplied firmware and utility files.

The USB drive must be formatted using the FAT32 file system.

WARNING:

Formatting the USB drive will erase its existing contents. Ensure any required data has been backed up before formatting.

2.2 USB DRIVE STRUCTURE

The USB drive must contain two folders in its root directory:

- EFI
- BIOS

The supplied files must be extracted or copied into their respective folders.

The folder structure supplied with the EFI files must be maintained.

The BIOS folder must contain all the files required by the BIOS Service Utility, including the deployment scripts and the firmware files.

Do NOT rename, move or delete any supplied firmware or utility files.

The completed USB drive should resemble the following structure:

USBROOT:\EFI\BOOT	Folder should contain 4 files and 1 ‘Normal-Efi’ folder containing 3 files
USBROOT:\BIOS	Folder should contain 8-9 files depending on model type

2.3 EFI FOLDER

Extract or copy the supplied EFI boot files and supporting folder structure into this folder.

The supplied EFI folder structure must be maintained otherwise the system will not boot into the EFI Shell.

2.4 BIOS FOLDER

Extract or copy the supplied BIOS Service Utility files into this folder.

The BIOS folder must contain all files required by the deployment process.

The number and contents of files may vary between firmware releases. Do not remove or rename files supplied as part of the approved update package.

3. TARGET SYSTEM PREPARATION

3.1 BACK UP IMPORTANT DATA

Ensure any important user or system data has been backed up before performing the firmware update.

3.2 SUSPEND BITLOCKER PROTECTION

BitLocker protection must be temporarily suspended before beginning the firmware update.

This is necessary because changes to BIOS firmware and Secure Boot configuration can alter the system measurements used by BitLocker.

Suspending BitLocker does **NOT** decrypt the drive. The data remains encrypted throughout the procedure.

IMPORTANT:

Ensure that the BitLocker recovery key is available before proceeding.

Do **NOT** begin the firmware update if the recovery key cannot be obtained or verified.

1. Start Windows normally and sign in with an account that has appropriate administrative privileges.
2. Open **Control Panel**.
3. Select: **System and Security** > **Bitlocker Drive Encryption**
4. Locate the Windows operating system drive, normally C:.
5. Select: **Suspend protection**
6. Select **Yes** when prompted to confirm.
7. Verify that BitLocker protection is shown as suspended before continuing.

IMPORTANT:

Do **NOT** select an option to decrypt, turn off, or disable BitLocker.

The required action is to **SUSPEND** protection only.

3.3 TEMPORARILY DISABLE SECURE BOOT

Secure Boot must be temporarily disabled before booting the Prepared USB into the EFI Shell.

1. Power on or restart the target system.
2. When the ONYX splash screen appears, repeatedly press the Delete key until the AMI BIOS is displayed.
3. Scroll to the Security menu and select the Secure Boot menu option.
4. Change the Secure Boot setting from Enabled to Disabled using the PgUp or PgDown keys.
5. Press F4 to save the settings and restart the system.

Secure Boot should remain disabled only for the duration of the firmware deployment.

Secure Boot will be re-enabled during the final system verification process.

4. BOOT FROM THE PREPARED USB

1. Insert the Prepared USB flash drive into the target system.
2. Power on or restart the system.
3. When the ONYX splash screen appears, repeatedly press F7 to enter the boot override menu.
4. Select the USB device by choosing:

   UEFI:<USB NAME>: Partition 1

5. If successful, the system will enter the AMI EFI Shell command line environment.
6. Navigate to the USB filesystem by entering one of the following commands.

   For a blank system with no operating system installed, the USB drive will normally be available as:

   fs0:

   Press Enter after entering the command.

   For a system with an installed operating system, the USB drive will normally be available as:

   fs1:

   Press Enter after entering the command.

   If the expected filesystem is not present, use the EFI Shell filesystem mappings to identify the USB device before proceeding.

5. BIOS DEPLOYMENT

The BIOS deployment process consists of two stages:

Stage 1:
System information backup and BIOS programming

Stage 2:
System information restoration and, where applicable, Embedded Controller programming

5.1 RUN THE BIOS DEPLOYMENT

From the USB filesystem, navigate to the BIOS folder by typing:

cd BIOS

Press Enter after typing the command.

Run the deployment script by typing:

Deploy.nsh

Press Enter after typing the command.

The deployment utility will automatically:

- Create a backup report.
- Record the existing system information.
- Back up the system SMBIOS information.
- Back up the Intel network adapter MAC addresses.
- After prompting to proceed, will program the approved BIOS firmware.
- Automatically restart the system.

5.2 RUN THE RESTORATION AND EC UPDATE

After the system restarts, boot back into the AMI EFI Shell from the Prepared USB by repeating steps 1-6 in Section 4.

Return to the BIOS folder by typing:

cd BIOS

Press Enter after entering the command.

Run the restoration script:

Restore.nsh

The restoration utility will:

- Restore the system SMBIOS information.
- Restore the system BIOS OEM information.
- Restore the Intel network adapter MAC addresses.
- Display the restored system information for verification.
- Update the Embedded Controller firmware where applicable.

Where an Embedded Controller update is included in the approved firmware package, the update will cause the system to power off automatically when the update has completed.

IMPORTANT:

Do **NOT** remove power during an Embedded Controller update.

6. CONFIRM UPDATE AND RESTORE SYSTEM

After the firmware deployment has completed, perform the following checks to confirm that the update was applied successfully and that the system is ready to return to normal operation.

1. Power on the system and enter the BIOS by repeatedly pressing the Delete key when the ONYX splash screen appears.

2. From the BIOS Summary screen, confirm that the correct BIOS version is displayed.

   For B224 / B244 systems, the version will be formatted similarly to:

   BVEN3S00.V30

   For B224P / B244P systems, the version will be formatted similarly to:

   BVEN5400.V10

3. Confirm that the correct EC firmware version is displayed under Firmware Version, where applicable.

   For B224 / B244 systems, the version will be formatted similarly to:

   EVEN3S00.V12

   For B224P / B244P systems, the version will be formatted similarly to:

   EVEN5400.V03

   NOTE:

   The EC firmware version shown above is dependent on the firmware package applicable to the target system.

4. Scroll to the Security menu and select the Secure Boot menu option.

5. Confirm that Secure Boot is set to **Enabled**.

   Secure Boot is normally enabled by default. If it is shown as Disabled, change the setting to Enabled using the PgUp or PgDown keys.

6. Press F4 to save the settings and restart the system.

7. Allow the system to boot normally into Windows.

8. Confirm that the system operates normally before proceeding to resume BitLocker protection.

6.1 RESUME BITLOCKER PROTECTION

Once Windows has started successfully and the system has been confirmed to be operating normally, BitLocker protection must be resumed.

1. Sign in to Windows using an account with appropriate administrative privileges.

2. Open **Control Panel**.

3. Select: **System and Security** > **Bitlocker Drive Encryption**

4. Locate the Windows operating system drive, normally C:.
5. Select: **Resume Protection**
6. Select **Yes** when prompted.
7. Verify that BitLocker protection is shown as active.

Resuming BitLocker allows protection to be re-established against the new measured system state following the firmware and Secure Boot changes.

IMPORTANT:

Do **NOT** leave BitLocker protection suspended after completing the firmware deployment.

If BitLocker does not resume successfully, do NOT return the system to service. Contact the appropriate technical support team.

7. IMPORTANT WARNINGS

- Do **NOT** remove power during BIOS or EC firmware programming.
- Do **NOT** interrupt a firmware update once programming has started.
- Do **NOT** use firmware intended for a different system model.
- Do **NOT** mix BIOS, EC or EFI utility files from different firmware packages.
- Do **NOT** rename supplied firmware or EFI utility files.
- Ensure BitLocker protection has been suspended before beginning the firmware deployment.
- Ensure BitLocker protection is resumed after the deployment has successfully completed.
- Ensure Secure Boot is re-enabled before returning the system to normal operation.
- If an unexpected error occurs, do **NOT** continue with the next stage. Record the displayed error and contact the appropriate technical support team.
- Failure to complete all steps in this procedure may result in system malfunction or abnormal behaviour.