White Paper
September 2020

DeltaV™ System Software Update Deployment

This brief whitepaper provides a handy index to Emerson documents related to deployment of software updates, along with summary information about software update delivery and deployment services available from Emerson.

Timely deployment of security updates and software patches contributes to secure and reliable operations.

EMERSON™

Index of documents related to Software Update Deployment

The following Knowledge Base Articles (KBAs) are relevant to the general topic of software update deployment. KBAs are highly technical documents, intended for use by qualified individuals, issued and supported by the Emerson Technical Support organization.

KBAs are available via an access-controlled Internet support website for DeltaV™ systems subscribed to either FOUNDATION Support or Guardian Support Service. Individual KBAs can be furnished for non-subscribed systems via request to the local Emerson service department. Always ensure you have the latest revision of a particular KBA before implementing, since these can be revised on a regular basis.

Document	Title	Synopsis
AP-0400-0004	Recommended Antivirus and Installation Procedure for DeltaV Workstations	This document provides a compatibility chart, specifying the approved Symantec™ antivirus product for each DeltaV / OS version. Known issues are identified.
AP-0800-0025	Symantec Endpoint Protection 11.0 Installation Procedure on DeltaV Workstations	This document provides instructions for installing Symantec's Endpoint Protection Version11 antivirus product. The procedure is limited in scope to an unmanaged mode of deployment.
AP-0900-0040	Using a Batch File to Aid the Installation of Microsoft™ Security Updates	This document provides instruction for creating a BAT batch file to manually install multiple Microsoft security updates in a single workstation. Essentially an optimized unmanaged mode of deployment for Microsoft security updates.
AK-1000-0124	Application Notes for Patch Management Deployment	This document provides information regarding the implementation of a managed mode deployment of Microsoft security updates, Symantec antivirus definition files, and DeltaV software updates via the Emerson Automated Patch Management Service. This managed mode solution utilizes Microsoft's Windows Server Update Services (WSUS), Symantec's Endpoint Protection Manager (SEPM), Symantec's Live Update Administrator (LUA), and Emerson's Guardian WSUS Interface (GWI) software, approved for use with DeltaV version 9.3.1 and up.
AP-0900-0030	Procedure and Tips for Submitting the DeltaV System Registration File via the Internet	This document provides advice for setting up a secure internet path for the DeltaV system registration utility to automatically deliver an encrypted xml file to Emerson, to maintain fresh system content and version information in Guardian.
AK-1300-0005	Microsoft Released Security Updates for DeltaV Systems	This document lists the approval status of Microsoft security updates issued for supported versions of DeltaV. It also lists the KBA numbers for previous years.

Figure 1 - KBAs Related to Software Update Deployment

The following guideline documents are relevant to software update deployment. Guideline papers are issued to provide information concerning the practices that should be used for installation and deployment of updates in a DeltaV system that is to be supported by Emerson. It is important that these guidelines be followed in order for Emerson to provide technical support for your DeltaV system. Failure to follow these guidelines may compromise our ability to provide timely and complete technical support for your DeltaV digital automation system.

Document	Title	Synopsis
P_MS_Patch_Mgt.doc	Microsoft Security Bulletin Administration on DeltaV Systems	This guideline relates to the testing and deployment of operating system updates, security bulletins and new operating system service packs.
P_Anti_Virus_on_DeltaV.doc	Antivirus Scanning in DeltaV Systems	This guideline elates to the testing, support and deployment of antivirus scanning software.

Figure 2 - Guidelines Related to Software Update Deployment

The following whitepaper documents are relevant to software update deployment or cybersecurity. Whitepapers provide general guidance and background information. Whitepapers are available on the DeltaV internet website: **http://www2.emersonprocess.com/en-US/brands/deltav/documentation/Pages/whitepapers.aspx**.

Document	Title	Synopsis
WP_DeltaVSystemSecurity.doc	DeltaV System Cybersecurity	This whitepaper outline the system philosophy, guidelines and rules for providing cybersecurity policy to the DeltaV system.
WP_BestPrac_CyberSec.doc	Best Practices for Cybersecurity	This whitepaper is supplementary and complimentary to the whitepaper “DeltaV System Cybersecurity”. It addresses keeping a DeltaV system secure from hacker attacks, viruses, worms and other malware and security threats.
CS_DeltaV_Security_Manual.doc	Cybersecurity for DeltaV Digital Automation Systems	This document is a guide for process engineers, information technology personnel, operations managers and other plant personnel responsible for developing and maintaining the cybersecurity of DeltaV digital automation systems.

Figure 3 - Whitepapers Related to Software Update Deployment

Software Update Types

System software updates come in a variety of types with different sources:

Update Type	Description and Source	Rollout Directions
DeltaV Hotfixes	Hotfixes are made available at Emerson's discretion to address issues in a specific build of DeltaV system software. Hotfixes can either be issue-specific or supplied in a 'bundle' of multiple hotfixes. Each hotfix has a corresponding KBA that explains the issue. KBAs and hotfix executables are obtained from the access-restricted Emerson support websites.	Users are encouraged to install hotfixes proactively for maximum system robustness. Install them per individual KBA instructions.
Microsoft Operating System Security Updates	Security updates are issued by Microsoft to address cybersecurity issues. Typically they are issued in a monthly batch, however especially critical updates can be issued at any time. Emerson determines which security updates are necessary for supported DeltaV / OS version combinations and tests them for compatibility. Approved updates can be downloaded from the access-restricted Emerson support websites, or from the Microsoft Knowledgebase website.	Only install security updates that have been approved for use by Emerson, at the earliest opportunity following approval. Special instructions if any are provided in the KBA listing of approved updates. It is recommended to stagger the installation, updating a small number of computers ahead of the majority. Refer to the Guideline Microsoft Security Bulletin Administration on DeltaV Systems for more information.
Microsoft Operating System and Application Updates	Microsoft issues updates for reasons other than cybersecurity. In general, Microsoft non-security updates are not approved for use with the DeltaV system, other than to address a DeltaV software issue. An example exception is the Microsoft OS update to accommodate the 2007 change in US daylight savings time. Microsoft non-security updates are approved for use by way of an issue-specific KBA.	Never install Microsoft OS or application non-security updates unless specifically directed by a KBA. Follow KBA instructions for installation.

Antivirus Updates	McAfee and Symantec frequently issue updates to their virus/worm pattern files, sometimes with multiple updates the same day. These updates can also include minor updates to the antivirus engine (application) itself to adapt to the latest cyber threats. The updates are cumulative, meaning that each update encompasses all of the latest antivirus patterns and minor engine updates. These updates have historically had no impact to DeltaV system compatibility and are considered acceptable for use as received from Symantec. Concurrent with the monthly compatibility check of Microsoft Security updates, Emerson checks the latest available Symantec virus definition file for DeltaV compatibility.	Customer may elect to install antivirus updates as received in real-time from McAfee and Symantec or only apply the ones that Emerson has checked each month. It is recommended to stagger the installation, updating a small number of computers ahead of the majority. Refer to the Guideline Antivirus Scanning in DeltaV Systems for more information.
McAfee and Symantec Antivirus Application Updates (AKA Virus Engine Updates)	New releases of McAfee and Symantec Antivirus scanning products are tested for DeltaV compatibility by Emerson, with new approved versions documented via KBA.	Only use approved versions of Symantec antivirus products, identified in KBA AP-0400-0004 and AK-1600-0076. Install them per KBA AP-0400-0004. Refer to the Guideline Antivirus Scanning in DeltaV Systems for more information.
DDL/EDDL Update	Updated Device and Extended Device Definition Language Files are issued by the device manufacturer. Conceptually similar to a PC printer driver, they provide the DeltaV system with essential details for properly interfacing with the device. Device manufacturers supply the updates. Emerson tests many but not all DDL/EDDL updates for compatibility.	Install as needed. For best results only install updates that have been compatibility tested by Emerson. Install them per instructions in DeltaV Books on Line.

Figure 4 - Software Update Types, Sources and Direction

Software Update Deployment Methods

In general there are two software deployment methods, Managed and Unmanaged.

In a Managed Mode a 'Management Server' is employed to automatically transfer needed software updates to individual workstations. Once the updates are received by the workstation, they are either automatically installed or alternately saved to wait for a user-directed install command which might be given at the client workstation or remotely from the Management Server.

In an Unmanaged Mode, software updates are installed at each individual workstation, manually invoked by an individual physically present at the workstation. Simply stated, it is the manual method. However, it is often the best method for DeltaV systems with a small number of workstations.

The unmanaged mode is the default recommended method for deploying software updates to a DeltaV system and is the only choice for DeltaV system set up as a workgroup (vs. a domain).

Guardian and the Guardian Software Update Delivery Service

DeltaV customers are encouraged to subscribe to Guardian Support, a service from Emerson that provides technical support, DeltaV system software updates including hotfixes, and access to a restricted support website that presents technical information tailored to each individual DeltaV system installation.

One of Guardian's features is a software update delivery service that transmits software update files and accompanying installation instructions (KBAs), for unmanaged mode deployment, on demand or according to a schedule, targeted to the particular customer system.

For more information reference:

- The Emerson Guardian Support Service Datasheet: **http://www2.emersonprocess.com/en-US/brands/sureservice/availabilityservices/guardiansupportservice/Pages/GuardianSupportService.aspx**

Automated Patch Management Service

In 2009 Emerson introduced a DeltaV Automated Patch Management Service, to assist customers with the design, deployment and support of a managed mode delivery solution for Microsoft security updates and Symantec antivirus pattern files for DeltaV V9.3 or higher systems. The solution integrates the capabilities of Microsoft's Windows Server Update Service (WSUS), Symantec's End Point Protection Manager and Emerson's Guardian Software Update Delivery Service.

When enrolled in Automated Patch Management Service, the Guardian software update delivery service transmits a file containing the latest list of approved and disapproved Microsoft security updates for a specific DeltaV system, in a format that is compatible with WSUS. The file is updated and transmitted whenever Emerson completes the compatibility testing of a security update relevant to the DeltaV system. With the help of a WSUS API interface provided with the Automated Patch Management Service, WSUS approval/disapproval transactions are automated, such that security update deployment can be automatically initiated in a managed mode triggered by the Emerson completion of compatibility testing.

For more information reference these documents:

- The Emerson Automated Patch Management Service Datasheet: **http://www2.emersonprocess.com/en-US/brands/sureservice/availabilityservices/PatchManagementServices/Pages/PatchManagementServices.aspx**
- The KBA AK-1000-0124 Application Notes for Patch Management Deployment

Deployment Status Reporting

To support unmanaged mode deployment, the Guardian website provides an automated comparison of installed vs. approved security updates, based on timely submissions of a DeltaV system registration files. Complete details are described in the Guardian Users Manual available on the Guardian Website. If not on Guardian Support, the customer should regularly compare installed updates to the KBA listing of approved updates.

Deployment status reporting is automated in a managed mode deployment. Methods for comparing approved vs. installed updates are covered in detail as part of the Automated Patch Management Service.

Emerson
North America, Latin America:
+1 800 833 8314 or
+1 512 832 3774

Asia Pacific:
+65 6777 8211

Europe, Middle East:
+41 41 768 6111

www.emerson.com