DIEBOLD NIXDORF

COMPREHENSIVE SERVICES

SOFTWARE DEPLOYMENT

The Diebold Nixdorf Software Deployment Service is a complete solution for applying Microsoft Operating System Security Patches to the ATM.

MINIMUM REQUIREMENTS

a. Diebold Nixdorf Opteva or ix ATM
b. Windows XP Pro Operating System, SP2
c. Agilis 91x 1.3
d. Agilis XV 2.0
e. TCS + 1.6
f. TCP/IP capable with Ethernet capability (dial-up connections not supported)

STANDARD FEATURES

a. Automated deployment/installation of Microsoft OS security patches identified by Diebold Nixdorf as being applicable to the ATM
b. Automated re-installation of removed security patches
c. ATM compliance Reporting via SERAS

HOW IT WORKS

Diebold Nixdorf Software Deployment automates the deployment, installation, and removal of Microsoft Windows security patches. The following requirements are needed for this to occur:

- Installation of the Diebold Nixdorf Software Deployment Client on the ATM
- Addition of rules to the ATM's firewall software that are tailored to the Software Deployment Service
- Connectivity from the ATM to the Diebold Nixdorf Software Deployment Server

During the Client installation process, custom policies are applied to the ATMs that facilitate the Software Deployment process. Two of these critical policies are detailed below:

- Patch Notify Policy – defines when the ATM will attempt a "check-in" to the Diebold Nixdorf Software Deployment Server to confirm that existing managed patches are still installed successfully and to also identify if any new patches are available for download/installation.
- Reboot Monitor Policy - defines when the ATM will perform a reboot if one is required to complete a patch installation that has occurred as a result of the Patch Notify Policy.

As security patches are released by Microsoft (normally the second Tuesday of each month), they are investigated by Diebold Nixdorf for their relevance to the ATM. Once patches are deemed as applicable to the ATM and subjected to QA testing, they are assigned to the managed ATM based upon the Client's Patching Schedule.

When the Patch Notify Policy is executed on the ATM, it will identify that new patches have been assigned and begin the download/installation process.

- Download/installation of patches does not interrupt consumer activity on the ATM

- Reboots that are needed due to a patch installation are suppressed until the Reboot Monitor Policy is executed and there is no consumer activity taking place on the ATM
- Prior to the ATM rebooting, a proper shutdown of the ATM applications takes place.

PATCHING SCHEDULE

a. Although ATMs will attempt periodic "check-ins" to the Diebold Nixdorf Software Deployment Server, new patches will only be assigned (i.e. made available for download/installation) on a monthly basis.
b. Upon contract acceptance a detailed Patch Deployment Schedule will be confirmed with the Client. (i.e. ATM check-in times, days of the month when patching will occur, groupings of ATMs to be patched, etc.)
c. An e-mail notification providing information on the patches to be installed will be sent to the designated Client contact prior to the deployment of new patches.

PATCH TESTING

Testing of Microsoft OS patches prior to their deployment will be performed

☒ Solely by Diebold Nixdorf against standard Diebold Nixdorf factory images

-OR-

☐ First by Diebold Nixdorf against standard Diebold Nixdorf factory images then by the Client in their own lab environment.

- Deployment of patches to the Client's pre-identified test ATM(s) will begin after the Diebold Nixdorf QA process has been completed. ***Deployment of the patches to the Client's remaining ATMs will not begin until Diebold Nixdorf has received written confirmation from the Client approving the release***. This written release must be received forty-eight (48) hours prior to start of the deployment.
- Support for ATM software/hardware issues related to patch testing are in addition to the Software Deployment contract pricing

PERFORMANCE REPORTING

Reporting is available to help the Client identify ATM's that are having their OS patches managed and their current state of compliance. Diebold Nixdorf Software Deployment reports are provided via SERAS.
Included reports

- Overall ATM Patch Compliance
- Listing of patches installed on the ATM

IMPLEMENTATION PROJECT – DIEBOLD NIXDORF RESPONSIBILITIES

a. Configuring the Diebold Nixdorf Software Deployment System for the standard Software Deployment service.
b. If required, configuring of the Software Deployment Proxy Server.
    - ***Additional Site Visit costs are in addition to the Software Deployment contract pricing.***

IMPLEMENTATION PROJECT – CLIENT RESPONSIBILITIES

a. Client must have a valid Master Licensing Agreement (MLA), Master Equipment and Services Agreement (MESA), or Diebold Nixdorf Comprehensive Agreement (DCA) with Diebold Nixdorf representing the copies of Windows XP Pro they have purchased for their ATMs. The number of copies purchased must equal the number of ATMs to be managed by this service.

b. From a host perspective, the Client's host processor must be able to recover from an ATM reboot. Successful installation of certain patches will require the ATM to be rebooted. Although the ATM will be shut down in a graceful manner, the host driving the ATM must be able to recognize a power fail has occurred and issue the proper commands to bring the ATM back in service.
c. Client must provide Diebold Nixdorf technician with administrative rights access to the ATM during the Software Deployment Client installation process.

Client must accept the addition of pre-defined rules to the ATMs firewall application to allow it to communicate with the Software Deployment Server.