DIEBOLD NIXDORF

COMPREHENSIVE SERVICES

OPTEVIEW REMOTE SERVICES

Diebold Nixdorf OpteView® enables a direct communication flow between the ATM and Diebold Nixdorf. When data is transmitted, it's encrypted via SSL protocol allowing the Client to manage and control access to data and ATM with Diebold Nixdorf's Policy Manager Tool. OpteView® immediately reacts to status faults or messages by remotely correcting the situation or diagnosing the problem.

MINIMUM REQUIREMENTS

a. Opteva, IX or I-Series ATM Hardware
b. Windows based Operating System
    - Windows 2000 minimum SP3, Windows Server 2003, Windows XP minimum SP2, Windows 7
c. Agilis or TCS+ Business Application.
d. TCP/IP Communication at the ATM with connectivity to Internet.
e. ATMs must be able to communicate via TCP/IP across the Client's local area network to the Policy Server application on the Client provided workstation or server (usually over 1024 or higher) and resolve to a DNS name of opteview.Diebold Nixdorf.com (SSL encrypted port 443).
    - DNS is the preferred method for the ATM to resolve the names by communicating with a Client's internal DNS server. Alternatively, the Client can utilize Internet DNS servers or look up names in a local host file on the ATM.

STANDARD FEATURES

a. Enables Remote Diagnostic and ATM Failure Resolution within minutes of machine failure.
b. Remote Service intervention available Monday through Friday, 8am to 2am EST; 5am to 11pm PST and Saturday-Sunday, 8am to 8pm EST; 5am to 5pm PST.
c. Visibility to all Remote Service intervention activities.
d. Secure communication path established between Diebold Nixdorf service network and Client ATM network.
    - the Internet, over SSL encrypted port 443, same as the On-line Banking programs used.
e. Continuous monitoring of ATM failure status without disrupting current monitoring/dispatch process.
f. SNMP transport utilized where custom or other non-Diebold Nixdorf business applications are implemented on Diebold Nixdorf hardware.
g. Detailed device status provides OpteView® operations with critical information for troubleshooting root cause and taking immediate corrective action.
h. Client maintains complete control and visibility of all OpteView® activity via OpteView® Policy Manager Software application provided by Diebold Nixdorf.

HOW IT WORKS

Once a an OpteView® message is received, Diebold Nixdorf OpteView® Remote Support operations may perform the following tasks depending on the nature of the received status data:

a. Initiate a communication session with the ATM machine based on permissions set by the Client.
    - Notify Client operations of the nature of the status using a Client provided e-mail address as inputted to the Policy Manager application.

b. Perform one or more diagnostic tests.
c. Fix the machine remotely or recommend to a Diebold Nixdorf technician who will service the machine, recovery solutions and/or parts needed for the repair.

OPTEVIEW® ACCESS SYSTEM ARCHITECTURE

a. OpteView® software agent needs to be installed on each ATM and the ATM needs to be configured to allow the agent to access the internet via SSL communications.
b. The ATM performs a DNS query to look up the TCP/IP address of the OpteView® server at Diebold Nixdorf. This query can be resolved by the Client's internal server, internet DNS servers, or by looking up an entry in the ATM's local host file.
c. The ATM initiates an outbound connection across the Client's network (via firewall, proxy servers or routers) to the OpteView® server within the Diebold Nixdorf System DMZ.
    - A Firewall rule may need to be added to the Client Management Server or locally at the ATM to allow the agent's ekernel.exe to access the OpteView® server outbound over TCP/IP.
        - The above rule will also allow the OpteView® agent's ekernel.exe to access the Policy Manager server on the Client's network. However, if additional application security is required, two rules may be added: one for ekernel.exe outbound port 443 (agent to OpteView® server) and one for ekernel.exe outbound port 80 (agent to Policy Manager) where 80 is the port number specified during Policy Manager Installation.
d. The OpteView® Agent will communicate with the Diebold Nixdorf OpteView® Server by first passing through Client's TCP/IP network. Client will route all OpteView® Agent traffic outbound to the Internet using DNS address OpteView.Diebold Nixdorf.com.
e. The OpteView® agent authenticates itself to the OpteView® server at Diebold Nixdorf via an independent third party digital certificate.
f. The ATM makes an outbound connection via SSL (port 443) to verify the authenticity of the digital certificate for Diebold Nixdorf's OpteView® server.
g. The ATM registers itself with Diebold Nixdorf's OpteView® server via a unique Diebold Nixdorf assigned serial number.
h. A periodic message is sent from the Policy Manager server on the Client's network to the ATM to download any updates to the ATM's security policy. This policy is defined, maintained and is the responsibility of the Client.

OpteView® Access Policy Manager Application

a. For the Client to have visibility and control over OpteView® access Diebold Nixdorf will provide for the duration of the Advisor Services and while this agreement is in place for OpteView®, a Policy Manager application to be installed on a Client provided workstation or server inside the Client's network.
b. Each ATM (OpteView® Agent) must be able to communicate with the Policy Manager server on the Client's internal TCP/IP network.
c. The ATM makes a connection to the Policy Manager server using standard http on TCP port 1024 (or an alternative port if needed).
d. The ATM keeps a current copy of its policy – as defined by the Policy Manager software – on its hard drive. This policy is consulted before allowing any action to be taken between the OpteView® agent on the ATM and the Diebold Nixdorf OpteView® Remote Support operations group. The local policy is verified each time the OpteView® Agent checks in with the Policy Manager and is updated only if the defined policy has changed.
e. The Policy Manager application will notify Client Operations using a Client provided email address. For this reason, the Policy Manager server must be able to access the Client email system.
    - Application must be installed on a Client provided Workstation / Server on the Client's LAN, accessible to all administering the system via Web Browser.

DIEBOLD NIXDORF

COMPREHENSIVE SERVICES

IMPLEMENTATION PROJECT – DIEBOLD NIXDORF RESPONSIBILITIES

a. Configuration of the Diebold Nixdorf OpteView® system for the standard OpteView® support model for the fault messages for break/fix.
b. Append MDS status messages' will be configured on each ATM if not already configured.
c. Activation and configuration of the EMS Notifier software at each ATM.
d. Installation and configuration of the OpteView® agent at each ATM.
e. Assist Client with enabling/configuring Sygate rules at each ATM.
f. Assist with installation of the Policy Manager software.
g. Provide Client with Policy Manager Application configuration training.

IMPLEMENTATION PROJECT – CLIENT RESPONSIBILITIES

a. Workstation or Server for Policy Manager application
    - Configuration Information
    - Operating System
    - Workstation or Server IP address
    - DNS Primary and Secondary IP addresses (if available)
    - Client Resource to install Policy Manager Application via Phone Support with OpteView® Implementation Team.
    - Client Resource(s) to be present at Policy Manager Training. Training is remote training provided by the OpteView Administrator.
    - Signature of Managed Equipment and Services Agreement (MESA) or Electronic Access Agreement for OpteView® Agents.
b. Client is responsible for providing any proxy authentication information required to allow the individual ATMs to access the Client internal network. Separate proxy authentication information may be provided for the OpteView® Agent to OpteView® server connectivity and for the OpteView® Agent to Policy Manager Connectivity.
c. Once the OpteView® agents at the ATMs are connected to the Client internal network, Client will be responsible for routing the message traffic to the DNS name OpteView.Diebold Nixdorf.com through the Internet.
d. Client is responsible for updating the Symantec/Sygate software (firewall) rules at the ATM (with Diebold Nixdorf's assistance) as required for the OpteView® agent to access the Policy Manager and the OpteView® server.
    o