FAQ:iDRAC Quick Sync & OpenManage Mobile

October 2014

Doug Iler – iDRAC Product Manager
Srikanth V Raghavan – OpenManage Mobile Product Manager
Sajjad Ahmed – iDRAC Quick Sync Senior Electrical Engineer

Dell | Enterprise Solutions Group

What is iDRAC Quick Sync?

IDRAC Quick Sync is a solution that allows an administrator to manage certain 13th generation rack-mounted PowerEdge servers (R630, R730, R730XD) from a mobile device. The mobile device must be running Android operating System 4.0.3 or higher, have Near Field Communication (NFC) technology, and must have DELL OpenManage Mobile app installed. This app can be downloaded for free from the Google play store here: https://play.google.com/store/apps/details?id=com.dell.omm&hl=en.

The supported servers when ordered with iDRAC Quick Sync come with a specific rack "ear" with connectors to the companion bezel that is equipped with NFC technology. An administrator can "bump" the mobile device (with the OpenManage app) against the iDRAC Quick Sync bezel and read basic server information such as device details, event logs, firmware details and network settings. An admin can also configure iDRAC network information and first boot device after proper authentication.

What is NFC?

NFC is a set of standards for smartphones and other devices to establish two-way communications by either touching or bringing them in to close proximity, usually not more than a few centimeters. This technology works via magnetic field induction and is based on RFID technology. It utilizes the key elements in existing standards for contactless card technology (ISO/IEC 14443 A&B and JIS-X 6319-4). More information about NFC can be found at http://nfc-forum.org

Why did Dell choose NFC technology for managing servers at the box?

Adoption of NFC technology is on the rise and it is expected to be available on ~575 million smart phones by 2015 according to Idate (http://www.nfcworld.com/2014/07/15/330373/idate-forecasts-nfc-phones-payments-volumes). NFC technology has been mainly used for mobile payment transactions and has been designed to be a secure technology. DELL's market research shows that more than 60% of customers perform various management activities inside a datacenter in front of their servers. Using the iDRAC Quick Sync mobile interface to manage servers at the data center improves business productivity by enabling 55% faster iDRAC configuration and 84% faster server information retrieval when compared with traditional methods.

Are mobile devices allowed in the data center?

Mobile devices are becoming the default choice for many users to perform their day job. Worldwide smart connected devices (SCD) are forecast to grow 15.6% year over year in 2014, reaching close to 1.8 billion devices according to the International Data Corporation (IDC). Android and iOS platforms are clearly the dominating Operating Systems since more than 80% of the end computing devices run these platforms.

The traditional concept of static end user or client computing devices is not valid anymore. Customers are not tethered to their desk at all times and are expected to be as productive as ever in spite of that. Based on DELL's customer conversations over the past two years, mobile phone use in data centers is increasing.

Is iDRAC Quick Sync secure?

NFC technology is very secure. It requires close proximity and/or physical contact (tap and hold) between the iDRAC Quick Sync bezel and the mobile phone. This means that only a person with access to the data center could perform this action. Once activated, the bezel is on for 30 seconds (the time out is configurable via the iDRAC) and the transfer of information between the mobile device and the server happens in less than 2 seconds.

Dell spent considerable effort in ensuring the security and data integrity in this feature. Data in Quick Sync is intelligently encrypted using Diffie-Hellman and symmetric cryptography providing security even in the event of a complete compromise of the iDRAC Quick Sync bezel.

What is the operational distance of iDRAC Quick Sync from a NFC-capable device?

iDRAC Quick Sync is designed to operate at a distance of 3cm or less.

Are smart phones more insecure than other means of managing a server at the data center?

No, they are not. A person with a laptop in a data center is no more secure than a person with a smart phone. The amount of functionality that one can access from a mobile phone is much less than what one can be done with a KVM or crash cart-style connection. And the server's front LCD panel offers several management functions. All of these avenues require a certain level of physical security in and around the data center. Physical access aside, iDRAC Quick Sync requires proper server authentication to perform any configuration changes.

Does OpenManage Mobile show sensitive information such as IP addresses?

Yes, it does. While the IP addresses are shown, not much can be done with it unless the servers are exposed to the internet. In general iDRAC IP addresses are behind the fire wall and are not exposed. Such exposure is a risk not just from smartphone applications but from any device that can connect to the internet. PowerEdge server IP addresses have also been available via the front panel screen for years, and can be accessed by anyone in the datacenter. It is imperative to ensure that your datacenter is secure regardless of what management tools and techniques you employ. For additional security, rack doors should be secured.

How secure is the iDRAC Quick Sync communication to server?

iDRAC Quick Sync is designed to replicate and enhance the LCD experience. This means that everything that user reads over iDRAC Quick Sync is also displayed over LCD. Writes to the server are password protected and will require user authentication from/via iDRAC.

Can I configure IDRAC Quick Sync access?

Yes, the embedded iDRAC provides full control over how IDRAC Quick Sync feature can be used. There are three main modes for access control:

1. "Disable" – This mode will disable any communication with IDRAC Quick Sync regardless of the press of activation button or change in physical IDRAC Quick Sync hardware.
2. "Read only" – this mode will disables any communication back to the server.
3. "Read-Write" – this configuration allows the flow of communication to and from server. Any communication to the server will be authenticated first before being accepted by iDRAC.

All of the IDRAC Quick Sync controls and configurations are independent of the IDRAC Quick Sync hardware and replacing hardware will not require reconfiguring these settings. User will have to log in iDRAC to make any changes to these controls. This provides the flexibility of keeping access controls as well as configuration controls of IDRAC Quick Sync on chassis level instead of on bezel level.

Where are the iDRAC Quick Sync settings located?

iDRAC Quick Sync configuration settings are located under "Front Panel" in the Hardware section of the iDRAC's web interface.

How much server power does iDRAC Quick Sync consume?

NFC in general requires extremely low power to operate. iDRAC Quick Sync will operate at less than 100mW of power.

How do I protect the information stored in the OpenManage Mobile app if the smart device is not company-provided?

Several mobile device/application management tools exist today that allows you to separate personal and corporate data. Corporate data and applications can be containerized for security purposes and can be wiped out remotely if an individual leaves the company or under other similar circumstances. Dell has a set of software solutions that can be used to protect your enterprise applications called "Enterprise Mobility Management." Learn more about these capabilities here: http://software.dell.com/solutions/enterprise-mobility-management/

Do iDRAC Quick Sync capabilities work on platforms other than Android?

As of today iDRAC Quick Sync works only on supported Android platforms. Apple has announced limited support for NFC technology within iOS, mainly focusing at mobile wallet applications. If and when Apple provides these APIs for other generic applications, DELL will extend its support to iOS platforms.