

# Smartphones and Tablets in the Enterprise

## Managing BYO Device Programs

### Introduction

Bring your own (BYO) device programs are becoming popular because they allow employees to work from the device of their choice. This can increase employee satisfaction while simultaneously reducing IT equipment acquisition costs. BYO programs are increasingly being extended – both in the breadth of devices and in connectivity to the corporate infrastructure – which in turn gives rise to new security and management challenges for corporate IT.

Employees bring the “gadget of the day” to work and expect it to function. This has resulted in what many are calling the “consumerization of IT,” where users expect their device will work on the network and help them do their job better. A highly automated workflow and processes are necessary to minimize the support cost and workload for corporate IT to make this happen.

Although not unique to employee-owned smartphones, tablets, netbooks, notebooks and other devices, the security concerns around co-resident private data and sensitive corporate data on the new generation of devices are once again becoming a focus issue. Any installed “app” from an online store is a potential backdoor into the corporate network. Realizing that restricting the use of additional “apps” on the devices via organizational rules/policies is not really a workable or practical solution, IT is faced with a daunting challenge.

This paper describes a solution architecture utilizing components from Enterasys that enables secure and automated device access to a corporate infrastructure in a variety of scenarios.

### Connectivity Scenarios

Many IT departments are faced with the need to connect BYO devices via WiFi (or wired Ethernet) to the corporate infrastructure so that employees can have full access to specific services. This could include the use of iPads in healthcare for medical rounds or in production environments for process management and documentation. Another growing trend is smartphones that use fixed mobile convergence to seamlessly transfer calls from a cellular network to a corporate WiFi network to save on costs and provide additional access to corporate data.

There are multiple approaches to how these devices can be connected to the corporate infrastructure. For example, if only email services are required, then it makes sense to block WiFi access to the corporate network and treat the devices via 3G/4G cellular services as external devices connecting to the corporate services via the DMZ. In this way, corporate data like emails and their attachments, along with contact data, resides on the device, but they have no native access into the corporate IT infrastructure. In this case, other security controls and usage guidelines have to be established to address these issues.

### Solution Architecture Components

In the following section the architectural components that form the foundation for the Enterasys solution to the BYO device challenge are described. These components together provide a solution for managing a number of different device types and operating systems, as well as overcoming the very dynamic nature of today's tablets and smartphones.

### Benefits

#### Automation

- Automates the provisioning of access for any device type entering the corporate network

#### Visibility and Control

- Granular control of access increases security for private/BYO devices on the corporate network

#### Reduced cost

- Leverage efficiency gains through use of new and innovative devices
- Reduced OPEX through automated service provisioning
- No dedicated infrastructure required to support new devices
- Leverages the same access control technology used for other devices

## Device Type Detection

Device Type detection is the first and critical step so appropriate security measures like device assessment and access control can be appropriately applied. The detection of new devices along with the ability to detect the type of device and enable the registration process for these devices is a feature provided by Enterasys [NAC<sup>NG</sup>](#) (Network Access Control - Next Generation), which is a network centric approach to NAC that goes further than traditional approaches. Besides the standard functions of NAC like authentication, authorization, assessment, remediation and monitor/contain, Enterasys NAC<sup>NG</sup> provides the ability to detect, profile (e.g. device type detection) and track any end system and user on the infrastructure. NAC<sup>NG</sup> detects new devices automatically and profiles them to determine the type of device. Various sources such as network and agent-based assessment, DHCP OS fingerprinting, captive portal (used for remediation and registration, guest services) and external profilers can be used. The device type can be an operating system family, operating system or hardware type, for example, Windows, Windows 7, Debian 3.0, HP Printer, iPhone, iPad, etc. Figure 1 depicts a number of types of devices that can be profiled via NAC<sup>NG</sup>.

MAC Address	Mobile Device Type	Operating System	Owner
90-21-55-EF-DD-9E	HTC EVO	Android 2.2	Chris
00-23-76-CD-C9-FB	HTC Hero	Android 2.3	Mike
40-FC-89-D2-2D-21	Droid Pro	Android 2.2.1	Tanya
3C-8B-FE-73-FE-9D	Samsung Galaxy Tablet	Android 2.2	IT
5C-DA-D4-50-99-1E	Samsung SCH-I500	Android 2.1	Joel
BC-47-60-B4-ED-FF	Samsung Intercept	Android 2.1	Andre
DC-2B-61-EA-38-47	iPhone	iPhone	Jamie
F4-0B-93-66-88-33	Blackberry Bolt 9700	Blackberry	Tanya
00-25-AE-22-93-33	Zune HD	Windows CE	Riley

Figure 1: Different Device Types Detected by NAC

Following device detection and profiling, access to resources can be controlled by using the device type and assessment information. For example, even if someone provides valid credentials to authenticate against the network, access can still be limited if an iPhone instead of a corporate managed notebook is used.

The capabilities used to detect and profile tablets and smartphones are the same ones broadly used by Enterasys solutions to automatically authenticate, assess and authorize any device connected to the infrastructure in a fully automated and dynamic fashion, lowering overall operational cost and enabling convergence while keeping security controls in place. Next we will take a look at the steps needed to ensure proper authentication, assessment and authorization for BYO devices.

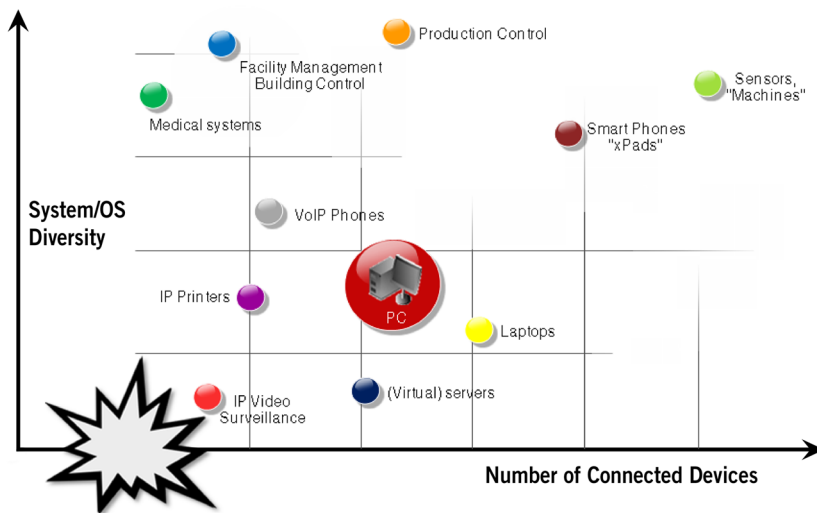


Figure 2: NAC Supporting Any Type of Device

## Authentication

Employees should be able to access the network anytime/anywhere and the network should dynamically assign the right access policy according to the rules/guidelines for the device and/or user connecting. Authentication is required to properly identify the employee along with their devices and dynamically grant them access to the IT infrastructure.

There are many technical methods that can be leveraged for authenticating end systems and/or users. A comprehensive NAC<sup>NG</sup> solution can support multiple methods like 802.1X port-based authentication for users and devices, MAC/IP and Hostname-based authentication, Web-based authentication and registration and Kerberos, along with LDAP-based integration.

Traditional authentication types used for managed devices typically involves 802.1x used in conjunction with certificate-based authentication using EAP-TLS. A BYO device won't have this type of authentication when first connected to the network and it might not be desirable to enroll certificates afterwards. Web-based registration plays an important role for BYO devices as they are not managed by the corporate IT, so they lack proper security configurations such as strong authentication using certificates and/or encryption settings for WiFi.

NAC<sup>NG</sup> provides an embedded web portal that allows users to register their device using their credentials – verified against LDAP or RADIUS servers. Subsequent actions could include the enrollment of certificates or the configuration of the device in an automated workflow using appropriate protocols like WMI (Windows Management Instrumentation) or MDM (Mobile Device Management), which are dependent on the use of WPA2-based encryption on the WiFi network.

enterasys  
Secure Networks™ There's nothing more important than our customers.

Welcome to the Enterprise Registration Center

**Access Denied!**

You have been denied network access because your device is not currently registered to the network. Please use the following button below to register your device and obtain network access. Note that you **must** have valid login credentials to register on the network.

<b>Network Login</b> If you have been issued credentials for this network, please login below. *User Name: <input type="text"/> *Password: <input type="password"/> <input type="button" value="Login"/>	<b>Register as a Guest</b> If you have not been issued credentials for this network, please register your device. <input type="button" value="Register"/>
--	---

Powered by  
enterasys  
Secure Networks™

xxxx Example Street, Example City, Example State xxxxxx | xxx.xxx.xxx | ©2011 Example Enterprise [About Us](#) | [Contact Us](#)

Figure 3: Web Registration Portal

## Assessment

The authentication process is an important component of any NAC implementation and BYO device management program. The function of assessment goes beyond the identity and tries to assess the end system itself. In doing so the compliance of the BYO endpoint configuration with corporate or governmental regulations can be verified and also potential vulnerabilities on the device can be detected. Subsequent remediation can also then be applied. Assessments, or health-checks, can be separated into two methods:

### Agent-less:

- Network-Based – a network scanner scans the end system remotely (over the network) or an API is used with valid credentials to remotely log-on to the device
- Applet-Based – a java applet is used to launch assessment functions on the end system (web-browser based)

---

## Agent-based:

- Dissolvable Agent – a temporary agent can be loaded and unloaded on the end system using various vendor-specific techniques
- Persistent Agent – a persistent suite of assessment software with firewall and host intrusion detection established on the end system

An extensive assessment can not only provide health and vulnerability status information about the end systems and devices, but also provide additional configuration data for inventory and auditing purposes. Network-based assessments with credentials (like mobile device management, or MDM) are preferable for BYO devices.

---

*“Students love to plug devices into our network, and with SIEM and NMS, no matter how many moves, adds or changes occur in our environment, we can keep everything in view and under control through role-based access controls and network behavior monitoring. NMS can even manage beyond Enterasys hardware to deliver standards-based control of other vendors’ network equipment, including our wireless network equipment. We were told by other vendors that this type of granular control wasn’t possible at the price point we required.”*

-Tannie Olsen, CIO, Oral Roberts University

---

## Authorization

Upon successful authentication and assessment, the last step in bringing an outside device on the network is authorization. Enterasys recommends using policies that are enforced at the entry point (access layer) into the infrastructure. This allows very granular control and also mitigates the risk associated with attacks to the infrastructure. The dynamic authorization at the entry point also enables mobility whereby the rules applied to the device moves with it throughout the network, seamlessly across wireless and wired connections.

Enterasys supports the assignment of rules and roles per user/device seamlessly across wired and wireless access devices. An important differentiator between the Enterasys solution and that from other vendors is the type of rules assigned. In the case of other solutions, only simple VLAN assignment is supported. Within the VLAN itself, there is no control at all, leading to the following issues:

- What happens if someone connects an unauthorized DHCP server to the VLAN (and logs on with appropriate credentials)?
- How do you distinguish VoIP from data traffic on a softphone (on the PC)?
- How do you distinguish data traffic from multiple virtual machines (VM) on the same host (PC or server)?
- How can you stop the propagation of a worm within a VLAN?

The rules applied by Enterasys to BYO devices are effective between the ports in the same VLAN and also recognize information from Layer 2 (VLAN/MAC address) through Layer 4 (applications such as e-mail, VoIP) – and will be extended up to Layer 7 in the future. Enterasys [NMS Policy Manager](#) ensures the performance of network services with the application of easy to configure individual policies (roles) seamlessly across wireless (WiFi) and wired access devices. The roles and rules are automatically distributed to all access devices so configuration consistency is ensured.

---

## Access Scenarios

While the steps needed to ensure proper authentication, assessment and authorization for BYO devices are important, it is also critical to determine the ways in which BYO devices access the network. There are various approaches on how to manage access to the network from BYO devices. Some corporations try to avoid BYO devices and focus on the management of these devices as they do for managed notebooks or desktops. This is quite challenging due to the dynamic nature of these devices and also the overall cost associated with them.

Connection of BYO devices and also corporate-provided tablets and smartphones can be managed by using either a Virtual Desktop Infrastructure (VDI) solution – so no data resides on these devices – or using the Enterasys approach of granular authorization for native access to mitigate risk and control access.

### Virtual Desktop Infrastructure

In a VDI infrastructure a hardware virtualization layer is used on the server side. The virtualization layer provisions numerous Virtual Machines (VMs) that are each supplied with an operating system, applications, and a unique GUI/desktop environment for each user. The solution provides the same basic functionality of a traditional server-based computing solution. With VDI, IT departments are presented with several benefits that cannot be achieved with the traditional approach:

- Centralized client OS management
- Rapid client deployment
- Reduction in desktop support costs
- Reduction in electricity costs, as thin client computers use only a fraction of amount of energy that is used by a desktop computer
- Improved data security as when devices are lost it does not affect corporate security since the data resides within the data center
- Fewer application compatibility problems as users have their own, single user OS
- Extension on the lifespan of legacy applications that aren't multiuser-enabled
- Easily deploy applications that use operating systems other than Windows

Due to these advantages existing VDI approaches should be extended to smartphones and tablets. New VDI deployments to support these devices have also been seen in the market but they typically require a justification beyond the operational advantages.

## Leveraging VDI

The VDI scenario works today in conjunction with the Citrix Receiver technology, the Citrix Virtual Desktop Infrastructure VDI solution XENDesktop and Enterasys NAC<sup>NG</sup> solution at the access layer of the network. Optionally, [Enterasys Data Center Manager](#) (DCM) within the data center can be used as well. Citrix Receiver is a universal client technology that enables the delivery of virtual desktops for Windows, web and SaaS applications, and can be delivered as an on-demand service to any location and device – whether a PC, Mac , laptop, netbook, tablet or smartphone . This approach has two advantages:

- Access into the corporate infrastructure can be restricted to just the virtual desktop access via Citrix ICA protocol, so no other resources are exposed
- Citrix Receiver does not require corporate data to be stored on the device, reducing the possibility of data leaks

Other VDI technologies like VMWare View 4.5 using PCoIP are supported as well with Enterasys DCM.

Leveraging Enterasys NAC<sup>NG</sup> at the access layer the devices can either be authenticated or automatically detected and profiled. After that step a very restrictive policy is dynamically applied to all intranet traffic originating from that device. This ensures that only the VDI services via the ICA protocol can be accessed in the corporate IT infrastructure. All internet traffic from that device is allowed so the users can fully leverage the benefits of the device and the apps installed.

As another option, the IT administrator can track users and virtual desktops in the data center by leveraging the integration of Enterasys DCM and Citrix XENDesktop (XDDC – XENDesktop Delivery Controller). Coordinating the automated assignment of VM's within both the virtual and physical network fabrics, DCM ensures that proper network resources are allocated when a VM is provisioned, no matter where it is on the network. In the case of VDI the provisioning is based on the role given to the user of any given VM. As VDI turns the policy enforcement model upside down – from client-side enforcement to server/VM side enforcement – it is key to keep the same controls in place as can be found in a typical fat client environment.

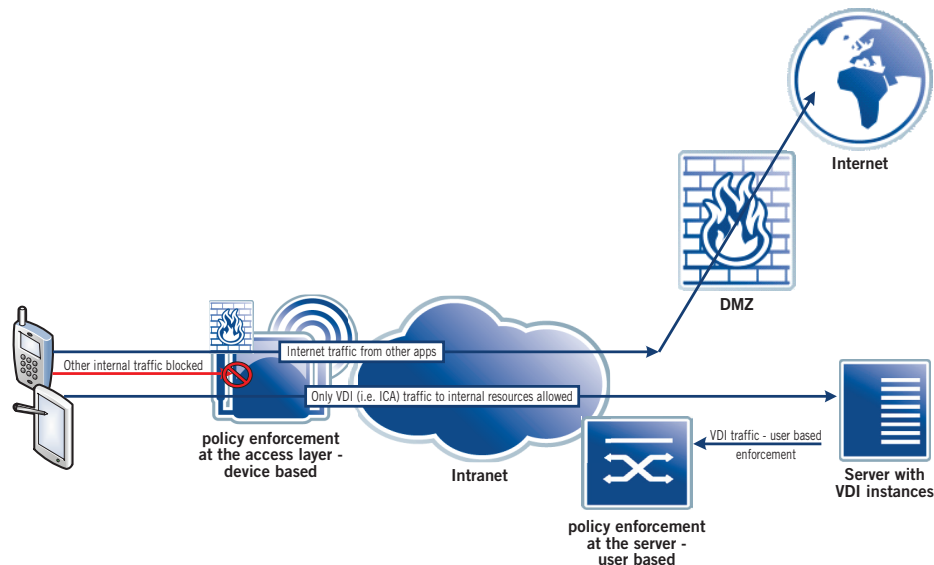


Figure 4: BYO Access Using VDI

## Native Access

As the VDI solution involves additional CAPEX and OPEX, some IT departments might opt for an Enterasys approach involving native access for BYO devices under strict guidelines and access control. In this case, the devices (or the users of that device) are authenticated or automatically detected similar to the VDI approach. Since the resulting policy will not be as restrictive as with the VDI approach, authentication, instead of auto detection, is recommended. With Enterasys NMS, the applied access control rules will allow access to the internet (if desired or required), also allow access to the necessary resources within the intranet, but block access to sensitive resources in the intranet. In doing so one can ensure service accessibility (i.e. access for mobile medical round support with iPads or electronic control slip in the production process) but still protect critical corporate resources. The advantage with this approach is reduced costs as corporate IT does not have to install and operate a VDI infrastructure. On the other hand, confidential corporate data might end up on a device that has internet access. Some applications do not require internet access – such as tablets in a production plant for monitoring purposes. In such a case, a potential security hole can be closed by denying internet access through policy.

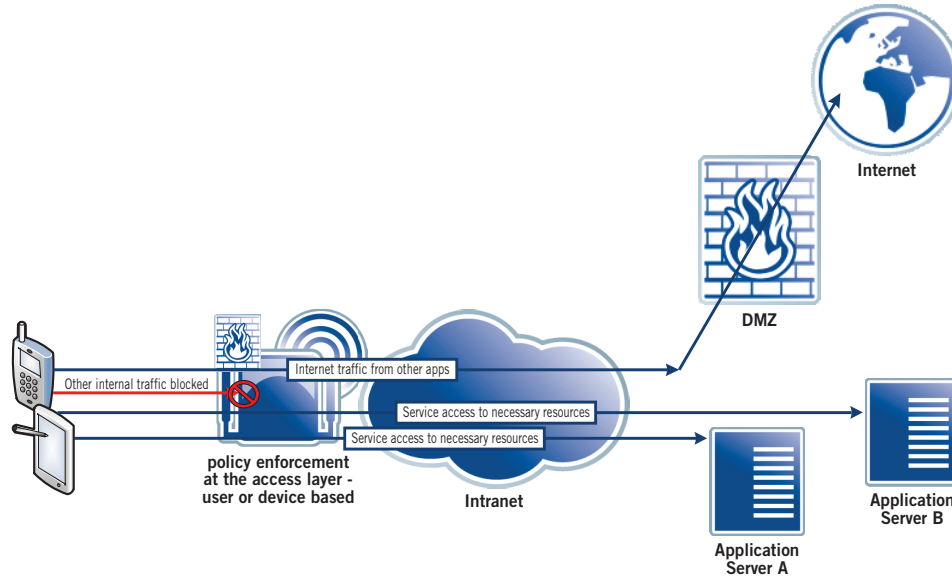


Figure 5: BYO Native Access

## Conclusion

The ability to support BYO devices is yet another example of how the Enterasys network and security architecture can be leveraged without additional software or hardware components to address new requirements in the IT infrastructure. The essential components, Enterasys NMS with NAC<sup>NG</sup>, policy-enabled WiFi [access points](#) and wired Ethernet switches leveraging the Enterasys [Coreflow2](#) technology, can be used to provide a higher degree of automation, visibility and control along with reduced operational costs for IT departments. The provisioning of access for any device type entering the corporate network is fully automated. Granular control of access is increased with security for unmanaged, unmanageable and private/BYO devices on the corporate network, with the business being able to leverage the efficiency gains of new and innovative devices.

## Contact Us

For more information, call Enterasys Networks toll free at **1-877-801-7082**, or +1-978-684-1000 and visit us on the Web at [enterasys.com](http://enterasys.com)



© 2011 Enterasys Networks, Inc. All rights reserved. Enterasys Networks reserves the right to change specifications without notice. Please contact your representative to confirm current specifications. Please visit <http://www.enterasys.com/company/trademarks.aspx> for trademark information.

