celestix

Delivering on the “PSN Compliant” Simplified Mobility Initiative

Whitepaper
March 2016

Simplified, Secure & Compliant Connectivity in the Public Sector

Mobile working in the public sector is not a new concept but in recent years the scale has increased significantly driven by the need to deliver greater efficiencies and work within mandated budget targets.

The demand for public organisations to deliver better services is challenging enough but the task is made harder when the books don't balance and you have to meet regulatory compliance standards.

The Public Services Network (PSN) was introduced in response to the need to drive efficiencies, and with the frameworks now in place organisations can focus on how to get the best outcomes from the PSN.

With greater mobile working, the introduction of cloud computing, and the need to engage the community, the traditional network perimeter has disappeared. Recent technological developments such as portable devices and touchscreen operating systems have provided the tools to deliver much greater collaboration, but with greater flexibility comes increased risk.

Organisations looking to embrace mobility as a means of improving services now need to consider security and compliance. The PSN Code of Connection focuses heavily on the need to achieve compliance for mobile working.

In this document we will explore the key considerations faced by public organisations when reviewing their mobile working strategy and we will review these in context of the PSN Code of Connection. We will look at how DirectAccess addresses the considerations for delivering secure, compliant and seamless mobile working.

The Nexus of Forces

There are many considerations that must be addressed by public sector organisations when reviewing their mobile working strategy but they can be grouped into three primary areas

- Ensuring compliance with regulatory guidelines
- Improving the remote working experience for users
- Reducing operational costs

Ensuring compliance

PSN guidelines take the form of the Code of Connection. This Co Co contains a number of Information Assurance Conditions that must be met in order to comply with the PSN.

There are four IA Conditions that relate directly to mobile working. The good news for public organisations looking to meet these conditions is that they are eminently reasonable. These conditions are as follows;

1. Operational Security
    a. Vulnerability & Patch Management – You must ensure that any exploitable vulnerability is managed. You must have a defined policy and supporting process to identify vulnerabilities, prioritise and mitigate those vulnerabilities
    b. Secure Configuration – You must ensure that all IT systems, software and services are appropriately configured to reduce the level of inherent vulnerability.
    c. Physical Security – You will ensure that appropriately secure accommodation and appropriate policies and practices governing its use are in place to protect from loss, damage or compromise
    d. Proactive Monitoring & Intrusion Detection – You will collect and retain event data and undertake activities that will help you detect actual or potential security incidents. You must have a protective monitoring policy…
    e. Security Incident Response – You must have a security incident management plan… EUDs must form part of the incident response plan… Your response plans should include how to manage such devices.

The conditions are fair but the challenge with mobile working is what happens when users and their devices do not regularly connect to the network. If devices do not connect then they cannot be patched, updated or scanned against the organisation’s security policies. Previous iterations of the PSN guidelines made reference to the need for organisations to be able to demonstrate “appropriate levels of management and control” of their IT estate. This requirement is still current, and many organisations perceive this as the most difficult objective to achieve.

2. Authentication & Access Control
    a) Users must identify and authenticate to devices and services. For passwords you must;
        a) Ensure all passwords are changed from defaults
        b) Combine passwords with some other form of strengthening authentication, such as lockouts, throttling or two-factor authentication
        c) Users will identify and authenticate to devices and services. Additionally only appropriately authorised devices will be provided with access to services.

Two factor authentication is commonly used to validate the identity of users who request access to the corporate network. Identifying users is essential but two factor authentication adds complexity to the login process and is a common cause of helpdesk calls. Ensuring sufficient levels of identity checking while not burdening the user or the helpdesk has to be a key component of a modern mobile working strategy. Complexity may result in lack of usability.

3. Boundary Protection & Interfaces

   a) You will ensure that your network has appropriately configured boundary protection between your network/services and the internet or any other network.

   b) Services presented outside of the protected enterprise should be delivered from an appropriate architecture, with access to any core information or services constrained.

   c) Unmanaged devices must not have access to the PSN. You must ensure that an unmanaged device accesses the corporate service through an appropriately secured connection

It is essential for organisations to consider the use of unmanaged devices. It is still common in the sector for an organisation to issue devices to their employees and prevent access from unmanaged devices. This typically requires a consideration around how to allow access from trusted users with managed devices and how to separate connectivity from unmanaged devices.

4. Protecting Data at Rest and in Transit

   Data will be protected by default whilst at rest and in transit

The need for encryption technology is well understood and the technology is already in widespread use. With the proliferation of encryption technology both at the endpoint and also to protect remote access sessions, most organisations should be able to demonstrate compliance with this condition without much of a challenge.

In addition to these guidelines is the requirement for public organisations to ensure they are using fully supported technologies. Due to the rapid technological advancements in mobile working technologies many remote access solutions have become End of Life (EoL). The use of EoL technologies is a risk that must be avoided.

Complying with the above guidelines is an excellent starting point for designing a mobile working strategy but compliance does not guarantee security. Compliance may also adversely impact the mobile working experience through the need to apply so much technology as to make the user experience difficult.

Improving the remote working experience

In surveys carried out by Celestix Networks, improvements to the remote working experience is the number one priority for public organisations when they address their mobility strategy.

Advancements in mobility technologies such as tablets, smart phones and software like Windows 8 and 10 have enabled organisations to embrace mobile working on a far greater scale.

The modern workforce now expects to be able to work remotely and in a flexible manner. Availability of the latest devices is seen as a benefit of most modern jobs.

The combination of a workforce that is hungry for flexibility and the availability of technology that supports it has provided organisations the ability to meet modern working requirements.

In public organisations the mobile working experience may also require the use of devices with 3G/4G connectivity, which further extends the capabilities of remote working, when signal reception allows.

But with greater flexibility comes a higher level of risk which, if not managed carefully, can affect an organisation's ability to comply with data handling regulations.

Reducing operational costs

Public organisations are under sustained pressure to demonstrate cost savings. Consolidating real estate and moving the workforce into fewer buildings is an obvious strategy but pressure is also on to drive the best return from the organisation's investment in infrastructure.

Organisations that have scaled down their real estate have been presented with an ideal opportunity to enable a more mobile workforce. The aforementioned advancements in mobile technologies support this. And because mobile working is not new, all organisations have technologies in place that can deliver mobile remote working already.

The challenge is not in enabling a mobile workforce but rather how to do it on a much larger scale.

Empowering a mobile workforce with new and diverse endpoints presents obvious security risks which are compounded by the greater number of staff now working remotely.

The other issue with reduction in real estate is that while it may allow an organisation to demonstrate cost savings it can often result in cost being moved rather than eliminated.

This is because of the increased cost in provisioning the mobile workforce with portable devices, and ensuring they are configured to connect to the network in a secure and compliant manner. There is likely to be a need to refresh the access gateway infrastructure to cope with the larger volume of remote connections.

Then there is the issue of increased burden on the IT helpdesk. Staff are employed based on their ability to deliver on the specific remit of their role, not on their ability to use IT. Many workers are not IT literate enough to work remotely without some level of assistance from the IT team.

When users have to interact with more IT such as a VPN client, endpoint encryption and two factor authentication there is more reason for things to go wrong. If that happens then they have to call IT because they cannot work until the issue is resolved.

So even through there is a focus on reducing operational costs, the provision of mobile working has the potential to increase IT costs considerably.

Summary of the Problem

Addressing the need for mobile working in the public sector requires a robust strategy. This is because of the increased scale of mobile working and the requirement to balance the needs of the organisation (the aim to reduce costs, the need to share data in a compliant manner) with those of the user (simplified experience, increasing productivity).

The good news is that due to developments in the field of mobile working there is a solution that can help organisations to balance all of these considerations while ensuring compliance with the PSN IA Conditions.

The Solution

With such a broad combination of compliance, security and flexibility, it would be understandable to assume that any solution would be expensive and complex to deploy. Yet since its launch, Celestix E Series has provided a very simple answer to the mobile working challenge.

Celestix delivers PSN compliant mobile working solutions to the public sector on their E Series range of appliance and virtual appliances. The platform includes a hardened and secure instance of Windows Server 2012 R2 which has been optimised to run the Unified Remote Access role.

Revolutionary remote access

One of the core remote access capabilities is DirectAccess, the most revolutionary advancement in the field of remote access since the launch of SSL VPN.
DirectAccess provides a secure and encrypted always on network connection for compatible domain joined Windows 7, 8 and 10 devices.

Furthermore, DirectAccess is CPA certified by CESG to deliver a compliant and secure remote access platform for the public sector.

Since its inception, Celestix E series has become the reference architecture for deploying simple mobile working that meets the PSN guidelines for secure collaboration. So how has DirectAccess been able to address the diverse and complex nexus of forces?

Improving the user experience

DirectAccess offers the remote worker the same experience as if they were sitting in their organisation's office. Connectivity from the endpoint device to the network is automated and requires no user interaction.

Not only does this enable the user to be more productive, it also removes the need for the user to interact with any complex technologies such as initiating a VPN session. This in turn reduces the volume of helpdesk calls from remote workers.

In addition, DirectAccess connectivity initiates rapidly, even over 3G networks, resulting in more remote devices connecting more regularly to the corporate domain. This drives even greater productivity gains particularly for truly mobile workers such as community workers.

Finally, DirectAccess will always attempt to connect to the network when the endpoint identifies an authenticated route to the internet. This process is automated meaning that even if a user's session drops it will automatically reconnect when able to do so.

Ensuring compliance AND security

DirectAccess is only available to domain joined devices running Windows 7 ultimate or Enterprise Edition, Windows 8 and 8.1 Enterprise Edition or Windows 10 Enterprise Edition. Connectivity between the endpoint device and the E series gateway appliance is encrypted and uses IPv6 for the transport to the gateway.

This has one powerful outcome when considering PSN compliance. It means that only employees using corporate issued devices that are a member of an AD group that is authorised to connect via DirectAccess, and that have a corporate issued certificate can gain access to the network.

Organisations that wish to show appropriate control and management of devices accessing their network can demonstrate this clearly with DirectAccess because the gateway is not available to anyone other than people and devices that meet the strict criteria.

In addition, the solution provides encryption profiles that are aligned to the PSN standards for interim and end state encryption, meaning that all remote sessions are fully encrypted in transit. In many instances, the session can be double encrypted.

DirectAccess delivers even greater security and control by virtue of its bi-directional connectivity.

Through this capability, DirectAccess empowers organisations to demonstrate far greater control and management of their IT environment in three principle ways;

1. DirectAccess enabled devices are always on the network and so can receive all group policy updates
2. DirectAccess enabled devices are always visible to the administrator and so user technical issues can be addressed without the need to use a third party tool to connect to the remote device.

3. DirectAccess enabled devices are accessible and so the organisation can initiate proactive vulnerability scans on all devices, regardless of their physical location.

The security capabilities don't end there. It is commonplace for organisations to enforce the use of endpoint encryption technologies such as bitlocker, which not only encrypt the device but can also be used to identify the user. The combination of machine based certificate, user credentials and encryption PIN being sufficient to achieve PSN approval.

Reducing costs

Unlike most traditional VPN solutions DirectAccess does not require the purchase of client access licenses. The only requirement to run DirectAccess is the use of a Windows Server 2012 R2 gateway device and a compatible version of Windows at the endpoint. Being able to reduce the need for licensing employees for remote access can deliver tangible cost reductions.

In addition the provisioning of the DirectAccess capability is delivered through issuance of group policy. There is no need to install any agent software on the devices.

Because of the high levels of security that are inherent in DirectAccess, most organisations are able to comply with PSN regulations while terminating the need for traditional user two-factor authentication, saving more money and further reducing IT administration overheads.

Meeting the Need – PSN compliant, user friendly, low cost mobile working

Transformational working initiatives aligned with developments in mobile working technologies have made it easier than ever to enable modern and flexible remote working.

Traditional VPN solutions may not be compatible with modern devices and operating systems and in many cases they are End of Life and require a significant investment to upgrade.

DirectAccess addresses all of the core PSN IA Conditions for mobile working and the bi-directional capability also enables organisations to comply with other aspects of the guidelines.

Compliance is easier to demonstrate by virtue of the CPA certification of DirectAccess.

But it is the improvement in remote working experience that really sets DirectAccess apart from other remote access solutions.

With DirectAccess it is possible to deliver a robust and consistent mobile working strategy.

Final Thoughts

This white paper concentrates solely on the use of DirectAccess for employee based access to the corporate network.

celestix

The E series solution also incorporates the other features of the Unified Remote Access role with Windows Server 2012 R2. These include IPsec VPN, web application proxy, AD FS proxy, Remote Desktop Gateway and Workplace Join.

About Celestix Networks: Celestix Networks is the world's largest Microsoft security OEM partner. The business has been supplying ISA server, TMG and UAG appliances to the public sector since 2004. Our solutions ensure a secure, reliable and performant platform and provide a range of enhancements to the DirectAccess solution.   Celestix e series is the reference architecture for deployment of Microsoft's DirectAccess solution within the public sector.

Copyright information

Corporate Headquarters
Celestix Networks, Inc.
3125 Skyway Court
Fremont, California 94539
+1 510 668 0700

EMEA Headquarters
95 London Street
Reading RG1 4QA
United Kingdom
+44 (0) 118 959 6198

Asia Pacific Headquarters
62 Ubi Road 1
#04-07 Oxely Bizhub 2
Singapore 408734
+65 6781 0700

Celestix Networks, Japan
2-12-4 Hirakawa-Cho
Chiyoda-ku
Tokyo, Japan
+81 3 5210 2991