Hardening BYOD: Implementing Critical Security Control 3 in a Bring Your Own Device (BYOD) Architecture

GIAC (GCCC) Gold Certification

Author: Christopher Jarko, csjarko@yahoo.com
Advisor: Tanya Baccam

Accepted: September 17, 2017

Template Version September 2014

Abstract

The increasing prevalence of Bring Your Own Device (BYOD) architecture poses many challenges to information security professionals. These include, but are not limited to: the risk of loss or theft, unauthorized access to sensitive corporate data, and lack of standardization and control. This last challenge can be particularly troublesome for an enterprise trying to implement the Center for Internet Security (CIS) Critical Security Controls for Effective Cyber Defense (CSCs). CSC 3, Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers, calls for hardened operating systems and applications. Even in traditional enterprise environments, this requires a certain amount of effort, but it is much more difficult in a BYOD architecture where computer hardware and software is unique to each employee and company control of that hardware and software is constrained. Still, it is possible to implement CSC 3 in a BYOD environment. This paper will examine options for managing a standard, secure Windows 10 laptop as part of a BYOD program, and will also discuss the policies, standards, and guidelines necessary to ensure the implementation of this Critical Security Control is as seamless as possible.

1. Introduction

Security professionals' desires are sometimes at odds with other trends in enterprise IT. One of those trends is called Bring Your Own Device, or BYOD. BYOD is a practice in which employees are allowed (or in some cases directed) to use personally-owned computing devices for work purposes. BYOD has its advantages and disadvantages, but from a security (or even a legal) standpoint, it is mostly a source of risk. Nevertheless, CISOs and their staffs may be forced by higher executives to implement BYOD. This research will examine the use of the Center for Internet Security's Critical Security Control 3 (*Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers*) as one part of that implementation. Specifically, this paper will focus on applying a standardized, hardened configuration to Windows 10, which could be found in either an enterprise environment or BYOD environment.

1.1. Bring Your Own Device (BYOD)

It is important to understand that for better or worse, BYOD is becoming increasingly widespread. According to one study, 74 percent of the companies surveyed had either already adopted BYOD or had plans to do so soon (Maddox, 2015). Accordingly, the information security community must try to figure out ways to securely implement BYOD.

1.2. Critical Security Controls

The Center for Internet Security (CIS) Critical Security Controls (CSCs) represent a collection of security best practices. Five tenets form the basis of CSCs: offense informs defense; prioritization (investment based on highest security gain); metrics; continuous diagnostics and mitigation; and automation (Center for Internet Security, 2016). The controls are organized into three families, *System* (Controls 1-10), *Network* (Controls 11-15), and *Application* (Controls 16-20) (Tarala, J.; Enclave Security, 2016). CIS does not prioritize the families but does prioritize controls within each family. CSC 1 (*Inventory of Authorized and Unauthorized Devices*) and CSC 2 (*Inventory of Authorized and Unauthorized Software*) provide greater risk reduction than CSC 3, and therefore should be implemented first (Center for Internet Security, 2016). An organization can begin work towards implementing CSC 11 (*Secure Configurations for Network Devices*) and CSC 16 (*Account Monitoring and Control*) at the same time it begins working on CSC 1, provided the organization has sufficient resources to do so (Tarala, 2016).

It is worth noting that CSC 3 is not the only control necessary to securely implement BYOD. Even in a BYOD environment, it is still necessary to maintain an inventory of all authorized and unauthorized devices and software (CSCs 1 and 2), to control access based on the need to know (CSC 14), and maintain a sound incident response infrastructure (CSC 19)(Center for Internet Security, 2016). Rather, this paper will focus on only one challenge to securely implementing BYOD – hardening an OS that will become increasingly prevalent with time, i.e., Windows 10. Furthermore, this paper will use a virtualized environment to demonstrate one method of hardening a Windows 10 laptop computer.

2. Problem – Securing BYOD

2.1. BYOD – A Heterogeneous Architecture

The term BYOD typically refers to mobile devices such as smartphones and tablets, but can also include laptops (Brooks, 2013). As the name states, “Bring Your Own Device” is the antithesis of a standardized (or homogeneous) architecture. In a traditional enterprise, limiting the number of different types of devices simplifies maintenance and configuration (Shinder, 2011). For example, since each make and model of laptop has different traits, having multiple models requires the IT staff to understand these differences so they can service the laptops more effectively. The heterogeneity of BYOD makes the IT staff’s job more complex, which in turn can necessitate higher wages to adequately compensate the IT technicians for the increased complexity.

2.2. Benefits of BYOD

2.2.1. User familiarity

The heterogeneous nature of BYOD architecture alleviates the issue of user familiarity since presumably each user is familiar with his or her own device, as well as the OS and applications typically installed on it. A user's familiarity with a device, OS, or application can significantly affect the overall user experience (Satia, 2013). The impact is perhaps most significant when considering the enterprise's Baby Boomer or Generation X users, who may not be as comfortable or literate with new technology as Millennials. For these older employees, learning to use new technology can be quite intimidating (Davis, 2016). The ability to use the same applications at work and at home has the potential to reduce employee stress.

2.2.2. Increased productivity and employee-driven innovation

Increased familiarity may translate into increased worker productivity. A 2012 study conducted by Cisco Internet Business Solutions Group (IBSG) showed that IT leaders cited increased productivity as a result of BYOD allowing employees to work when and where they liked (Cisco IBSG, 2012). Furthermore, this study linked employees' ability to choose when and where to work with an increase in employee-driven innovation. Being connected to company data around the clock also allows employees to develop good ideas as they happen, whenever they happen, rather than waiting until the next time they are in the office (Cisco IBSG, 2012).

2.2.3. Cost savings

Perhaps the most intuitive rationale behind adopting BYOD is the reduction in capital expenditures (CAPEX) and operating expenses (OPEX). Since the company is not responsible for procuring or maintaining the devices in a BYOD environment, this represents significant savings. The amount of savings varies from company to company, however, depending on how much direct IT support the company provides to employee-owned devices (Pinney, 2017).

2.3. Drawbacks of BYOD

2.3.1. Security risks

Data loss is perhaps the greatest risk introduced by BYOD. Companies seeking to implement BYOD securely must have policies on data storage and encryption, as well as the means to adhere to these policies. If a device is lost, the company must have the ability to wipe the devices to protect the data. This poses another problem; if the device cannot be selectively wiped, employees must accept the risk of permanently losing their personal data, even if their employer's data can be restored (Trend Micro Incorporated, 2012).

The ability to conduct work anywhere and anytime requires continuous Internet connectivity. This presumes the user will connect to networks beyond the company's control, which could range from open Wi-Fi to the employee's home network. Home networks have a high infection rate, as much as 14 percent according to one study (Alcatel-Lucent Motive Security Labs, 2015). This mobility and flexibility increases the risk of breach. Connecting to more networks increases the chance of connecting to an infected network. Moreover, connecting to a wider range of networks exposes the computer to a wider range of threats – perhaps including one against which his or her computer is not protected.

2.3.2. Legal risks

Securing corporate data in a BYOD environment can also expose the company to legal risk. If a company remotely wipes an employee's device and causes the employee to lose their digital media library permanently, the company might be liable for the value of the digital media. Given the storage capacity of modern devices, that media could be worth thousands of dollars (Pavón, 2013).

2.3.3. Privacy risks

Another significant risk of BYOD is the invasion of employee privacy. This risk affects both the company and the employee. Companies seeking overly broad control and monitoring over employee-owned devices may find themselves in court if they attempt to exercise that power (Pavón, 2013). From the employee's perspective, there is the possibility that the employer will be able to view all written communications from that device, whether business-related or not. This is a valid concern since there is at least one email client currently on the market that allows this (Pinney, 2017).

3. Tools for Securing BYOD

3.1. Policies and Standards

Security is not borne of technical solutions alone. In light of the concerns listed above, it is evident that any company wishing to implement BYOD securely must first develop well-reasoned policies, standards, and guidelines for their employees. This guidance should be written in consultation with corporate counsel to protect the company's interests and to ensure company leadership is aware of the risks they accept by adopting BYOD. Policies need to clearly delineate both the company's and the employees' responsibilities when company business is conducted on employee-owned devices. Standards for employee-owned devices may be necessary to ensure that any devices connecting to company resources are capable of being secured. For instance, the standard might require BYOD devices to run operating systems that are still fully supported by their manufacturer. The company should understand, however, that this may exclude some employees from being able to participate in BYOD, such as the accountant who refuses to migrate his laptop from Windows XP, or the HR specialist with a Windows Phone 8.1 (Microsoft ended support for Windows Phone 8.1 on July 11, 2017) (Forrest, 2017).

3.2. Security Templates

In order to implement CSC 3, an organization must choose a benchmark for the secure configuration of its hardware and software. Note that "secure" does not necessarily mean "standardized" by platform or OS across the entire enterprise. Effective security decisions take into consideration how and by whom the computers will be used. Different users have different requirements, rights, and privileges, but each user's hardware and software should be configured in such a way as to reflect sound information security principles (e.g., least privilege).

3.2.1. Group Policy Object (GPO) – based configuration

In an Active Directory Domain Services (AD DS) – based network, configuration requirements are typically enforced through the use of Group Policy Objects, or GPOs. GPOs contain a set of configuration instructions ("Group Policy") which are then applied to specific computers in the AD domain. GPOs give administrators the ability to build templates for standardizing the configuration of computers in the domain, and if desired, preventing users from changing the configuration of certain items. This is an excellent (and efficient) way to configure a large number of computers at once. Windows Domain Controllers apply Group Policy on a recurring basis: after Windows starts (computer settings), after user login (user settings), and at a predetermined recurring interval (the "Group Policy refresh interval") (Microsoft, Incorporated, 2011).

GPOs give administrators granular control over the AD domain, which means GPOs can be complicated. Also, by using the "Preferences" settings, the administrator can configure third-party applications by changing that application's registry settings (Microsoft, Incorporated, 2011). High granularity requires a significant time investment from the administrator, but fortunately GPOs are transferable in the form of an administrative template files. These files have the extension ".admx" and can be shared and applied to other domains by administrators with the appropriate permissions. Transferability notwithstanding, the ability to use a shared GPO does not relieve the receiving administrator of the burden of understanding that GPO's complexity. A responsible administrator does not make a change to his or her network without understanding the implications of that change.

Fortunately for administrators wishing to implement the Critical Security Controls, several good baselines already exist. Government agencies, non-government agencies, and commercial vendors have all produced baselines. The United States Government Configuration Baseline (USGCB) GPOs were developed by the National Institute of Standards and Technology (NIST). These GPOs are available for a wide range of OSs and applications. Unfortunately, as of July 2017, Windows 10 GPOs were not yet available (National Institute of Standards and Technology, 2017).

The U.S. Department of Defense (DoD) takes a slightly different approach to configuring their information systems. The Defense Information Systems Agency (DISA) has a downloadable Windows 10 Secure Host Baseline (SHB) image file which can serve as a starting point (Defense Information Systems Agency, 2016). To validate the configurations, the DoD relies upon Security Technical Implementation Guides (STIGs) and Security Recommendation Guides (SRGs), which are also produced by NIST. STIGs represent mandatory configuration settings for DoD computers and are subject to audit in DoD Command Cyber Readiness Inspections, while SRGs provide general security guidance (DoD Coalition of Apple Engineers, 2017). Within the STIG package, GPO templates are available for application to target systems.

As a non-government agency, the CIS also produces security benchmarks. Published after review and consensus by cybersecurity experts, the CIS benchmarks are like STIGs in that they contain configuration recommendations for hardening the target system. CIS benchmarks are free in .pdf format, but access to GPO templates requires a paid membership in CIS SecureSuite. CIS SecureSuite membership fees for a 100-employee company costs $3,240 for a one-year membership which includes additional benefits beyond access to the benchmark GPOs (Center for Internet Security, 2017). Nevertheless, the .pdf can be used to manually build the corresponding GPO – albeit with a significant investment in time. The Windows 10 Enterprise benchmark .pdf is over 900 pages long. It contains profile applicability, description and recommended settings, rationale, audit instructions, group policy remediation instructions, impact, default values, and references (Common Configuration Enumeration (CCE) and CIS CSC) for each configuration item (Center for Internet Security, 2017).

Vendors also produce hardening guides, and Microsoft is no exception. The "Security Baseline" is a downloadable package containing importable .admx files as well as a spreadsheet listing the security settings for the administrative templates. The spreadsheet columns can be filtered to assist administrators in finding settings or templates specific to their needs (Margosis, 2016).

3.2.2. EMM-based configuration

For all the benefits these templates bring to the administrator, there are a few disadvantages. First, templates and benchmarks are usually specific to only one part of a given computer's total software build. For example, the STIG and CIS Benchmark cited earlier apply only to the Windows 10 OS. To securely configure other software such as a browser or word processor application, an administrator would also need to apply the appropriate STIGs or CIS Benchmarks for these applications. More benchmarks equals more time to implement them as well as increased likelihood of compatibility problems between computer or network settings.

Second, with few exceptions, GPOs can only be applied to Windows computers, and with regards to Windows 10, only the Enterprise and Professional Editions, but not the Home Edition. In an enterprise setting, this is most likely not going to cause a problem, but in a BYOD scenario, it might. Assuming the company intends to implement BYOD to the broadest possible audience, it is reasonable to allow employees to register any currently supported version and edition of Windows, which could easily include Windows 10 Home Edition. Since Windows 10 Home Edition cannot be managed with GPOs, another solution must be found to manage these devices.

So if GPOs cannot be used to manage all of the company's BYOD devices, why mention them at all? The reason is that if the company's enterprise devices are predominantly Windows-based and networked in an AD DS environment like the vast majority of all business networks, GPOs will almost certainly be used to configure and enforce policy (Desktop Windows Versions Market Share Worldwide June 2016 to June 2017, 2017). This will come into play later if the company pursues a unified management platform, but in the meantime, there is another option to manage mobile devices – Enterprise Mobility Management, or EMM.

3.3. Enterprise Mobility Management (EMM)

Enterprise Mobility Management (EMM) refers to a class of software used to give administrators a degree of control over the mobile devices connecting to the enterprise. The amount and granularity of the control, as well as the variety of supported devices, varies from EMM suite to EMM suite. EMM may be cloud-based, hosted on premises, or a hybrid of the two (Microsoft, Incorporated, 2017). EMM typically performs one or more of the following functions: Mobile Device Management (MDM), Mobile Application Management (MAM), or Mobile Content Management (MCM) (Lorenc, 2016).

3.3.1. Mobile Device Management (MDM)

MDM gives a company the ability to remotely service mobile devices by monitoring and controlling hardware and software configurations on those devices. Among other things, MDM can control whether or not a given device is allowed to access company resources, push required software (and in some cases, delete unauthorized software), adjust device configuration to comply with security policies, and produce detailed reports on the device's hardware and software. Some MDM solutions can also allow companies the ability to selectively wipe a device, removing company data but leaving employee-owned data intact (B2Bwhiteboard, 2013). Finally, and perhaps most importantly for a company wishing to implement the CSCs, MDM can produce an inventory of authorized and unauthorized hardware and software in accordance with CSCs 1 and 2.

3.3.2. Mobile Application Management (MAM)

MAM gives a company the ability to control which applications are used to access specific company resources and to prevent the transfer of company data from authorized applications to unauthorized applications. By focusing on the application rather than the device, MAM is considered less intrusive than MDM (Hess, 2014). MAM can also be used to manage software licenses and deploy in-house applications to employees, whether through a company app store or another OS app store such as the Windows Store or the Apple App Store (Rouse, 2016).

3.3.3. Mobile Content Management (MCM)

MCM software stores and distributes files to mobile users, synchronizing changes to those files in order to ensure the file represents only the most current information. MCM is not new; Dropbox and SharePoint are examples of Content Management Systems (CMS). MCM is a logical extension of CMS to the mobile device business space (Lindner, 2016).

3.3.4. EMM Suites

There are several EMM solutions available, but as an exemplar EMM suite, Microsoft Enterprise Mobility + Security (EMS) combines MDM and MAM and provides companies significant granularity in configuration control of BYOD devices through its management tool, Microsoft Intune. Moreover, EMS works with many different OSs, including desktop versions of Windows. Intune can be implemented as part of a comprehensive cloud architecture (integrated with Azure Active Directory and Office 365), or it can be combined with on-premises computer management (integrated with System Center Configuration Manager (SCCM)) (Microsoft, Incorporated, 2017).

As might be expected, the capabilities that EMM suites can bring to a company do not come cheaply for any but the smallest organizations. Manage Engine offers free downloads of their Desktop Central desktop manager and Mobile Device Manager Plus EMM software for up to 25 computers and 25 mobile devices (Zoho Corporation, 2017), and AppTec offers a free download of its AppTec360 EMM for use on up to 25 mobile devices (AppTec GMBH, 2017). Microsoft does not offer a comparable free download of EMS for small businesses. Beyond such small-scale deployments, EMM costs add up quickly, with pricing models varying from vendor to vendor. As of July, 2017, a company wishing to implement Manage Engine's Desktop Central and Mobile Device Manager Plus on 100 computers and 100 mobile devices respectively will pay approximately $2,890 for licensing the software and one user, plus $10,000 for an additional 100 user licenses (Zoho Corporation, 2017). This implementation adds up to an annual cost of $12,890. Microsoft EMS is licensed per user at a rate of either $8.75 or $15.00 per user per month, depending on the version selected, for an annual cost of either $10,605 or $18,180 for the same 101 users. Given that EMS subscriptions include a Windows Server Client Access License (CAL) which allows users to access EMS services from multiple devices, the Microsoft pricing model could potentially represent a better Return on Investment (ROI) per user (Microsoft, Incorporated, 2017).

Beyond the cost of implementation, there is another reason to adopt a Microsoft MDM solution: integration with the remainder of the enterprise. As stated earlier in this paper, most enterprises are Windows-centric (Desktop Windows Versions Market Share Worldwide June 2016 to June 2017, 2017). Microsoft EMS and Intune seamlessly integrate with Microsoft's cloud-based applications, such as Azure Active Directory and Office 365 (Microsoft, Incorporated, 2017). Using another Microsoft solution decreases the risk of incompatibility with existing applications.

4. Implementation

4.1. Scene Setter – Hypergolic Reactions, LLC

There are many options available for securely implementing BYOD using EMM, and many driving factors for these options. The size and purpose of the company as well as the nature of the company's existing or planned network architecture (on-premises or cloud-based) can guide a company towards a particular solution. For a large company with a cloud-based architecture, it is more logical to pursue a cloud-based EMM solution rather than to procure and maintain separate on-premises architecture to manage BYOD. In this manner, the company can leverage existing Service-Level Agreements (SLAs) for cloud support and perhaps negotiate a better price for their existing cloud services by adding an EMM solution.

Another set of driving factors includes the degree of control the company chooses (or needs) to exert over personally-owned devices and the company's data protection compliance requirements. This second factor, data protection compliance requirements may subsequently decide which devices are allowed to integrate into the BYOD environment, perhaps by limiting which employees are allowed by the company to participate in BYOD. For example, an employee whose work deals almost entirely with Protected Health Information (PHI) could be excluded from participation in BYOD if the company's EMM solution does not comply with existing data protection laws. While there may be other solutions to limit exposure of PHI in this case (such as internal business rules governing the content of corporate emails, the company should still examine whether a particular EMM solution increases or mitigates the risk of unauthorized disclosure of protected information.

Finally, there are the questions of how much money the company is willing to spend, or whether the company chooses to use a particular vendor. As stated earlier, EMM solutions are not inexpensive, especially for a large enterprise. As with any infrastructure decision, a company's budget plays a decisive role. From a security perspective, a CISO must examine the EMM options available within the company's resource constraints and decide which options meet the minimum security needs. Vendor choice can also play a role, since price ranges vary among vendors. While software may interact better with other applications from the same vendor, a company with tight resource constraints may find itself unable to afford a suitable EMM solution.

Considering all the factors listed above, it is impossible to present a single solution that meets the needs of every situation. For this purposes of this paper, however, the following notional company will be used: Hypergolic Reactions, LLC, ("Hypergolic") a producer of liquid rocket fuel and other hazardous materials, has less than 500 employees. Although some of Hypergolic's servers are virtual machines, the company's IT hardware is entirely on premises. With regards to software, Hypergolic is already using some cloud-based Software as a Service (SaaS), in particular, Office 365, but provisions the majority of its software on-premises. This may change in the future, however, as there is a push from Hypergolic's Chief Financial Officer (CFO) to transition to the cloud (using Microsoft Azure) as much as possible within the next three years. Except for a few isolated UNIX and Linux-based servers and Industrial Control Systems (ICS) used in Hypergolic's headquarters and manufacturing facilities and equipment, the enterprise is Windows-based. Servers run Windows Server 2012 R2 using Active Directory Domain Services and SCCM (Current Branch), and enterprise desktops are running mostly Windows 7 Enterprise (a few newer desktops have Windows 10 Enterprise, and there is a developmental project using Windows Holographic). There is a plan to migrate all servers to Windows Server 2016 and all desktops to Windows 10 Enterprise by January 1, 2019. Potential BYOD devices will include Android, iOS, and Windows phones and tablets, MacOS and Windows laptops, and possibly even Microsoft HoloLens devices (pending the success of the developmental project).

The push to allow BYOD came from the CFO, who convinced Hypergolic's Chief Executive Officer (CEO) that adopting BYOD would result in a reduction of CAPEX and OPEX, making the benefits outweigh the security and legal risks voiced by the CISO and Hypergolic's Legal Department. With that in mind, the CISO has been tasked to find a way to implement BYOD securely. Hypergolic is a member of CIS SecureSuite, and the CISO was already in the process of adopting the CIS CSCs for the enterprise, having already completed CSC 1 *(Inventory of Authorized and Unauthorized Devices)* and CSC 2 *(Inventory of Authorized and Unauthorized Software)*. This is fortuitous since completion of CSCs 1 and 2 are required prior to implementing CSC 3 (Center for Internet Security, 2016). It is important to note, however, that implementing CSCs 1 and 2 will subsequently mandate the registration of BYOD devices with MDM software in order to allow Hypergolic the ability to maintain accurate and complete device and software inventories. Hypergolic's CISO will begin adoption of BYOD with a pilot program consisting of a few select users in the IT department.

4.2. Options

Given the nature of Hypergolic's enterprise and proposed BYOD, there are three options for managing mobile devices. The first option is a cloud-based EMM such as Microsoft's Enterprise Mobility + Security (EMS) or AppTec360 EMM. Despite being almost infinitely scalable, the significant cost of implementation, along with the fact that the enterprise has not yet become fully cloud-based, make this solution less than optimal for Hypergolic, at least for the time being. If the CFO's push to migrate to the cloud becomes reality, the company can revisit this option.

The second option for managing mobile devices is to use on-premises EMM. In the case of Hypergolic, this would be done through existing SCCM infrastructure, which Hypergolic is already using to manage its on-premises computers. However, since on-premises MDM can only be used to manage Windows 10 and Windows 10 Mobile devices, this option is also unsuitable (Microsoft, Incorporated, 2017).

The third option is hybrid MDM using SCCM (Current Branch) in conjunction with Intune. This option will best meet Hypergolic's needs for several reasons. First, it leverages Hypergolic's existing infrastructure, since no new IT hardware is required, and Intune integrates well with Office 365. Second, the cost to implement, though significant, is within Hypergolic's means. Third, hybrid MDM maintains homogeneity among enterprise management software, since it uses another Microsoft product. That being said, homogeneity is not a necessity; as shown earlier in this paper, there are many vendors with MDM and EMM products. Still, there can be benefits to going with a single vendor, as the IT staff may find it easier to learn another Microsoft product. Also, a different vendor could use different terminology or even a different approach to asset management. Finally, and perhaps most important, is that hybrid MDM could ease the transition into the cloud since Intune includes the ability to manage Office 365 applications. If Hypergolic increases its cloud presence, Intune can be used to manage more of these cloud-based applications.

4.3. Execution – Hybrid Mobile Device Management

4.3.1. SCCM

In this scenario, Hypergolic's previous use of SCCM to manage on-premises computers is a critical precondition. If SCCM had not already been in use, a better choice might have been to expedite the move to the cloud. The reason for this is that SCCM installation and configuration is not a trivial undertaking. A significant number of prerequisite roles and features that must be installed and configured on the SCCM site server for SCCM to properly function. These roles and features include Internet Information Services (IIS – Microsoft's Web server), SQL Server, Windows Server Update Services (WSUS), as well as several other server functions and management tools (Microsoft, Incorporated, 2017). Many of these roles and functions are necessary to ensure the SCCM server can communicate with the computers it manages. Some of these roles and functions may have been installed previously, but if not, they must be installed and configured in a manner appropriate for the network.

SCCM installation files come with a prerequisite checker, *prereqchk.exe*, which provides a report administrators can use to identify potential problems. However, not every issue identified by prereqchk.exe is necessarily a critical flaw. Some configuration issues may or may not be a problem, depending on other factors such as whether or not the Active Directory domain uses Public Key Infrastructure (PKI). Still, the results give administrators a place to start looking in case the SCCM installation does not go smoothly.

SCCM is not required to manage computers in an Active Directory domain. Active Directory organically contains all the tools required to manage computers, users, and accounts, while the Group Policy Management application can create, distribute, and enforce GPOs. Nevertheless, SCCM consolidates many management functions in a single location, and administrators should consider its use.

4.3.2. Microsoft Intune

Microsoft Intune, a cloud-based service, performs the other half of hybrid MDM. Intune acts as a delivery means from SCCM to the managed devices. With hybrid MDM, user devices are enrolled either automatically or by the users themselves, depending on the OS of the user's device, the type of AD used in the company domain (Azure AD or on-premises AD DS), and whether the user or the company owns the device. For user-owned Windows 10 devices, MDM enrollment is performed by the user (Microsoft, Incorporated, 2017). Each user must create an Intune account with their business domain identity through the Office 365 Portal, which is a simple process. Step-by-step instructions are available at https://docs.microsoft.com/en-us/intune/introduction-intune.

4.3.3. Device (and application) management

In hybrid MDM using SCCM and Intune, core device management functions (to include device and software inventory) require device enrollment. Beyond enrollment, there are additional ways to configure these devices. These methods, while optional, give administrators a significantly greater degree of control. The additional configuration methods include configuration items, application management, resource access, and conditional access.

Configuration items include matters such as password and PIN requirements (use, complexity, and quality), the ability to use or restrict the device's camera, microphone, or Bluetooth, and even the ability to take a screen capture from the employee's device, along with many other controls. Obviously, some of these controls are somewhat intrusive from the employee's perspective, but they do grant the company additional means of preventing data loss caused by an individual using an authorized device in an unauthorized manner. For example, disabling the camera and microphone would prevent unauthorized recording during a meeting discussing sensitive information. Since many people probably use their cellphones as digital cameras to record important moments of everyday life such as family vacations and their children’s birthday parties, disabling these features could prove very unpopular. On the other hand, these same employees might not question a prohibition on bringing a traditional video camera or other recording equipment into a meeting. This highlights the need to include employee education as part of the BYOD implementation process to help employees understand the intrusion on their personal lives caused by policies such as disabling cellphone cameras and microphones is necessary to protect company data.

In the context of hybrid MDM, application management refers primarily to the company's ability to deploy and manage company-created applications to the mobile devices. This type of application management is invaluable when a company uses proprietary software which produces proprietary data. In addition to application deployment, the application management function in SCCM allows the company to configure the applications to comply with company security policies. One such policy could be to prevent cutting data from a managed application and pasting it into an unmanaged one, resulting in data loss (Microsoft, Incorporated, 2017). In addition to company-produced applications, certain browsers can also be managed, providing the ability to more effectively restrict Internet use (but only by the managed browser).

Browser management policies can include URL whitelisting and blacklisting, which if used in coordination with credential restrictions at a company web portal for a sensitive database, can ensure that employees only view sensitive company data with the company-managed browser. If the company takes this a step further and combines browser management with another application management policy prohibiting cut-and-paste from managed to unmanaged applications, as well as a configuration policy preventing the user from taking screenshots, the sensitive data available from that web portal is much more secure.

Resource access refers to device access to Wi-Fi, email, and VPNs. These policies enable administrators to push configuration settings and Personal Information Exchange (PFX) certificates to target devices, enabling employees to connect to these services more easily. This ease of connection is not a security feature per se, as the users would need to configure their devices manually, but it does relieve the employees from the sometimes frustrating task of configuring connections (Microsoft, Incorporated, 2017).

Conditional access is essentially the use of configuration policies as a condition to access specific company resources such as Microsoft Exchange, SharePoint, or Skype. A typical conditional access policy could be to require a password on any device attempting to connect to the company's Exchange Online server. Another example applicable to BYOD would be to prohibit "jailbroken" devices from connecting to the company SharePoint site. It is important to note that only certain client/server/resource combinations support conditional access.

4.4. Using the Create Configuration Item Wizard

The Create Configuration Item Wizard is the means by which administrators apply security controls to enforce company policy. The following sections will discuss some of the settings chosen by Hypergolic for the BYOD Test Group. Screenshots taken while running the wizard will be provided in Appendix A of this paper and are hyperlinked to their references (e.g., pressing "control" and clicking "Figure 1" links to the appropriate screenshot).

4.4.1. Selecting and modifying a standard

Before actually running the wizard, the company must decide what to use as a foundation for the configuration item and then must modify it as appropriate for the circumstances. For the CISO of Hypergolic, selecting the foundational standard was easy. Since Hypergolic is a member of CIS SecureSuite, they already have access to and are using CIS Benchmarks for their enterprise hardware and software whenever possible. Modifying the benchmark for use by the BYOD Test Group was not as simple. The CIS Benchmark for Windows 10 was designed for use on Windows 10 Enterprise. It is very unlikely that an employee will have a licensed copy of that version of Windows on their personally-owned laptop, so the CIS Benchmark will contain some settings that will not be applicable and must either be ignored or modified. (Note that while this paper uses a CIS Benchmark as a foundation, other standards (such as STIGs) would also require modification.)

4.4.2. Starting the wizard

The Create Configuration Item Wizard is fairly user-friendly. Upon opening the wizard, the administrator is asked to provide a name and description for the configuration item, as well as the type of configuration item based on the devices to be managed by SCCM. In the description block, it may be advisable to list a point of contact for the policy in question, as this may help future administrators should there be questions about why certain configuration settings were chosen (Figure 1). Also, there is a block for selecting a category for the configuration item (Figure 2) or creating a new category if required (Figure 3). Next, the administrator must select the applicable target platforms, in this case Windows 10 (Figure 4). Since Hypergolic is creating a configuration item for use in conjunction with Hybrid MDM, the administrator has selected "Windows 8.1 and Windows 10" under "Settings for devices managed without the Configuration Manager client." While this may seem counterintuitive since administrators create configuration items on SCCM, under Hybrid MDM, the BYOD devices themselves are being managed with Microsoft Intune, as mentioned earlier.

4.4.3. Device settings

Now the administrator may choose what types of settings the configuration item will affect. The wizard bundles these settings into groups such as "Password," "Device," "Security," and "Encryption.” There are a total of 17 groups, plus the option to configure additional settings that are not in the default groups (Figure 5). It is not necessary to select all groups, but for each group selected, the administrator should perform a “cross-walk” with the foundational standard (in this case, the CIS Benchmark for Windows 10 Enterprise), making sure that the configuration item settings are congruent with the settings enforced for enterprise devices as appropriate. When a mobile device setting *could* be identical to an enterprise GPO, but is different, it should be as the result of a conscious decision by company leadership, and documented in a written company policy. Codifying the difference helps to ensure awareness of what risks the company accepts as a result of implementing a BYOD program. Note that this written policy requirement does not apply when settings are different as the result of technological differences between BYOD and enterprise devices. Moreover, administrators should keep in mind that the enterprise may not adhere to their selected standard verbatim, either. As with any collection of security recommendations or best practices, a company or business unit within that company may have legitimate reasons for deviating from a standard, but these too should be documented as audit exceptions and supported by written policy.

In the Password Settings group (Figure 6), the Hypergolic administrator has selected “Required” in keeping with the CIS Benchmark, and as is the case for all settings for this configuration item, has also selected the box marked "Remediate noncompliant settings." As the name implies, this means that when BYOD devices connect to Hypergolic servers, the servers will not only check for compliance but will also apply changes as required to ensure compliance with the benchmark. This remediation serves as an effective backstop in the event that users are inadvertently or intentionally allowed to reconfigure their devices when not connected to company assets. All password settings selected by Hypergolic meet or exceed the CIS Benchmark: 16 character minimum password length, 60-day password expiration, strong password complexity, and 24 passwords remembered. Additionally, some settings do not directly correspond to the CIS Benchmark but are analogous. Whereas the CIS Benchmark for Windows 10 Enterprise calls for account lockout after anywhere between one and ten failed login attempts, the SCCM configuration item options call for the device to be *wiped* after a specified number of failed login attempts (in this case, eight) (Center for Internet Security, 2017). The ability to wipe a device rather than merely lockout an account provides improved security in the event of a lost or stolen device, which is much more likely with a BYOD laptop than with an enterprise computer.

The Configure Device Settings group (Figure 7) contains several settings that can mitigate insider threat. These include the ability to disable screen capture, copy and paste, and voice recording, each of which could be used to circumvent conditional access controls. Also, there are settings in this group that can be used to reduce the device's attack surface by prohibiting the use of Bluetooth. While the Windows 10 benchmark does not address Bluetooth, it does address Cortana. Adhering to the benchmark, the Hypergolic administrator has set Cortana to "Prohibited."

Many of the options in the Configure Email Management Settings group (Figure 8) are also generally not found in the CIS Benchmark for Windows 10 but may be addressed elsewhere, such as the benchmark for Microsoft Outlook. Therefore, when selecting a foundational standard – whether CIS benchmarks, DISA STIGs, or vendor's hardening guides – administrators should be careful to use *all* available relevant standards and not just the one for the OS. Another factor to consider with regards to this group is the fact that the administrator may be forced to deviate from the benchmark depending on how company provisions email, or possibly for other reasons, such as internal business practices or even the practices of external business partners. For example, Hypergolic has an external business partner who uses HTML format for email. If “Allowed message formats” is set to “Plain Text,” HTML email messages will not render properly without manual intervention by the recipient. Since the business partner is a trusted sender whose email is necessary for Hypergolic to conduct its operations, the Hypergolic administrator has little choice but to set “Allowed message formats” to “HTML and Plain Text” despite the increased security risk.

The Configure Browser Settings group (Figure 9) contains default settings for browsers but does not have an option to select a default browser. Microsoft Edge, the browser designed specifically for use with Windows 10, is configured by a separate settings group. The Microsoft Edge Settings group contains settings similar to those found in the Configure Browser Settings group. Regardless of which browser or browsers the company uses, administrators should reference additional standards as needed to ensure secure configuration.

Device Security Settings (Figure 10) and Device Encryption Settings (Figure 11) provide additional opportunities to reduce the attack surface or reduce the risk of data loss. Some settings accomplish both. For example, prohibiting USB connections can prevent sensitive company data from being exfiltrated via USB connection (e.g., removable media or another computer), while simultaneously preventing the introduction of malware through infected removable media.

Administrators can pre-configure BYOD devices to assist users in connecting to company wireless networks through the Configure Mobile Device Wireless Communication Settings group (Figure 12). Multiple wireless connections can be predefined (Figure 13), which can be particularly beneficial for BYOD users who need to visit multiple company locations. Additionally, this settings group can be used to disallow manual wireless configuration, effectively restricting the device’s wireless use exclusively to networks defined in this configuration item.

The System Security Settings group is used to enforce good security practices such as the use of anti-virus software with current malware definitions, or the automatic download and installation of Windows updates. Administrators should take care with this latter item, however. In the example shown in Figure 14, the Hypergolic administrator has selected “Auto install and reboot at maintenance time." This setting could have adverse effects for some users, depending on their work habits. Having one's work interrupted by software installation and reboot could be not only inconvenient but also operationally unsound. Administrators should coordinate with BYOD workers before deploying this configuration item to avoid unintended consequences.

While Hypergolic did not choose to implement settings not defined in an existing group, they could have done so using the Additional Settings group seen in Figure 15. This group allows administrators to choose one or more settings from an otherwise unused group, or even create a new setting by providing an appropriate registry key. The Additional Settings group is also noteworthy for the warning it gives administrators, admonishing them that modifying a setting through this group can cause a conflict if the same setting has already been modified elsewhere.

The screenshots represented in Figure 16, Figure 17, Figure 18, and Figure 19 are from the Configure Windows Information Protection (WIP) Settings group. WIP, formerly known as Enterprise Data Protection (EDP), is a Data Loss Prevention (DLP) solution designed by Microsoft for MDM. According to Microsoft, WIP enhances segregation between personal and company data, improves encryption of company data, and also performs certain conditional access functions (Microsoft, Incorporated, 2017). Configuring WIP settings is fairly involved and requires the enterprise domain to be well-defined by both Fully Qualified Domain Name (FQDN) and IP address ranges. Since data encryption plays a significant role in WIP, a Data Recovery Agent (DRA) certificate can be used or created as needed. Finally, there is an option to remove encryption keys from devices automatically upon disenrollment from MDM. Removing keys prevents circumvention of conditional access controls and also protects encrypted company data even if the device is stolen or the employee leaves the company without clearing their BYOD devices through the IT department.

The Configure Windows Defender Settings group (Figure 20, Figure 21, and Figure 22) helps companies take advantage of the organic anti-malware capabilities built into Windows desktop operating systems. There are two considerations to keep in mind regarding this settings group. First, third-party anti-malware solutions may not work in tandem with Windows Defender. If the company wishes to use Windows Defender for BYOD devices, they should consider it the required anti-malware solution. On the positive side, using Windows Defender in this manner eliminates the need for users to pay for anti-malware software, although this may not represent a concern for a significant number of users. Second, administrators should be aware that beginning with Windows 10 version 1703, Windows Defender is now known as Windows Defender Security Center. The new Windows Defender Security Center includes several other functions including parental controls, device health and performance, application and browser control, and firewall and network protection (Windows Firewall is no longer a separate application) (Microsoft, Incorporated, 2017). Administrators need to be aware of this because as of August 2017, the Configure Windows Defender Settings group only addresses the anti-malware function.

Once the administrator has configured all selected settings groups, the wizard checks the applicability of the settings for the designated target computers (Figure 23). The absence of excluded settings does not mean all configurations will work on the target devices without affecting their performance; it only means the settings are *configurable* on these devices. Moreover, the absence of exclusions does not imply that the configuration item (or any particular setting in the configuration item) is in line with good security practices or a particular benchmark. Finally, the presence of an excluded setting does not mean the setting in question is "incorrect" in terms of providing security or being in conflict with other settings. Rather, the setting is not applicable to one or more of the intended platforms.

Following the applicability check, the wizard produces a summary of the configuration item showing which settings were affected (but not the values for each setting) (Figure 24). This summary can be used to review against the chosen benchmark to see if there are any gaps in what needs to be configured. If the administrator missed something, he or she can go back through the wizard and change settings or add or remove groups as needed. Once the administrator has appropriately configured all settings, the wizard can apply the changes and create the configuration item. If successful, a completion screen is shown (Figure 25). At this point, the administrator may want to copy the item summary text and paste it to a document for easy reference in the future. Such a document is shown in Part 2 of Appendix A to this paper and shows how extensive configuration items can be. After creating the configuration item, it is ready for deployment to BYOD devices (Figure 26). If necessary, configuration items can be edited later.

5. Conclusion - Taking an Integrated Approach to BYOD Security

Hybrid MDM with SCCM and Intune facilitates the technical means of integrating security. To quote Microsoft, this approach provides a "single pane of glass" to manage the configuration of mobile devices and on-premises computers (Microsoft, Incorporated, 2017). To be more effective, however, security professionals should look past the technical solution to ensure some degree of consistency between on premises and BYOD security policy and enforcement. “Some degree” is a very important caveat in a scenario with BYOD. Complete consistency – true standardization – is almost certainly impossible to achieve, between the peculiarities of EMM solutions, the seemingly endless possible configurations of employee-owned devices, and the degree to which employees (to include management) will be willing to accept company control over their personal smartphones, tablets, and laptops. Nonetheless, a company wanting to implement a BYOD program must consider those devices as part of the enterprise, at least for security purposes. Administrators must compare configuration items, resource access, and other mobile device policies against the analogous GPOs for on-premises computers. If the company is unwilling to promulgate and enforce the same policy for a desktop PC in Accounting as for an accountant’s smartphone, it begs the question as to whether or not the desktop policy is still a valid one.

The risk of this inconsistency is one of the reasons is so difficult to implement BYOD securely. For a CISO caught between the desire to realize BYOD's stated benefits of increased productivity and reduced cost and the necessity to secure all company IT, the

Center for Internet Studies' Critical Security Controls offer a helpful framework. While this paper focused primarily on using MDM as a means for implementing secure configurations for CSC 3, in reality, the hybrid MDM solution also satisfies parts of several other controls (Center for Internet Security, 2016).

Finally, this paper chose to use a Windows 10 laptop as a notional target for MDM. While laptops are sometimes not taken into consideration when people consider BYOD, this oversight should be addressed, as laptops have yet to be rendered totally obsolete by the tablet form factor. Hybrid MDM using SCCM in conjunction with Microsoft Intune is capable of supporting Windows 10 computers, which will become more prevalent in the enterprise environment, even if the laptop fades from the scene as a mobile business computing device.

References

Alcatel-Lucent Motive Security Labs. (2015). *Motive Security Labs Malware Report - H2 2014.* Boulogne-Billancourt: Alcatel-Lucent.

AppTec GMBH. (2017). *Prices - AppTec360*. Retrieved July 22, 2017, from AppTec Web site: https://www.apptec360.com/prices/

B2Bwhiteboard (Director). (2013). *Mobile Device Management (MDM) - Explained* [Motion Picture]. YouTube. Retrieved July 22, 2017, from https://www.youtube.com/watch?v=5SiEJAWUe28

Brooks, C. (2013, May 22). *What is BYOD (Bring Your Own Device)?* Retrieved July 15, 2017, from Business News Daily: http://www.businessnewsdaily.com/4526-byod-bring-your-own-device.html

Center for Internet Security. (2016). *Critical Security Controls for Effective Cyber Defense: Consensus Audit Guidelines* (6.0 ed.). East Greenbush, New York: Center for Internet Security.

Center for Internet Security. (2017). *CIS Microsoft Windows 10 Enterprise (Release 1511) Benchmark* (v.1.1.1 ed.). East Greenbush, New York, United States of America: Center for Internet Security.

Center for Internet Security. (2017, July 13). *CIS SecureSuite Membership Pricing and Categories - End User*. Retrieved July 30, 2017, from Center for Internet Security Web site: https://www.cisecurity.org/cis-securesuite/pricing-and-categories/end-user/

Cisco IBSG. (2012). *BYOD: A Global Perspective - Harnessing Employee-Led Innovation.* San Jose: Cisco Internet Business Solutions Group.

Davis, J. (2016, March 3). *5 Technology Challenges Faced by Adult Learners*. Retrieved July 15, 2017, from eLearning Industry: https://elearningindustry.com/5-technology-challenges-faced-adult-learners

Defense Information Systems Agency. (2016, April 5). NOTE - Secure Host Baseline (SHB) OS Image Available . Fort George G. Meade, Maryland, USA. Retrieved July 30, 2017, from https://iase.disa.mil/stigs/compilations/Pages/index.aspx

Desktop Windows Versions Market Share Worldwide June 2016 to June 2017. (2017, July 9). Retrieved from Stat Counter Global Stats: http://gs.statcounter.com/os-version-market-share/windows/desktop/worldwide

DoD Coalition of Apple Engineers. (2017, July). *What are SRGs and STIGs?* Retrieved July 30, 2017, from DoD Coalition of Apple Engineers (CAE): http://dodcae.osd.mil/content/what-are-srgs-and-stigs

Forrest, C. (2017, July 12). *Why Windows Phone users are now a serious security risk to their employers*. Retrieved July 12, 2017, from Tech Republic: http://www.techrepublic.com/article/why-windows-phone-users-are-now-a-serious-security-risk-to-their-employers/

Hess, K. (2014, June 13). *5 Mobile Application Management Features That Matter*. Retrieved July 22, 2017, from tomsitpro.com: http://www.tomsitpro.com/articles/mam-solutions-comparison,2-753.html

Lindner, J. (2016, November 14). *Enterprise Mobility Management (EMM) 101*. Retrieved July 18, 2017, from tomsitpro.com: http://www.tomsitpro.com/articles/enterprise-mobility-management-emm-101,2-1033.html

Lorenc, K. (2016, May 26). *Enterprise Mobility Management: Trends And Solutions*. Retrieved July 22, 2017, from tomsitpro.com: http://www.tomsitpro.com/articles/enterprise-mobility-management-solutions,1-1911.html

Maddox, T. (2015, January 5). *Research: 74 Percent Using or Adopting BYOD*. Retrieved from ZDNet: http://www.zdnet.com/article/research-74-percent-using-or-adopting-byod/

Margosis, A. (2016, October 17). *Security baseline for Windows 10 v1607 ("Anniversary edition") and Windows Server 2016.* Retrieved April 19, 2017, from Microsoft Security Guidance blog: https://blogs.technet.microsoft.com/secguide/2016/10/17/security-baseline-for-windows-10-v1607-anniversary-edition-and-windows-server-2016/

Microsoft. (2017, May). *Windows Lifecycle Fact Sheet*. Retrieved July 9, 2017, from Microsoft Support: https://support.microsoft.com/en-us/help/13853/windows-lifecycle-fact-sheet

Microsoft, Incorporated. (2011, April 27). *Group Policy for Beginners.* Retrieved July 29, 2017, from Microsoft Technet: https://technet.microsoft.com/en-us/library/hh147307(d=printer,v=ws.10).aspx

Microsoft, Incorporated. (2017, July). *Enterprise Mobility + Security Pricing Options*. Retrieved July 26, 2017, from Microsoft Web site: https://www.microsoft.com/en-us/cloud-platform/enterprise-mobility-security-pricing

Microsoft, Incorporated. (2017, June 19). *Hybrid mobile device management (MDM) with System Center Configuration Manager and Microsoft Intune.* Retrieved July 31, 2017, from Microsoft Docs: https://docs.microsoft.com/en-us/sccm/mdm/understand/hybrid-mobile-device-management

Microsoft, Incorporated. (2017). *Manage BYOD and corporate-owned devices with MDM solutions*. Retrieved July 19, 2017, from Microsoft Web site: https://www.microsoft.com/en-us/cloud-platform/mobile-device-management

Microsoft, Incorporated. (2017, February 14). *Prepare Windows Servers to support System Center Configuration Manager*. Retrieved July 31, 2017, from Microsoft Web site: https://docs.microsoft.com/en-us/sccm/core/plan-design/network/prepare-windows-servers

Microsoft, Incorporated. (2017, April 5). *Protect your enterprise data using Windows Information Protection (WIP).* Retrieved August 27, 2017, from Microsoft Docs: https://docs.microsoft.com/en-us/windows/threat-protection/windows-information-protection/protect-enterprise-data-using-wip

Microsoft, Incorporated. (2017, April 5). *The Windows Defender Security Center*. Retrieved August 27, 2017, from Microsoft Docs: https://docs.microsoft.com/en-us/windows/threat-protection/windows-defender-security-center/windows-defender-security-center

Microsoft, Incorporated. (2017, May 4). *What is Intune?* Retrieved July 26, 2017, from Microsoft Docs: https://docs.microsoft.com/en-us/intune/introduction-intune

Narayanan, S. (2017, April 29). *Gartner Revises Windows 10 Adoption Rates for Businesses from 50% to 85% in 2017*. Retrieved July 9, 2017, from 1reddrop.com: https://1reddrop.com/2017/04/29/gartner-revises-windows-10-adoption-rates-businesses-85-percent-from-earlier-50-percent-2017/

National Institute of Standards and Technology. (2017, May 9). *The United States Government Configuration Baseline (USGCB) - Windows 7 Content.* Retrieved July 30, 2017, from The United States Government Configuration Baseline (USGCB): https://usgcb.nist.gov/usgcb/microsoft/download_win7.html

Pavón, P. (2013, September 1). *Risky Business: "Bring-Your-Own-Device" and Your Company*. Retrieved May 12, 2017, from Business Law Today: https://www.americanbar.org/publications/blt/2013/09/01_pavon.html

Pinney, G. (2017, May 12). Interview with George Pinney. (C. Jarko, Interviewer)

Rouse, M. (2016, June). *Definition: Mobile Application Management (MAM)*. Retrieved July 26, 2017, from TechTarget Web site: http://searchmobilecomputing.techtarget.com/definition/mobile-application-management-MAM

Satia, G. (2013, December 2). *Familiarity in User Experience*. Retrieved July 15, 2017, from InfinVision Web site: http://infinvision.com/familiarity-in-user-experience/

Shinder, D. (2011, December 7). *Securing Your Network in an Era of Heterogeneity*. Retrieved July 15, 2017, from TechGenix Web site: http://techgenix.com/securing-network-era-heterogeneity/

Spiceworks. (2017, April 3). *Windows 10 Adoption Surges, Yet Businesses Still Hang On to Windows XP and Vista*. Retrieved from Spiceworks Community: https://community.spiceworks.com/networking/articles/2628-windows-10-adoption-surges-yet-businesses-still-hang-on-to-windows-xp-and-vista

Tarala, J. (Composer). (2016). SANS SEC566.1 - Background and Philosophy of the Critical Security Controls. [J. Tarala, Performer]

Tarala, J.; Enclave Security. (2016, 4th Quarter). 566.1 - Implementing & Auditing the Critical Security Controls - In Depth - Book 1. *SANS SEC566 - Implementing & Auditing the Critical Security Controls - In Depth*. Bethesda, Maryland: The SANS Institute.

Trend Micro Incorporated. (2012, January 31). *The Dark Side of BYOD – Privacy, Personal Data Loss and Device Seizure*. Retrieved July 16, 2017, from Trend Micro Blog Web site: http://blog.trendmicro.com/consumerization-byod-privacy-personal-data-loss-and-device-seizure/

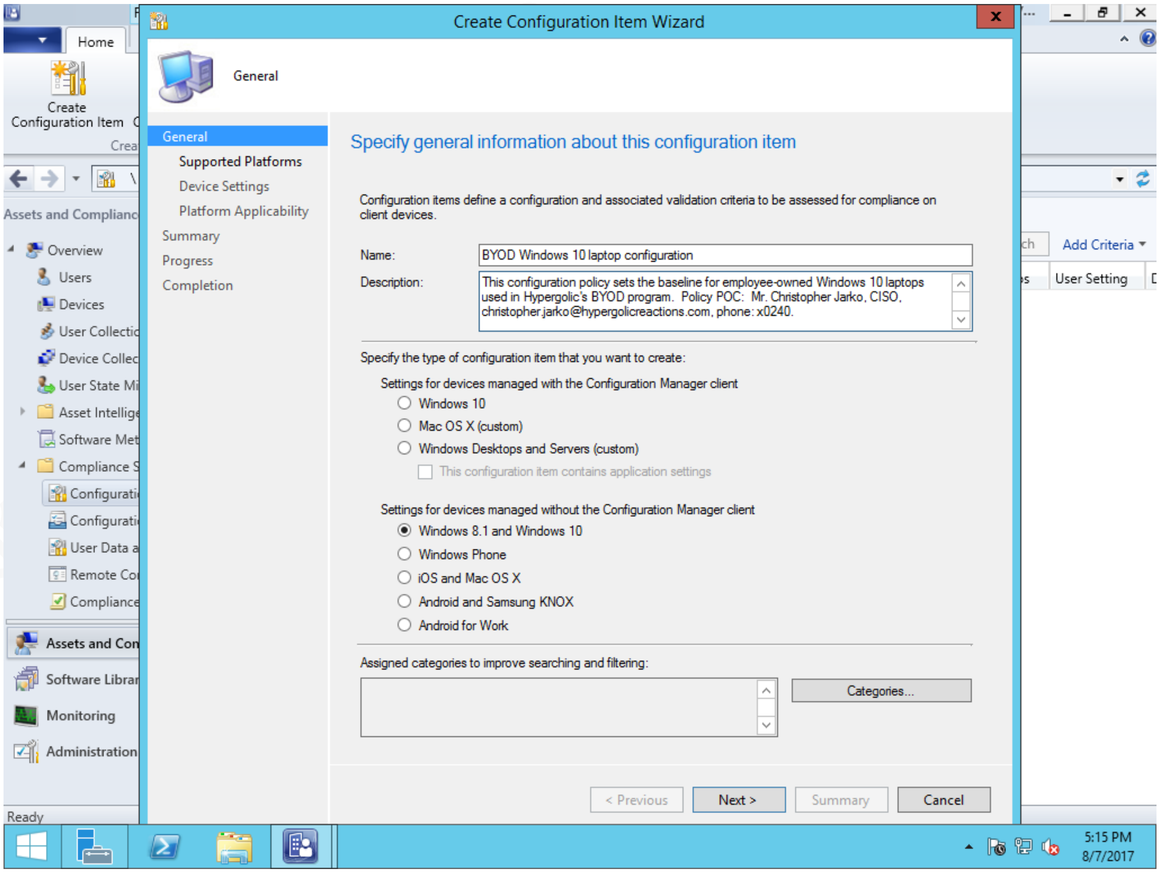
Zoho Corporation. (2017, July). *Desktop Central Edition Comparison Matrix.* Retrieved July 22, 2017, from Manage Engine Web site: https://www.manageengine.com/products/desktop-central/edition-comparison-matrix.html

Zoho Corporation. (2017, July). *Desktop Central Store*. Retrieved July 29, 2017, from Manage Engine Web site: https://store.manageengine.com/desktop-central/#tabs

Appendix
Create Configuration Item Wizard – System Center Configuration Manager (SCCM)

Part 1: Screenshots

The following screenshots were taken while running the Create Configuration Item Wizard in SCCM with the intent of creating a configuration item for Windows 10 laptops as part of a notional BYOD deployment test.



Specify general information about this configuration item

Configuration items define a configuration and associated validation criteria to be assessed for compliance on client devices.

Name: BYOD Windows 10 laptop configuration

Description: This configuration policy sets the baseline for employee-owned Windows 10 laptops used in Hypergolic's BYOD program. Policy POC: Mr. Christopher Jarko, CISO, christopher.jarko@hypergolicreactions.com, phone: x0240.

Specify the type of configuration item that you want to create:

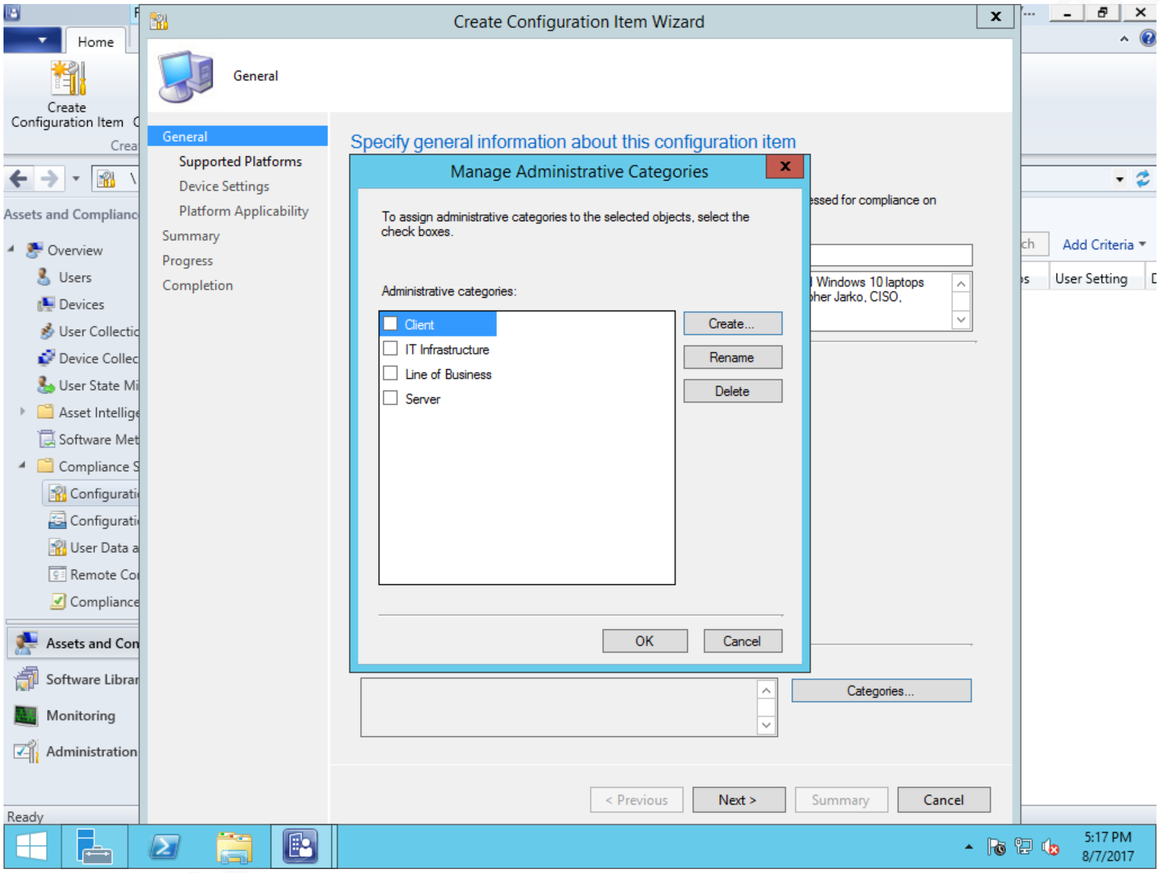
Settings for devices managed with the Configuration Manager client
- ○ Windows 10
- ○ Mac OS X (custom)
- ○ Windows Desktops and Servers (custom)
  - □ This configuration item contains application settings

Settings for devices managed without the Configuration Manager client
- ● Windows 8.1 and Windows 10
- ○ Windows Phone
- ○ iOS and Mac OS X
- ○ Android and Samsung KNOX
- ○ Android for Work

Assigned categories to improve searching and filtering:

Categories...

Figure 1: Opening the Wizard



Specify general information about this configuration item

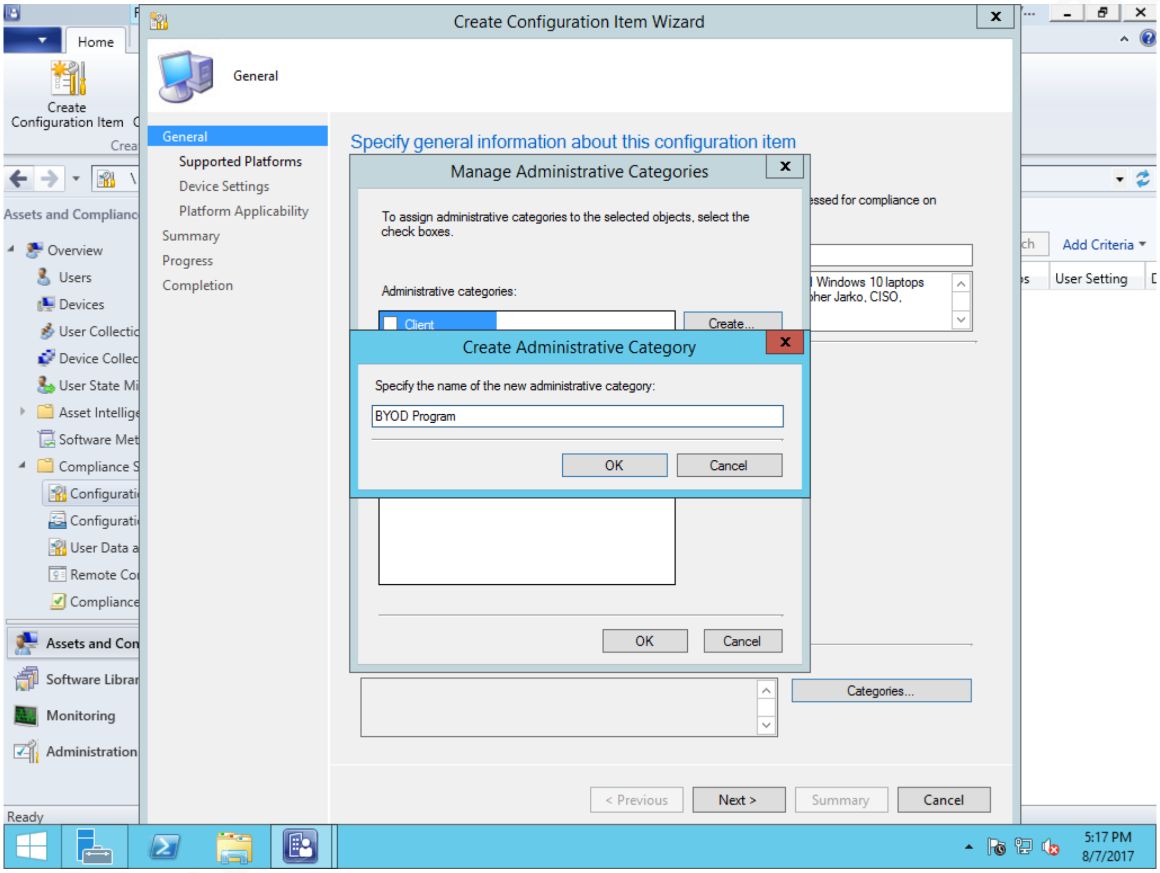
Manage Administrative Categories

To assign administrative categories to the selected objects, select the check boxes.

Administrative categories:

- □ Client
- □ IT Infrastructure
- □ Line of Business
- □ Server

Figure 2: Category selection; “BYOD” was not an option



Specify general information about this configuration item

Manage Administrative Categories

To assign administrative categories to the selected objects, select the check boxes.

Administrative categories:

□ Client

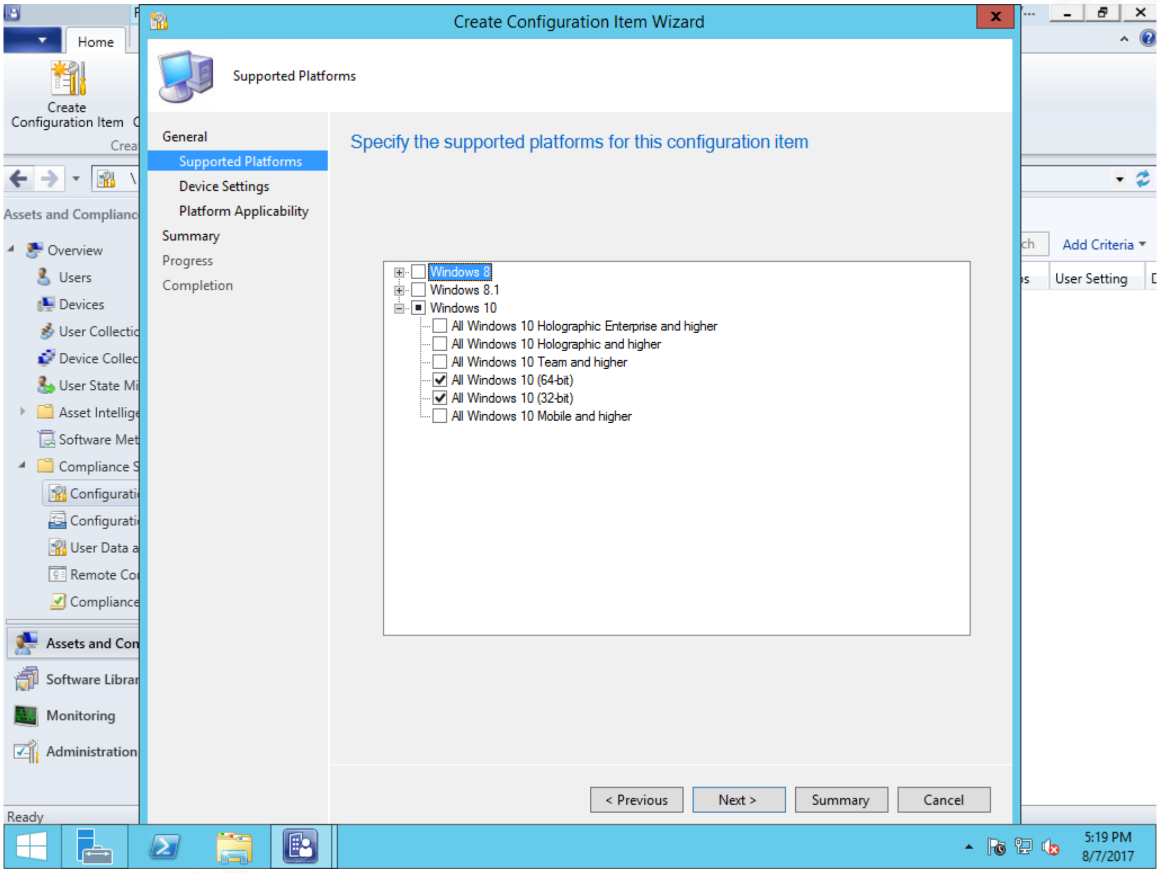
Create Administrative Category

Specify the name of the new administrative category:

BYOD Program

OK Cancel

Figure 3: Creating a new category for the BYOD Program



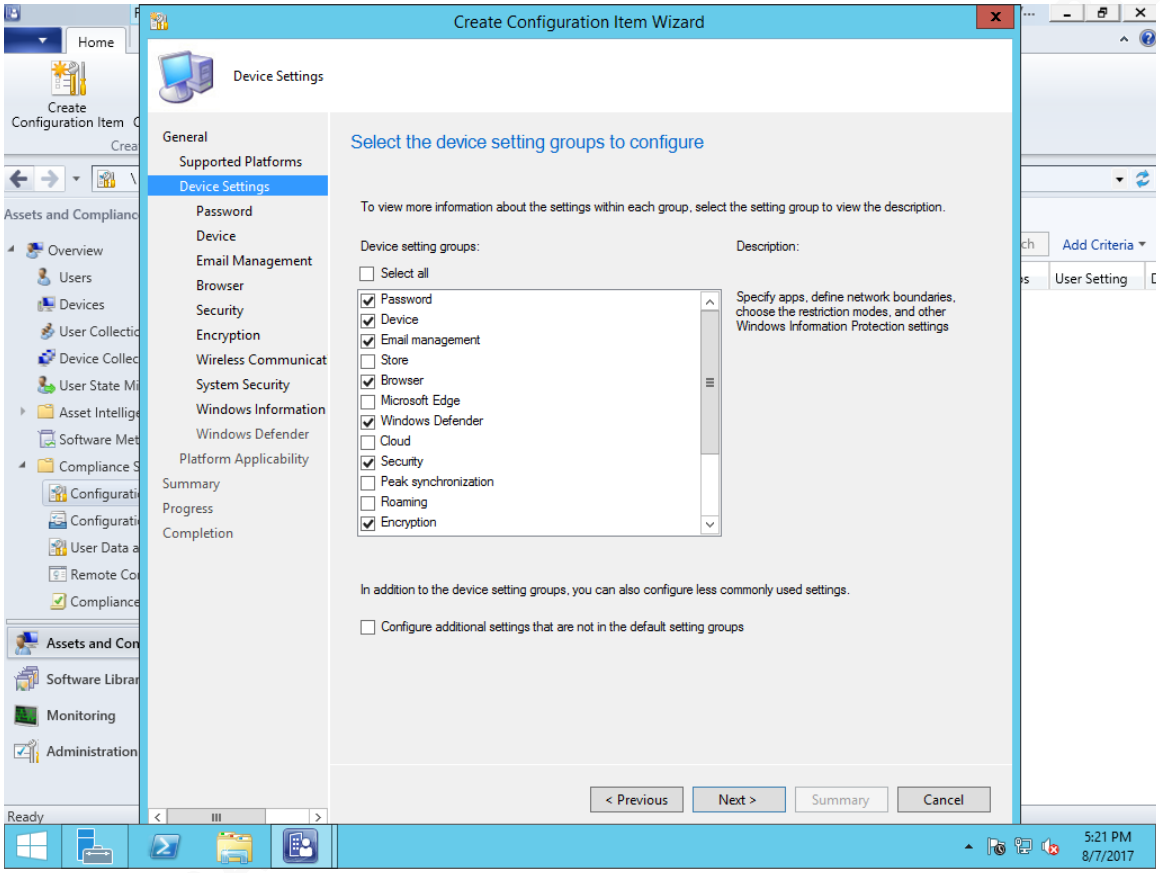
Create Configuration Item Wizard

Supported Platforms

Specify the supported platforms for this configuration item

- ☐ Windows 8
- ☐ Windows 8.1
- ■ Windows 10
  - ☐ All Windows 10 Holographic Enterprise and higher
  - ☐ All Windows 10 Holographic and higher
  - ☐ All Windows 10 Team and higher
  - ☑ All Windows 10 (64-bit)
  - ☑ All Windows 10 (32-bit)
  - ☐ All Windows 10 Mobile and higher

Figure 4: Selecting applicable target platforms



Select the device setting groups to configure

To view more information about the settings within each group, select the setting group to view the description.

Device setting groups:

□ Select all

☑ Password
☑ Device
☑ Email management
□ Store
☑ Browser
□ Microsoft Edge
☑ Windows Defender
□ Cloud
☑ Security
□ Peak synchronization
□ Roaming
☑ Encryption

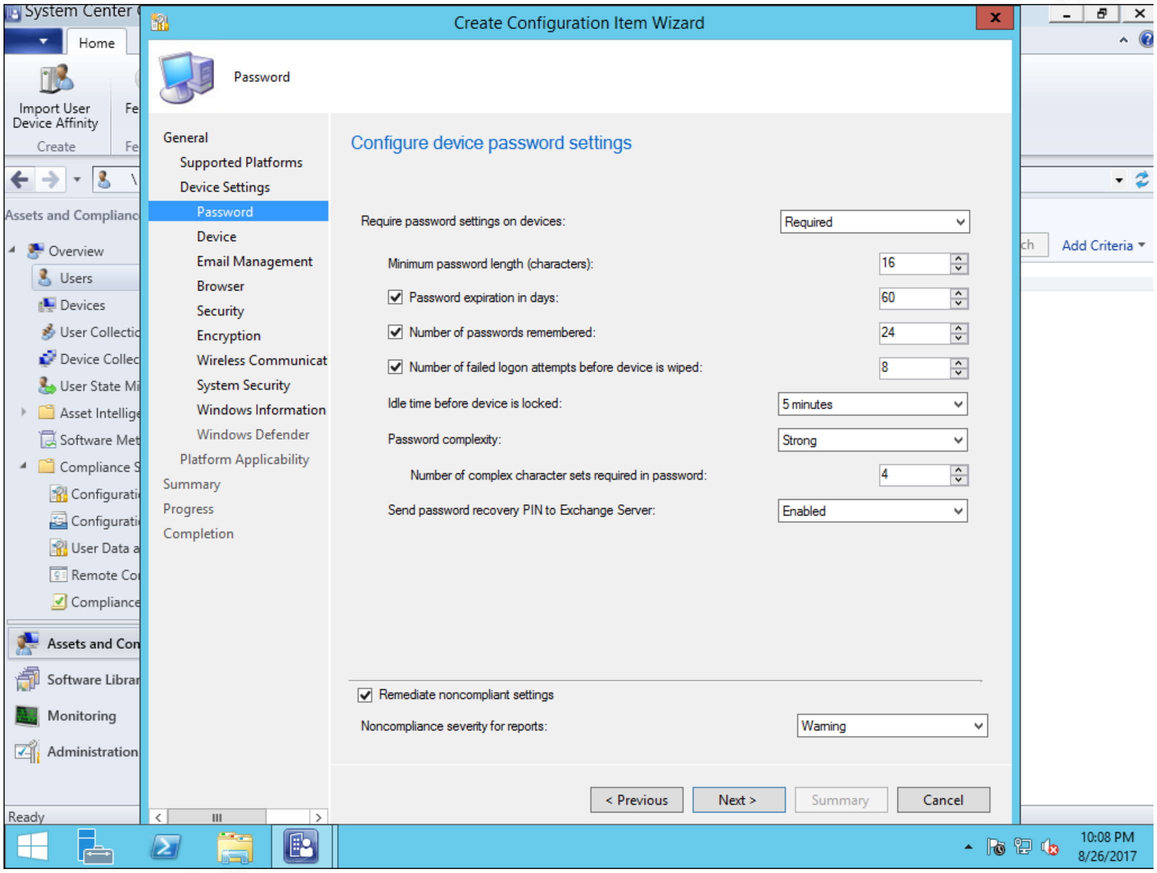
Description:

Specify apps, define network boundaries, choose the restriction modes, and other Windows Information Protection settings

In addition to the device setting groups, you can also configure less commonly used settings.

□ Configure additional settings that are not in the default setting groups

Figure 5: Device setting group selection



Configure device password settings

Require password settings on devices: Required

Minimum password length (characters): 16

☑ Password expiration in days: 60

☑ Number of passwords remembered: 24

☑ Number of failed logon attempts before device is wiped: 8

Idle time before device is locked: 5 minutes

Password complexity: Strong

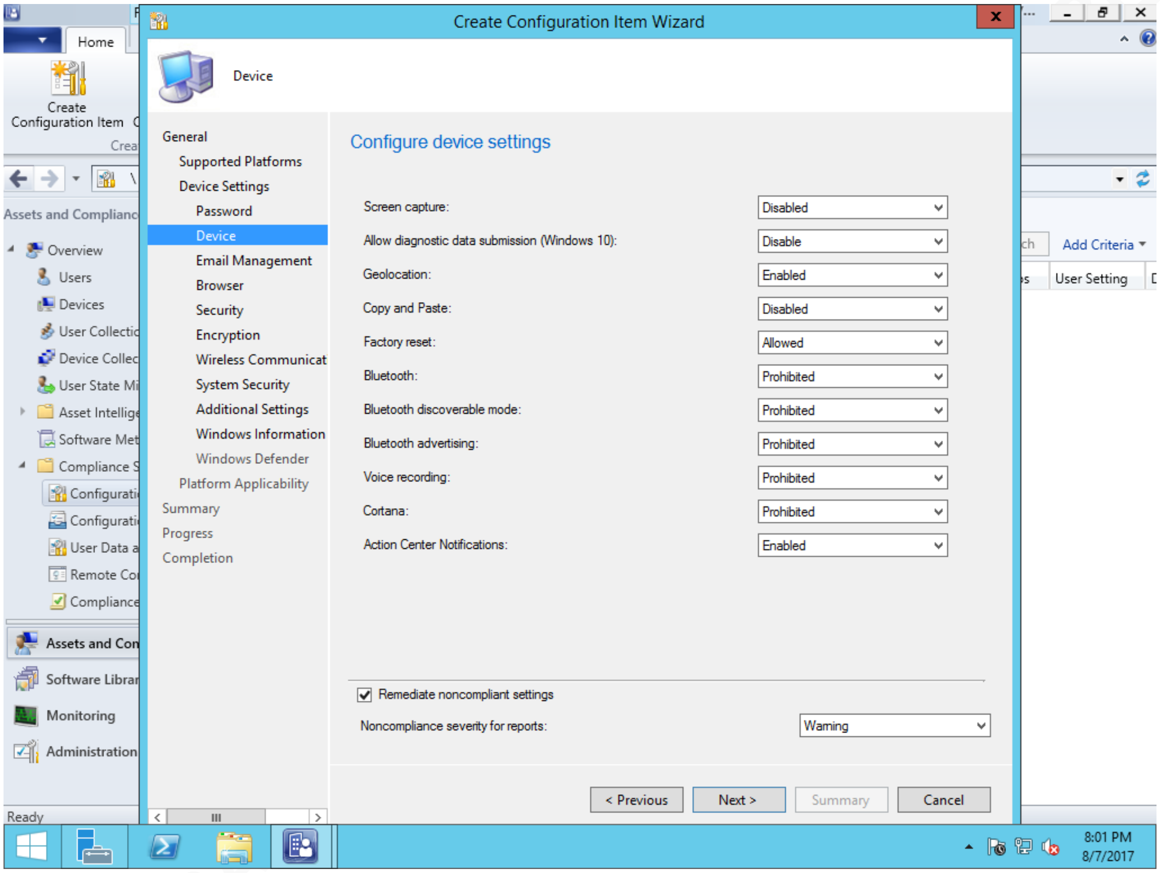
Number of complex character sets required in password: 4

Send password recovery PIN to Exchange Server: Enabled

☑ Remediate noncompliant settings

Noncompliance severity for reports: Warning

Figure 6: Password settings



Configure device settings

Screen capture: Disabled

Allow diagnostic data submission (Windows 10): Disable

Geolocation: Enabled

Copy and Paste: Disabled

Factory reset: Allowed

Bluetooth: Prohibited

Bluetooth discoverable mode: Prohibited

Bluetooth advertising: Prohibited

Voice recording: Prohibited

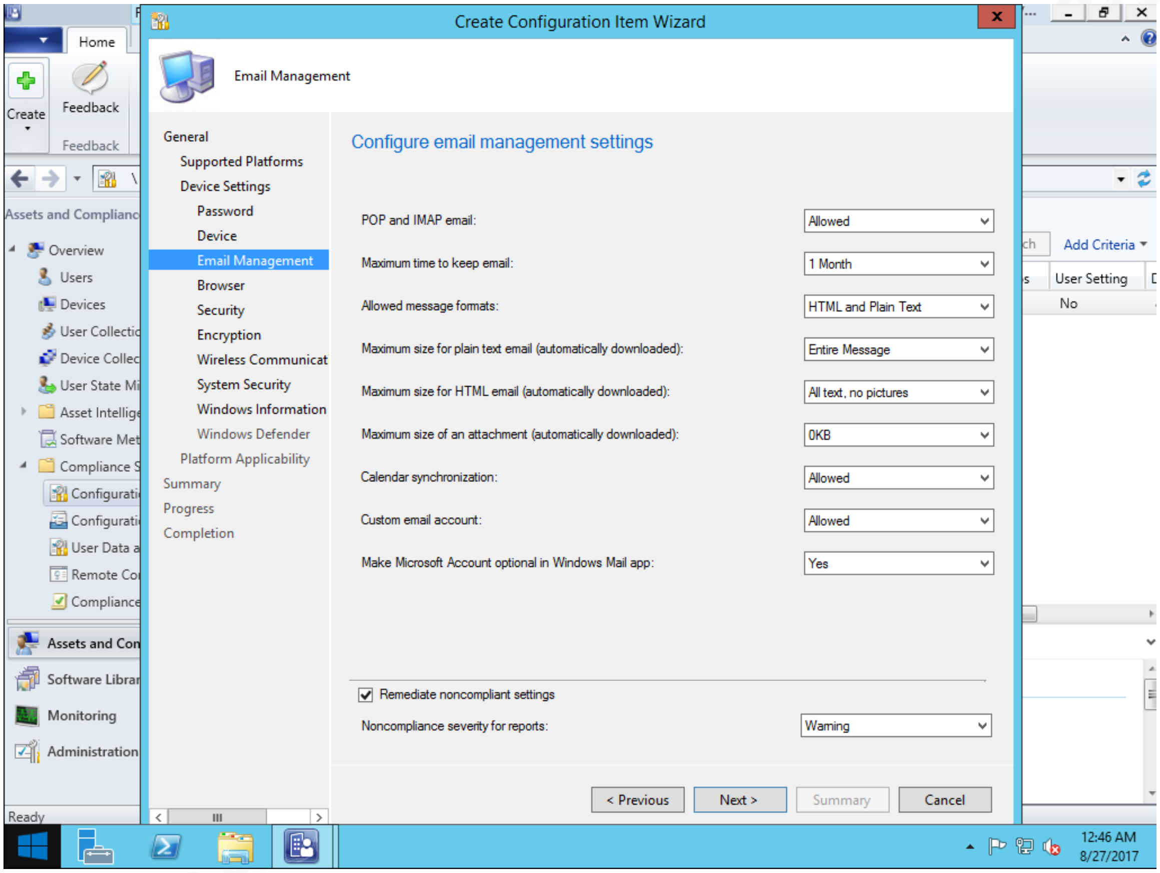
Cortana: Prohibited

Action Center Notifications: Enabled

☑ Remediate noncompliant settings

Noncompliance severity for reports: Warning

Figure 7: Device settings



Email Management

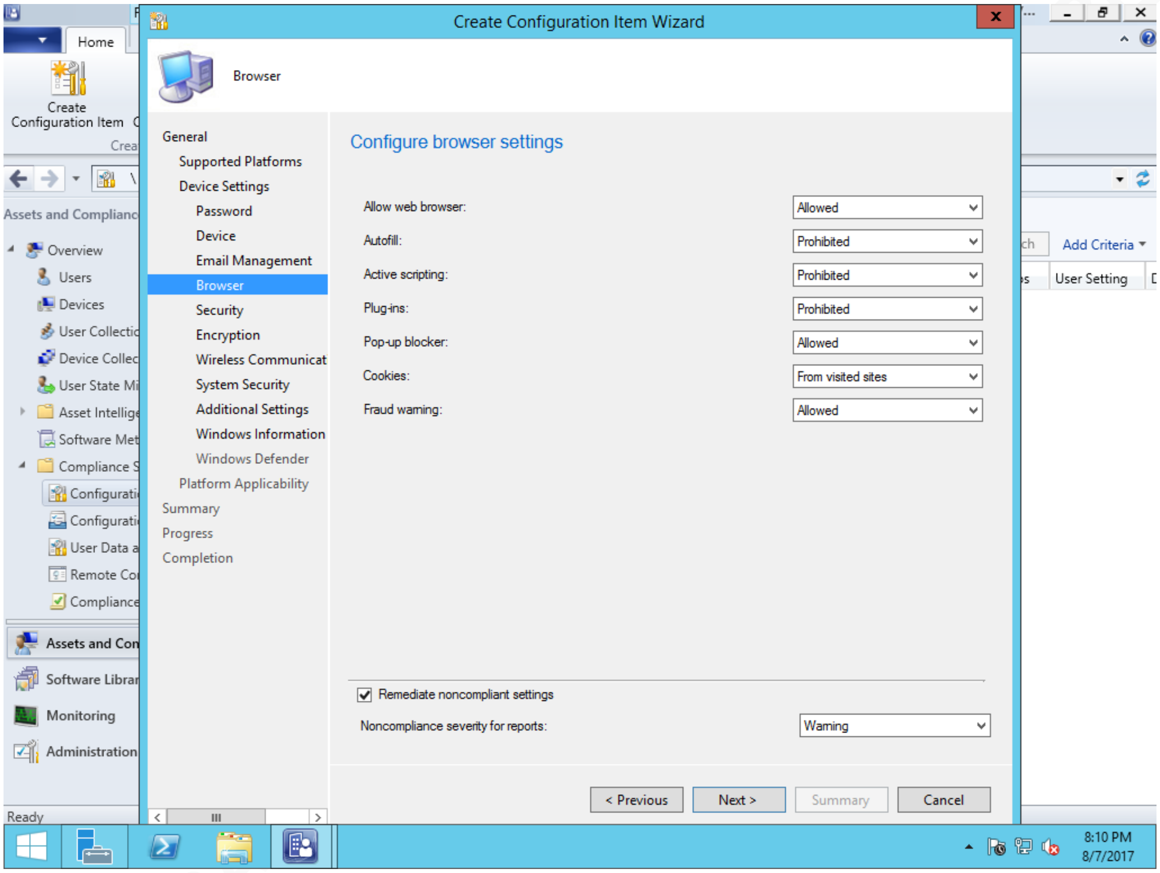
Configure email management settings

POP and IMAP email:	Allowed
Maximum time to keep email:	1 Month
Allowed message formats:	HTML and Plain Text
Maximum size for plain text email (automatically downloaded):	Entire Message
Maximum size for HTML email (automatically downloaded):	All text, no pictures
Maximum size of an attachment (automatically downloaded):	0KB
Calendar synchronization:	Allowed
Custom email account:	Allowed
Make Microsoft Account optional in Windows Mail app:	Yes

☑ Remediate noncompliant settings

Noncompliance severity for reports: Warning

Figure 8: Email settings



Configure browser settings

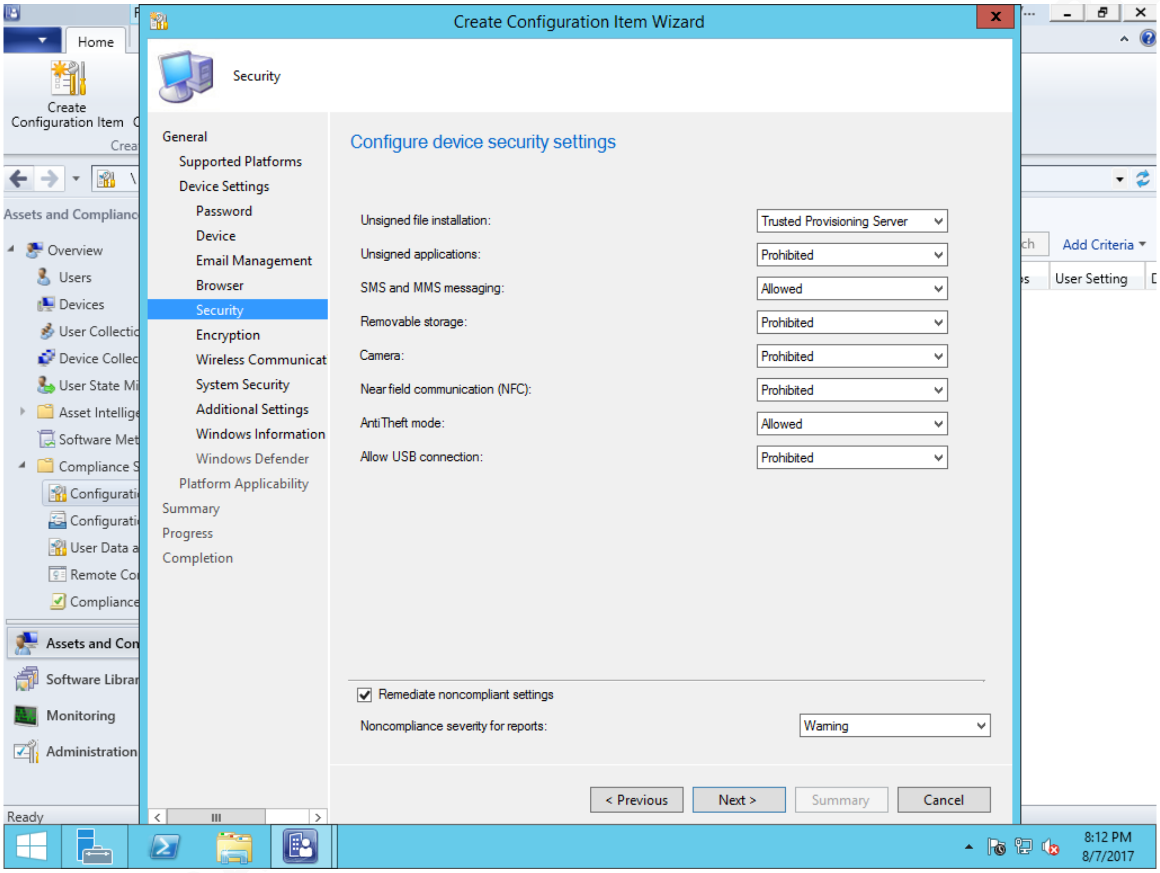
Allow web browser:	Allowed
Autofill:	Prohibited
Active scripting:	Prohibited
Plug-ins:	Prohibited
Pop-up blocker:	Allowed
Cookies:	From visited sites
Fraud warning:	Allowed

☑ Remediate noncompliant settings

Noncompliance severity for reports: Warning

Figure 9: Browser settings (Microsoft Edge is configured separately)

Christopher Jarko, csjarko@yahoo.com



Configure device security settings

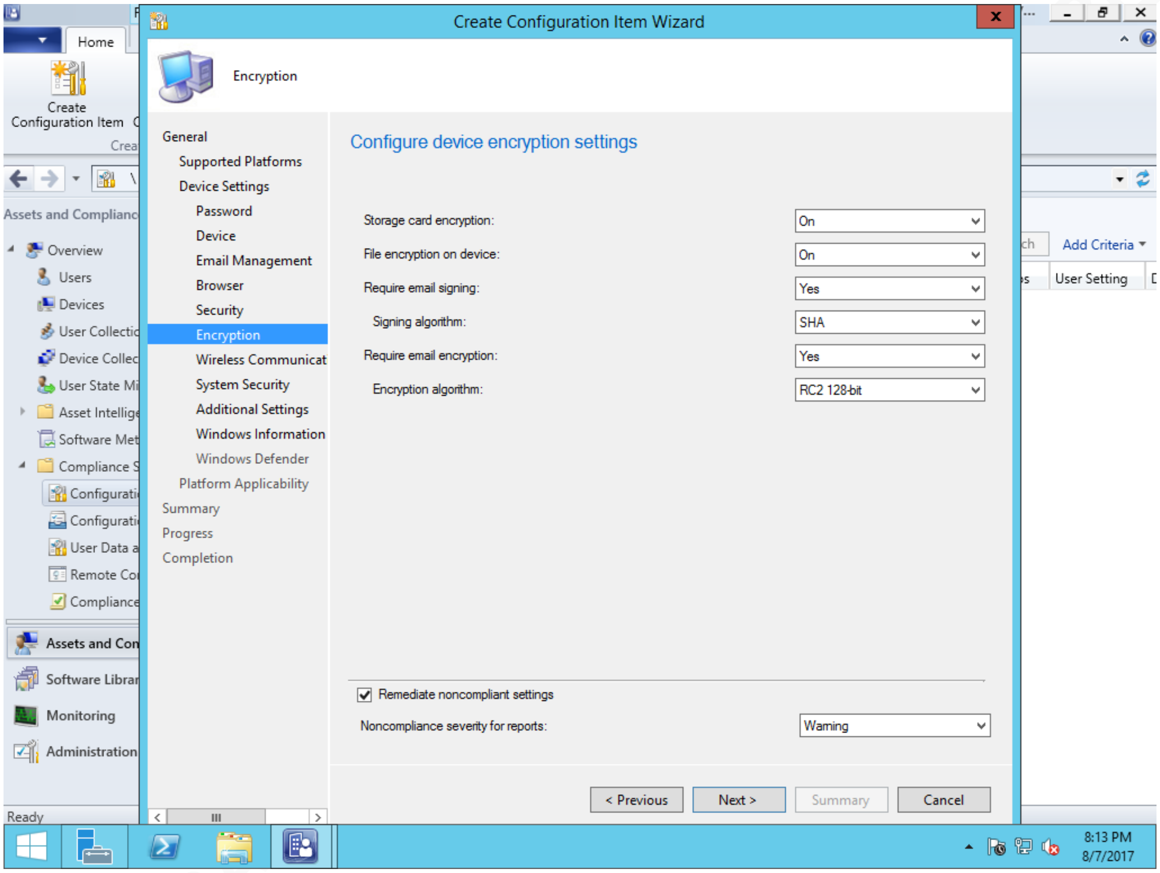
Unsigned file installation:	Trusted Provisioning Server
Unsigned applications:	Prohibited
SMS and MMS messaging:	Allowed
Removable storage:	Prohibited
Camera:	Prohibited
Near field communication (NFC):	Prohibited
AntiTheft mode:	Allowed
Allow USB connection:	Prohibited

☑ Remediate noncompliant settings

Noncompliance severity for reports: Warning

Figure 10: Device security settings

Christopher Jarko, csjarko@yahoo.com



Create Configuration Item Wizard

Encryption

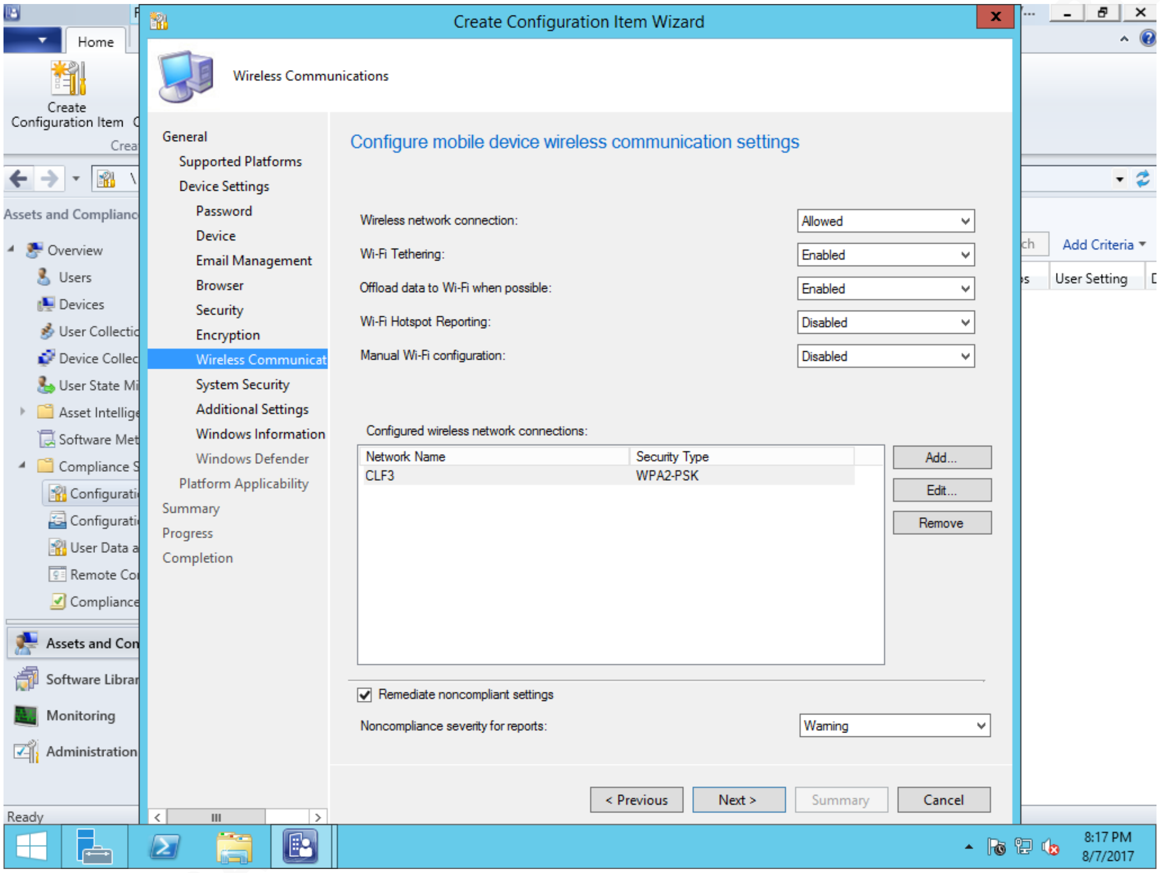
Configure device encryption settings

Storage card encryption:	On
File encryption on device:	On
Require email signing:	Yes
Signing algorithm:	SHA
Require email encryption:	Yes
Encryption algorithm:	RC2 128-bit

☑ Remediate noncompliant settings

Noncompliance severity for reports: Warning

Figure 11: Device encryption



Configure mobile device wireless communication settings

Wireless network connection: Allowed

Wi-Fi Tethering: Enabled

Offload data to Wi-Fi when possible: Enabled

Wi-Fi Hotspot Reporting: Disabled

Manual Wi-Fi configuration: Disabled

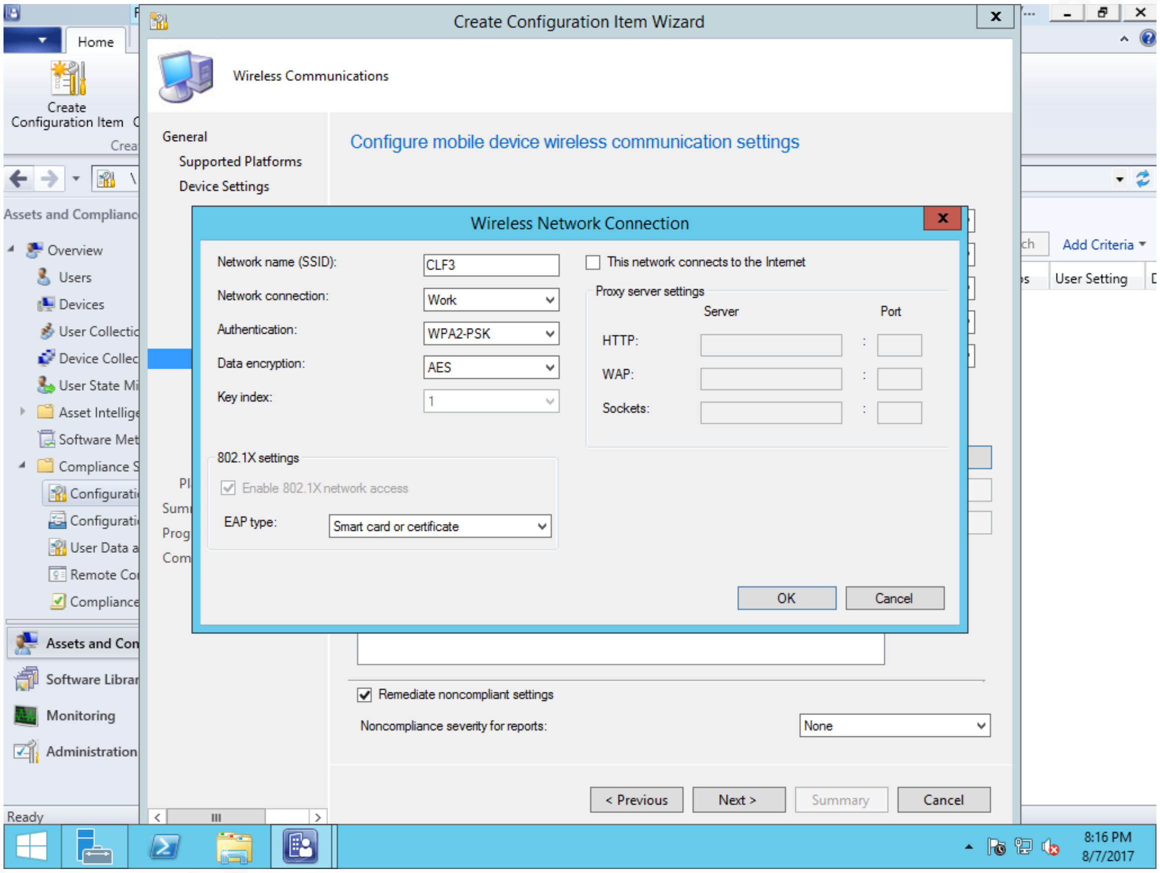
Configured wireless network connections:

Network Name	Security Type
CLF3	WPA2-PSK

☑ Remediate noncompliant settings

Noncompliance severity for reports: Warning

Figure 12: Mobile wireless settings



Create Configuration Item Wizard

Wireless Communications

Configure mobile device wireless communication settings

Wireless Network Connection

Network name (SSID): CLF3

Network connection: Work

Authentication: WPA2-PSK

Data encryption: AES

Key index: 1

□ This network connects to the Internet

Proxy server settings

	Server	Port
HTTP:		
WAP:		
Sockets:		

802.1X settings

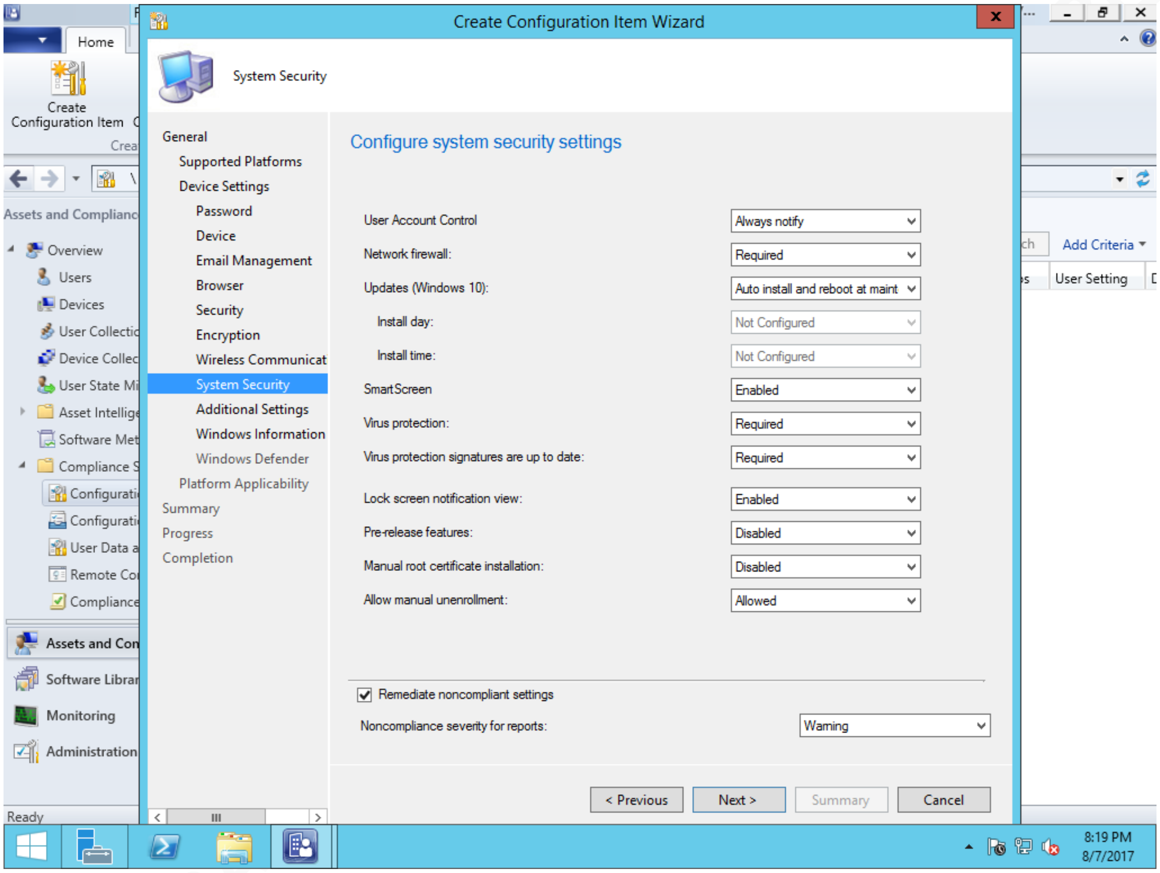
☑ Enable 802.1X network access

EAP type: Smart card or certificate

☑ Remediate noncompliant settings

Noncompliance severity for reports: None

Figure 13: Configuring the wireless connection for the previous setting



Configure system security settings

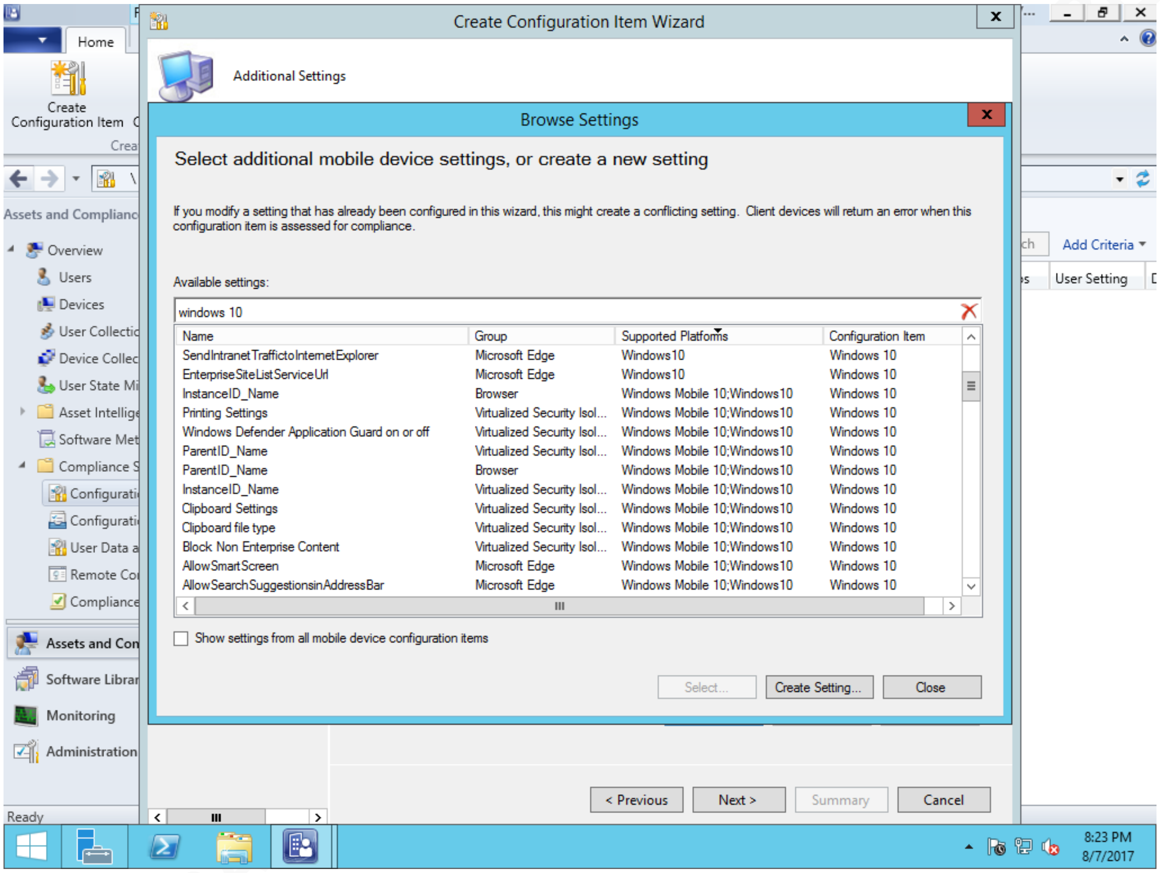
User Account Control	Always notify
Network firewall:	Required
Updates (Windows 10):	Auto install and reboot at maint
Install day:	Not Configured
Install time:	Not Configured
SmartScreen	Enabled
Virus protection:	Required
Virus protection signatures are up to date:	Required
Lock screen notification view:	Enabled
Pre-release features:	Disabled
Manual root certificate installation:	Disabled
Allow manual unenrollment:	Allowed

☑ Remediate noncompliant settings

Noncompliance severity for reports: Warning

Figure 14: System security settings

Christopher Jarko, csjarko@yahoo.com



Create Configuration Item Wizard

Additional Settings

Browse Settings

Select additional mobile device settings, or create a new setting

If you modify a setting that has already been configured in this wizard, this might create a conflicting setting. Client devices will return an error when this configuration item is assessed for compliance.

Available settings:

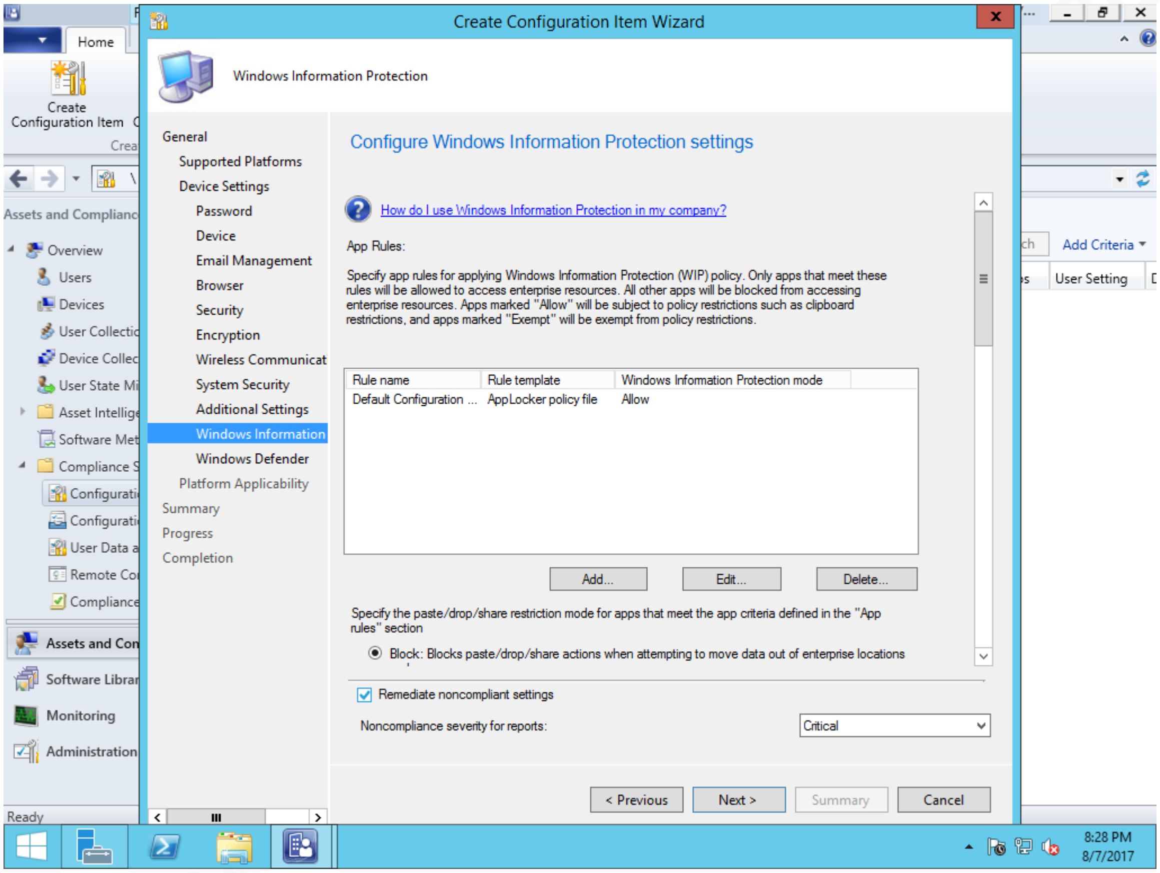
windows 10

Name	Group	Supported Platforms	Configuration Item
SendIntranetTraffictoInternetExplorer	Microsoft Edge	Windows10	Windows 10
EnterpriseSiteListServiceUrl	Microsoft Edge	Windows10	Windows 10
InstanceID_Name	Browser	Windows Mobile 10;Windows10	Windows 10
Printing Settings	Virtualized Security Isol...	Windows Mobile 10;Windows10	Windows 10
Windows Defender Application Guard on or off	Virtualized Security Isol...	Windows Mobile 10;Windows10	Windows 10
ParentID_Name	Virtualized Security Isol...	Windows Mobile 10;Windows10	Windows 10
ParentID_Name	Browser	Windows Mobile 10;Windows10	Windows 10
InstanceID_Name	Virtualized Security Isol...	Windows Mobile 10;Windows10	Windows 10
Clipboard Settings	Virtualized Security Isol...	Windows Mobile 10;Windows10	Windows 10
Clipboard file type	Virtualized Security Isol...	Windows Mobile 10;Windows10	Windows 10
Block Non Enterprise Content	Virtualized Security Isol...	Windows Mobile 10;Windows10	Windows 10
AllowSmartScreen	Microsoft Edge	Windows Mobile 10;Windows10	Windows 10
AllowSearchSuggestionsinAddressBar	Microsoft Edge	Windows Mobile 10;Windows10	Windows 10

□ Show settings from all mobile device configuration items

Select... | Create Setting... | Close

Figure 15: Creating a new setting (sorted by supported platform)



Configure Windows Information Protection settings

How do I use Windows Information Protection in my company?

App Rules:

Specify app rules for applying Windows Information Protection (WIP) policy. Only apps that meet these rules will be allowed to access enterprise resources. All other apps will be blocked from accessing enterprise resources. Apps marked "Allow" will be subject to policy restrictions such as clipboard restrictions, and apps marked "Exempt" will be exempt from policy restrictions.

Rule name	Rule template	Windows Information Protection mode
Default Configuration ...	AppLocker policy file	Allow

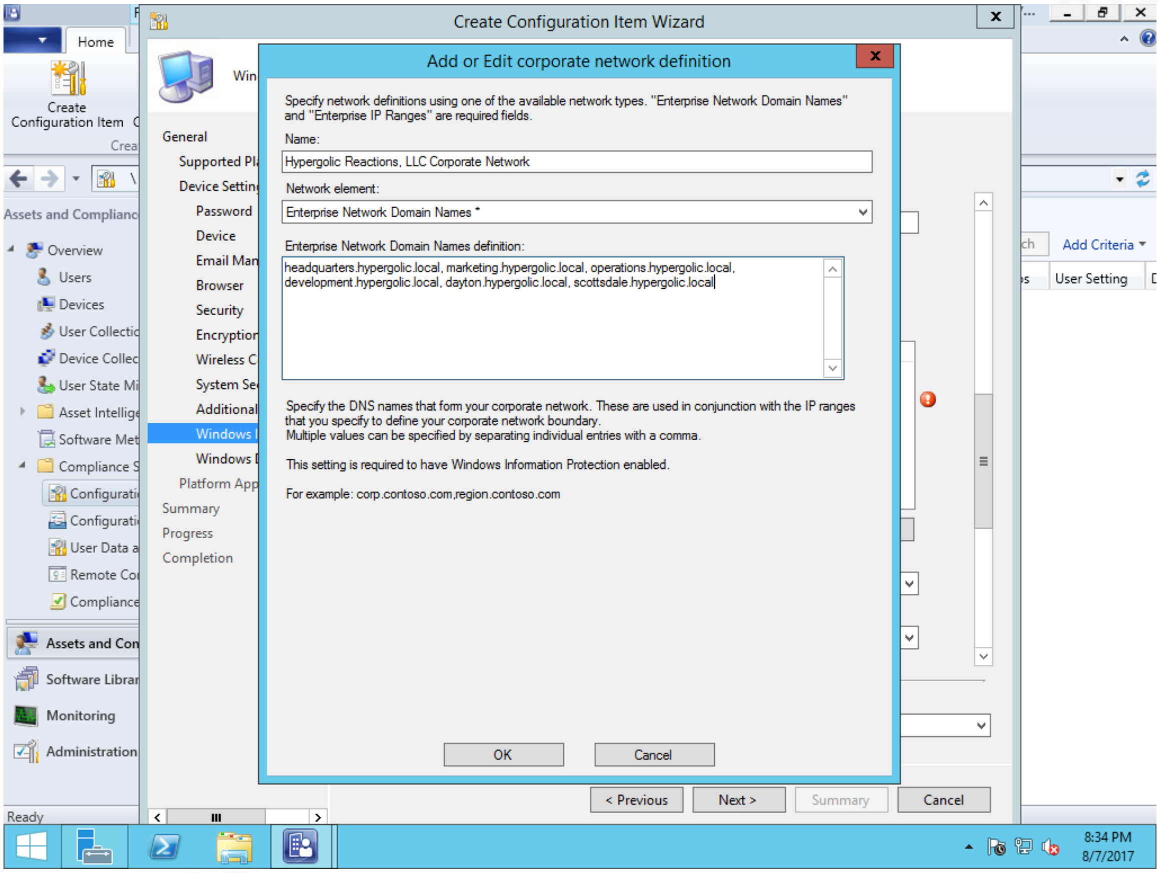
Specify the paste/drop/share restriction mode for apps that meet the app criteria defined in the "App rules" section

● Block: Blocks paste/drop/share actions when attempting to move data out of enterprise locations

☑ Remediate noncompliant settings

Noncompliance severity for reports: Critical

Figure 16: Windows Information Protection (WIP) settings



Add or Edit corporate network definition

Specify network definitions using one of the available network types. "Enterprise Network Domain Names" and "Enterprise IP Ranges" are required fields.

Name: Hypergolic Reactions, LLC Corporate Network

Network element: Enterprise Network Domain Names *

Enterprise Network Domain Names definition:

headquarters.hypergolic.local, marketing.hypergolic.local, operations.hypergolic.local, development.hypergolic.local, dayton.hypergolic.local, scottsdale.hypergolic.local

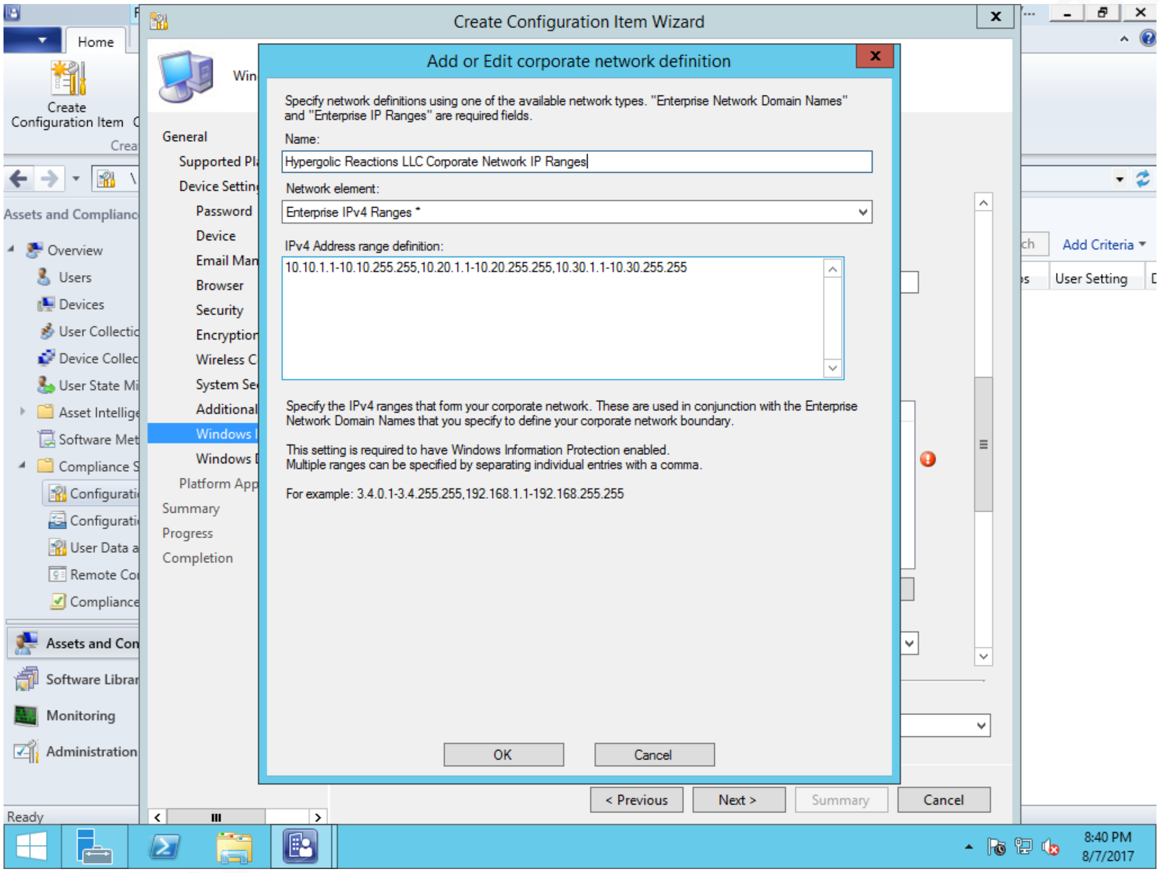
Specify the DNS names that form your corporate network. These are used in conjunction with the IP ranges that you specify to define your corporate network boundary.
Multiple values can be specified by separating individual entries with a comma.

This setting is required to have Windows Information Protection enabled.

For example: corp.contoso.com,region.contoso.com

OK Cancel

Figure 17: Defining the corporate network (domain names) for WIP



Add or Edit corporate network definition

Specify network definitions using one of the available network types. "Enterprise Network Domain Names" and "Enterprise IP Ranges" are required fields.

Name: Hypergolic Reactions LLC Corporate Network IP Ranges

Network element: Enterprise IPv4 Ranges *

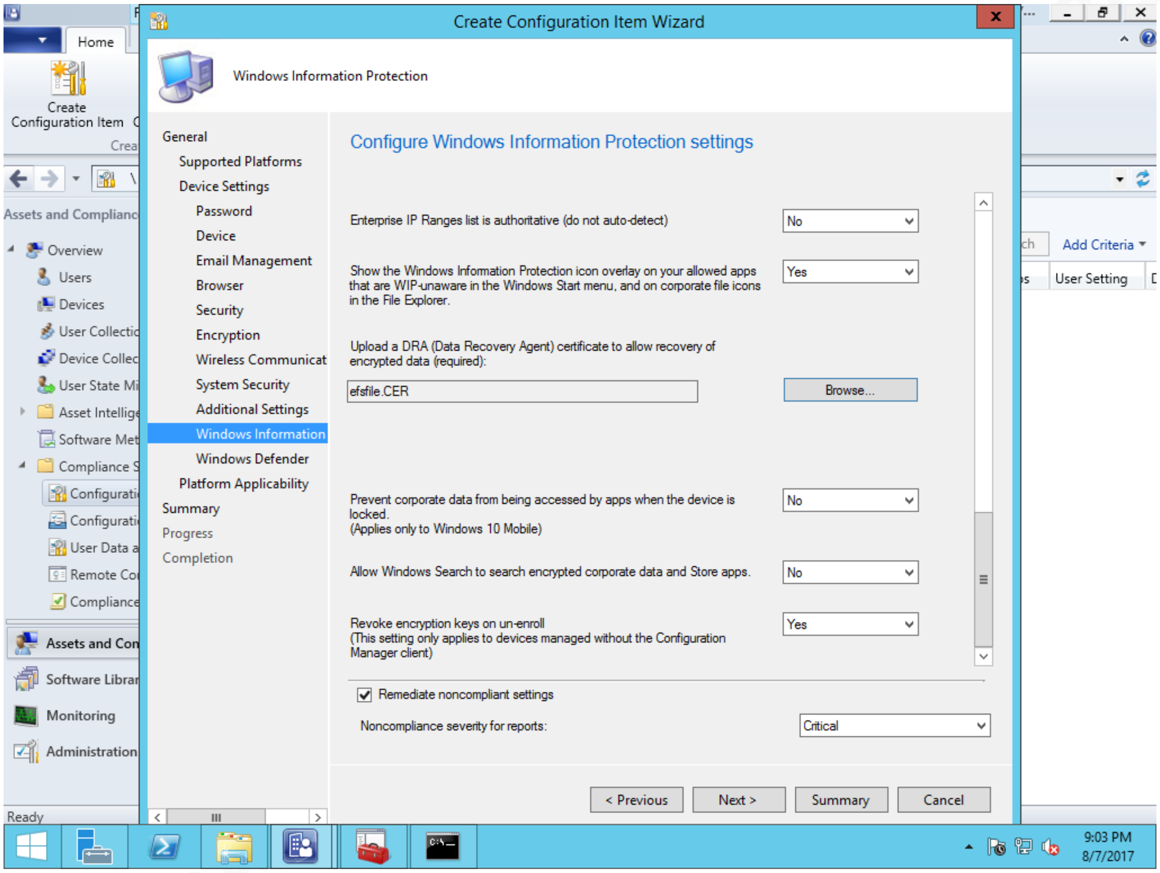
IPv4 Address range definition: 10.10.1.1-10.10.255.255,10.20.1.1-10.20.255.255,10.30.1.1-10.30.255.255

Specify the IPv4 ranges that form your corporate network. These are used in conjunction with the Enterprise Network Domain Names that you specify to define your corporate network boundary.

This setting is required to have Windows Information Protection enabled.
Multiple ranges can be specified by separating individual entries with a comma.

For example: 3.4.0.1-3.4.255.255,192.168.1.1-192.168.255.255

Figure 18: Defining the corporate network (IPv4 ranges) for WIP



Windows Information Protection

Configure Windows Information Protection settings

Enterprise IP Ranges list is authoritative (do not auto-detect): No

Show the Windows Information Protection icon overlay on your allowed apps that are WIP-unaware in the Windows Start menu, and on corporate file icons in the File Explorer.: Yes

Upload a DRA (Data Recovery Agent) certificate to allow recovery of encrypted data (required): efsfile.CER

Prevent corporate data from being accessed by apps when the device is locked. (Applies only to Windows 10 Mobile): No

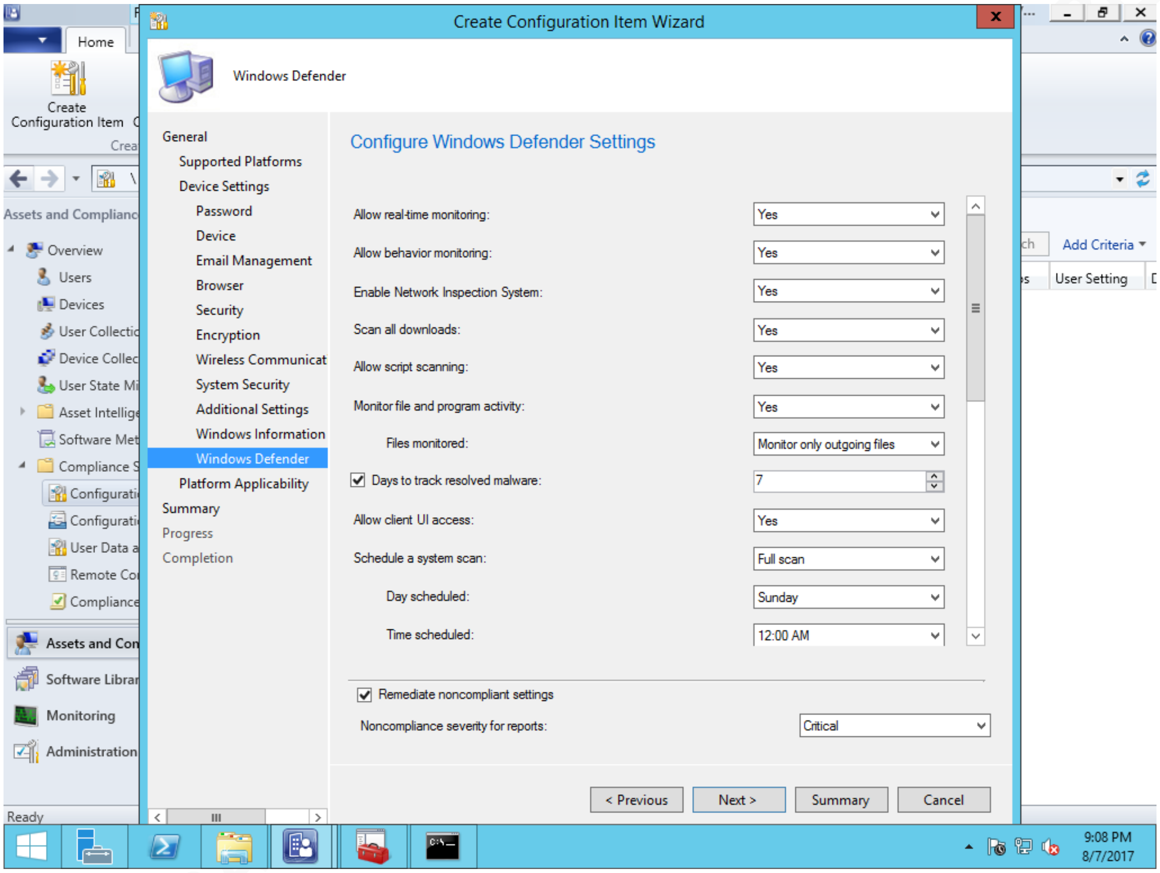
Allow Windows Search to search encrypted corporate data and Store apps.: No

Revoke encryption keys on un-enroll (This setting only applies to devices managed without the Configuration Manager client): Yes

☑ Remediate noncompliant settings

Noncompliance severity for reports: Critical

Figure 19: Specifying a Data Recovery Agent (DRA) certificate for recovery of encrypted data as part of WIP; also note ability to revoke encryption keys on device unenrollment



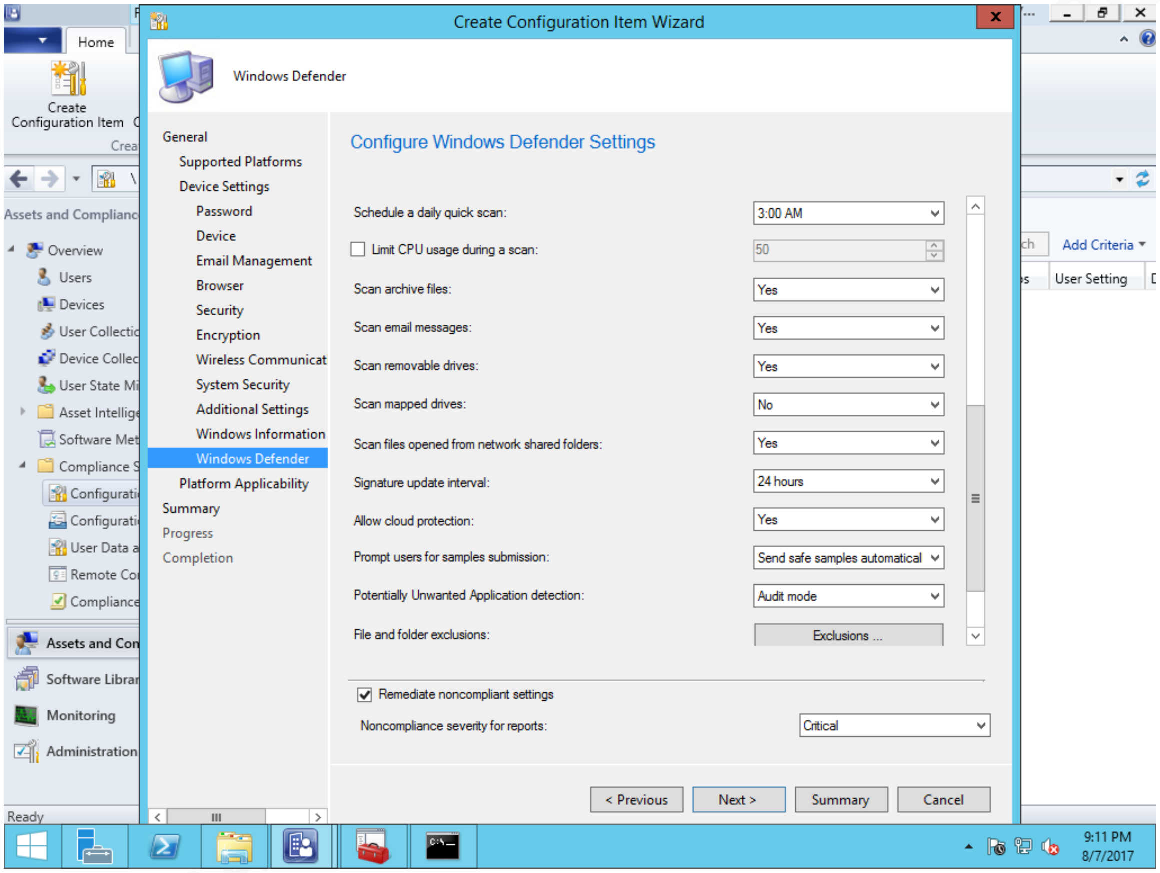
Configure Windows Defender Settings

Allow real-time monitoring:	Yes
Allow behavior monitoring:	Yes
Enable Network Inspection System:	Yes
Scan all downloads:	Yes
Allow script scanning:	Yes
Monitor file and program activity:	Yes
Files monitored:	Monitor only outgoing files
☑ Days to track resolved malware:	7
Allow client UI access:	Yes
Schedule a system scan:	Full scan
Day scheduled:	Sunday
Time scheduled:	12:00 AM

☑ Remediate noncompliant settings

Noncompliance severity for reports: Critical

Figure 20: Windows Defender settings (part 1 of 3)



Create Configuration Item Wizard

Windows Defender

Configure Windows Defender Settings

Schedule a daily quick scan: 3:00 AM

□ Limit CPU usage during a scan: 50

Scan archive files: Yes

Scan email messages: Yes

Scan removable drives: Yes

Scan mapped drives: No

Scan files opened from network shared folders: Yes

Signature update interval: 24 hours

Allow cloud protection: Yes

Prompt users for samples submission: Send safe samples automatical

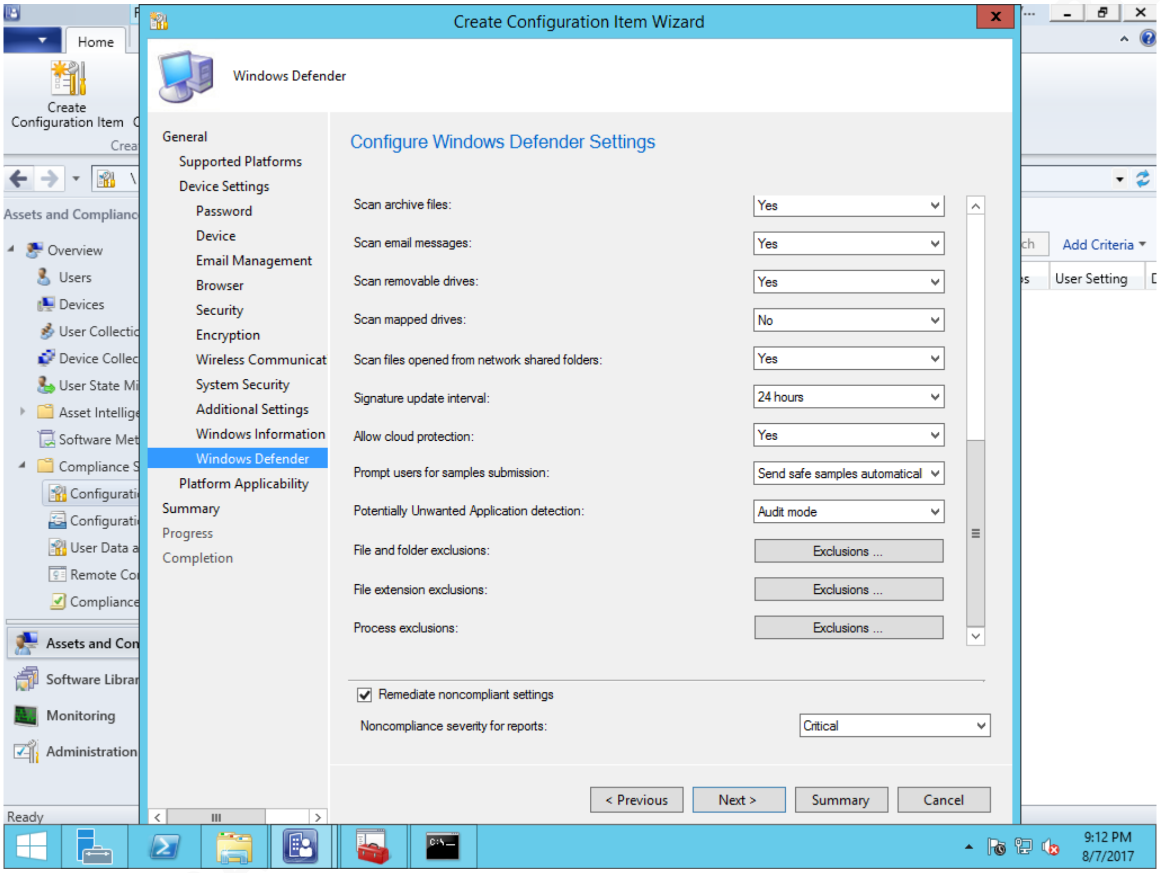
Potentially Unwanted Application detection: Audit mode

File and folder exclusions: Exclusions ...

☑ Remediate noncompliant settings

Noncompliance severity for reports: Critical

Figure 21: Windows Defender settings (part 2 of 3)



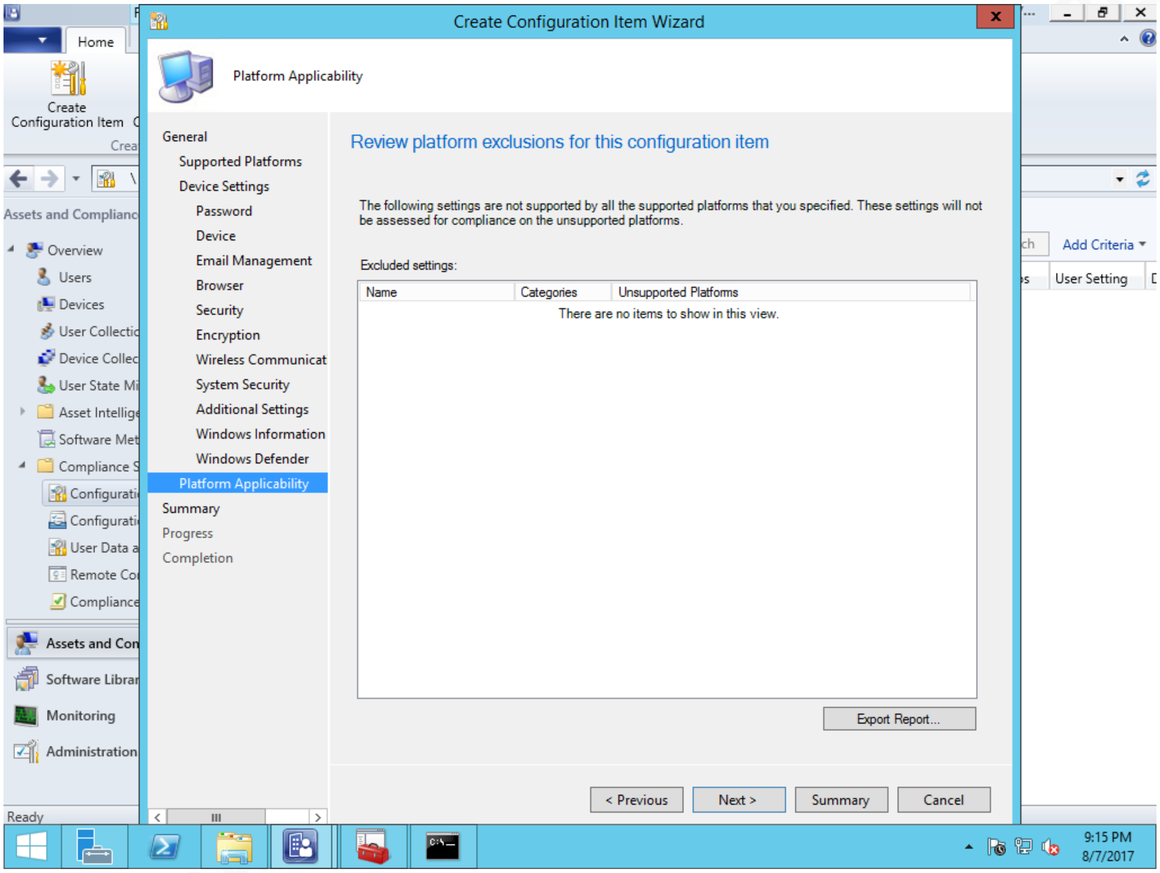
Configure Windows Defender Settings

Scan archive files:	Yes
Scan email messages:	Yes
Scan removable drives:	Yes
Scan mapped drives:	No
Scan files opened from network shared folders:	Yes
Signature update interval:	24 hours
Allow cloud protection:	Yes
Prompt users for samples submission:	Send safe samples automatical
Potentially Unwanted Application detection:	Audit mode
File and folder exclusions:	Exclusions ...
File extension exclusions:	Exclusions ...
Process exclusions:	Exclusions ...

☑ Remediate noncompliant settings

Noncompliance severity for reports: Critical

Figure 22: Windows Defender settings (3 of 3) (note buttons to define exclusions)



Create Configuration Item Wizard

Platform Applicability

Review platform exclusions for this configuration item

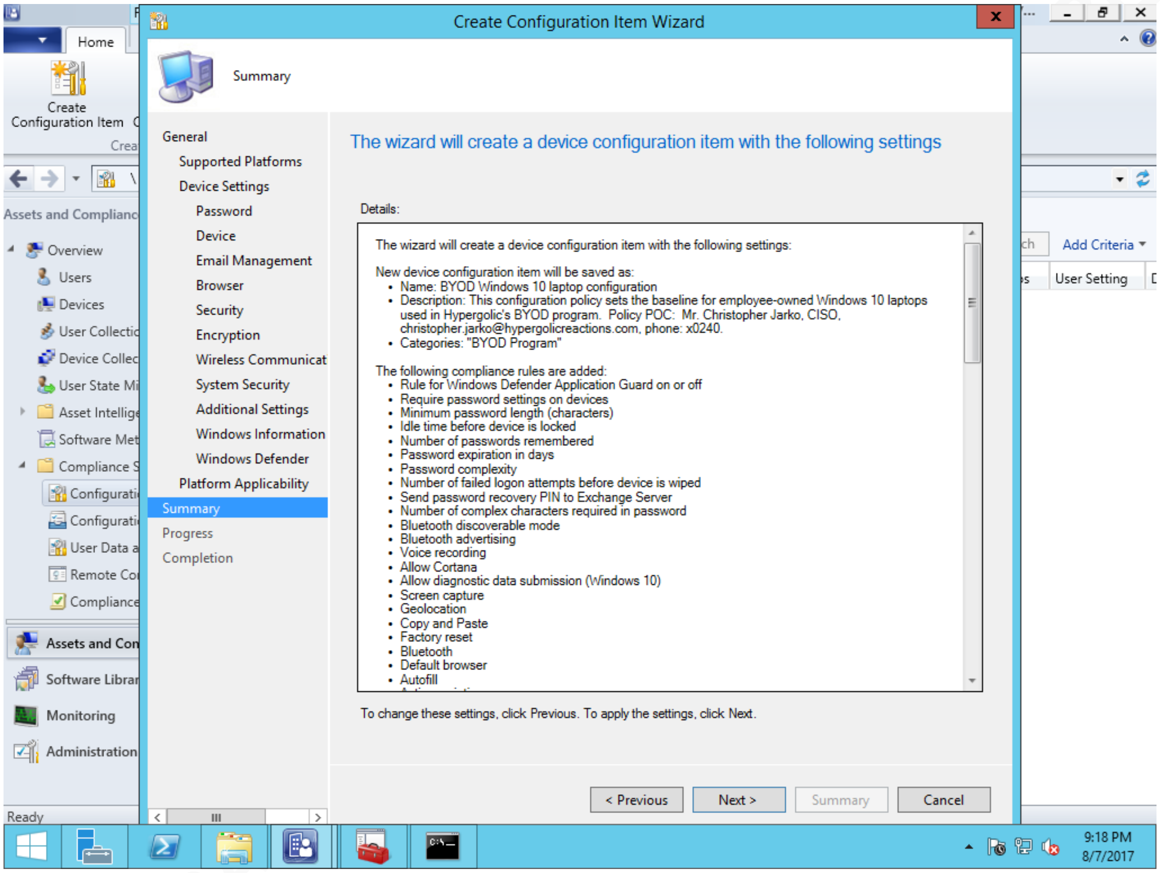
The following settings are not supported by all the supported platforms that you specified. These settings will not be assessed for compliance on the unsupported platforms.

Excluded settings:

Name	Categories	Unsupported Platforms

There are no items to show in this view.

Figure 23: Platform applicability check



The wizard will create a device configuration item with the following settings

Details:

The wizard will create a device configuration item with the following settings:

New device configuration item will be saved as:

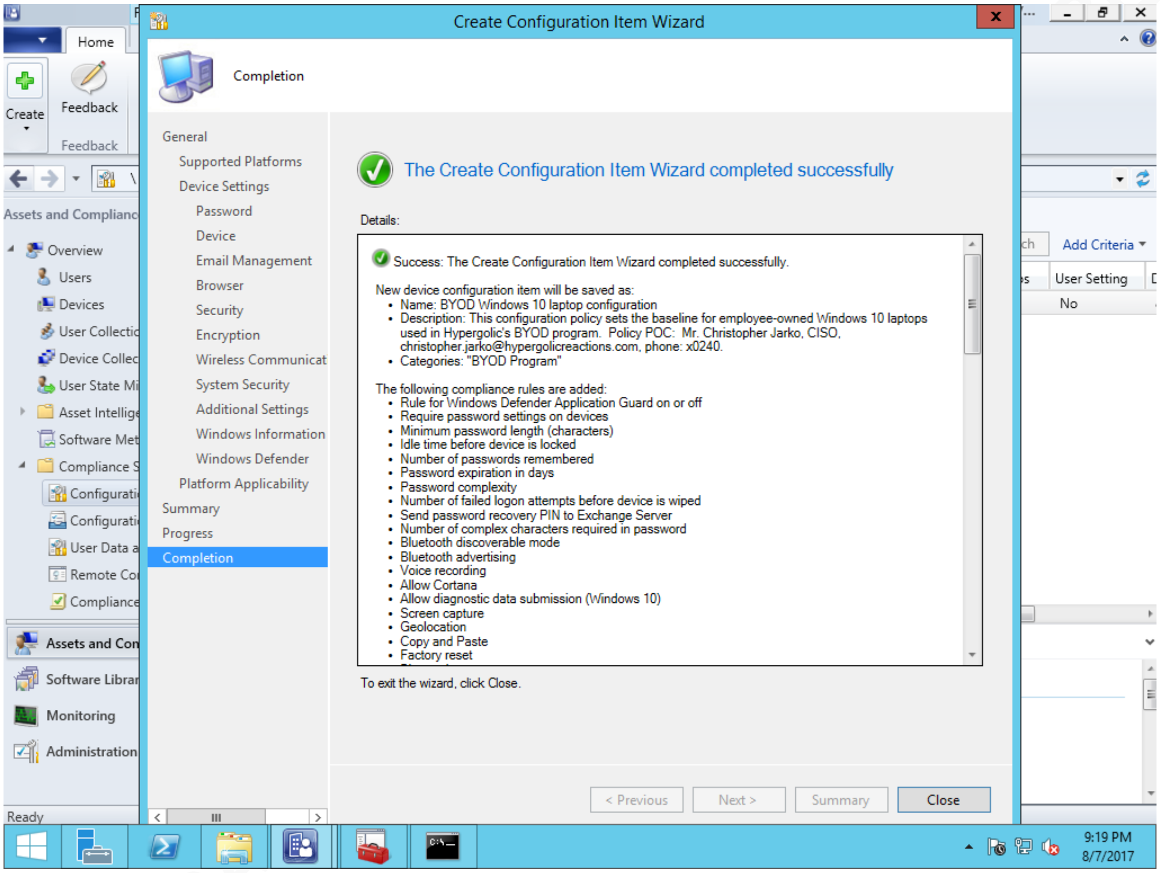
- Name: BYOD Windows 10 laptop configuration
- Description: This configuration policy sets the baseline for employee-owned Windows 10 laptops used in Hypergolic's BYOD program. Policy POC: Mr. Christopher Jarko, CISO, christopher.jarko@hypergolicreactions.com, phone: x0240.
- Categories: "BYOD Program"

The following compliance rules are added:

- Rule for Windows Defender Application Guard on or off
- Require password settings on devices
- Minimum password length (characters)
- Idle time before device is locked
- Number of passwords remembered
- Password expiration in days
- Password complexity
- Number of failed logon attempts before device is wiped
- Send password recovery PIN to Exchange Server
- Number of complex characters required in password
- Bluetooth discoverable mode
- Bluetooth advertising
- Voice recording
- Allow Cortana
- Allow diagnostic data submission (Windows 10)
- Screen capture
- Geolocation
- Copy and Paste
- Factory reset
- Bluetooth
- Default browser
- Autofill

To change these settings, click Previous. To apply the settings, click Next.

Figure 24: Summary of proposed settings



The Create Configuration Item Wizard completed successfully

Details:

Success: The Create Configuration Item Wizard completed successfully.

New device configuration item will be saved as:

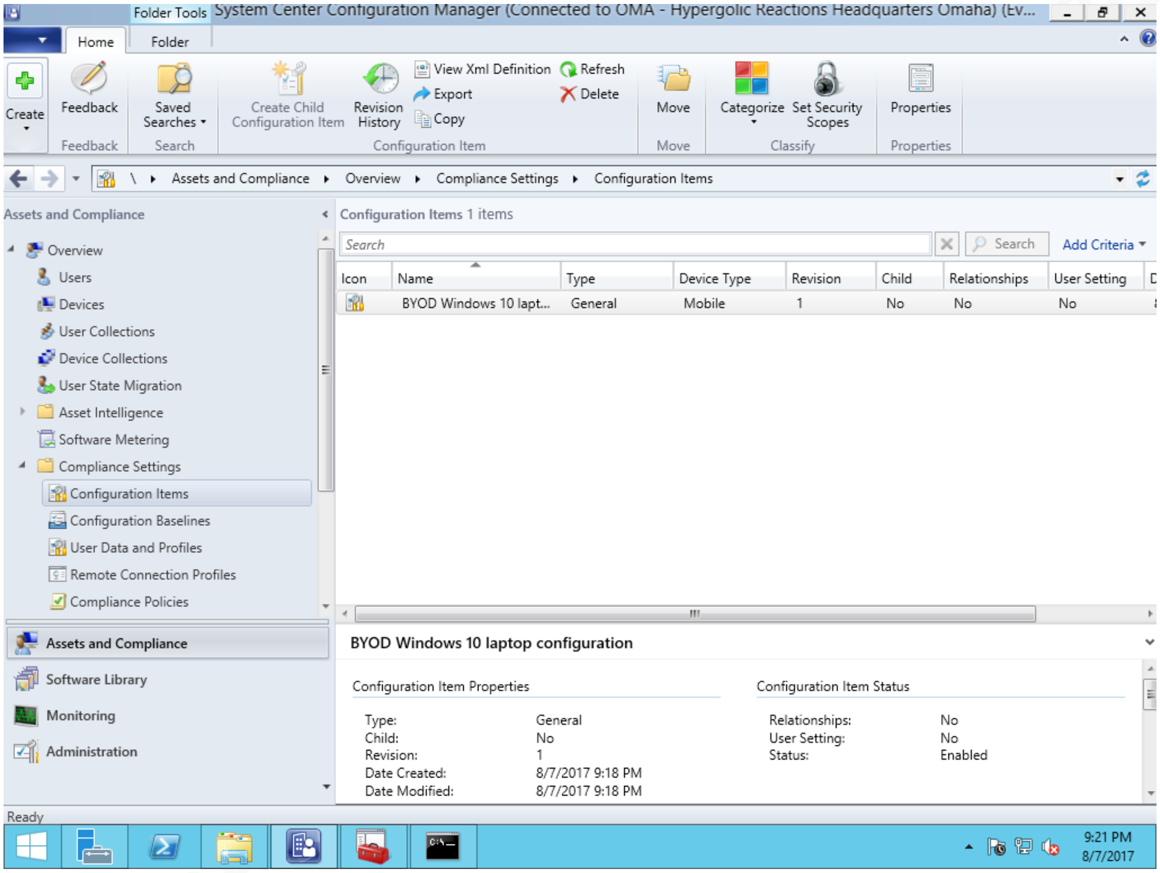
- Name: BYOD Windows 10 laptop configuration
- Description: This configuration policy sets the baseline for employee-owned Windows 10 laptops used in Hypergolic's BYOD program. Policy POC: Mr. Christopher Jarko, CISO, christopher.jarko@hypergolicreactions.com, phone: x0240.
- Categories: "BYOD Program"

The following compliance rules are added:

- Rule for Windows Defender Application Guard on or off
- Require password settings on devices
- Minimum password length (characters)
- Idle time before device is locked
- Number of passwords remembered
- Password expiration in days
- Password complexity
- Number of failed logon attempts before device is wiped
- Send password recovery PIN to Exchange Server
- Number of complex characters required in password
- Bluetooth discoverable mode
- Bluetooth advertising
- Voice recording
- Allow Cortana
- Allow diagnostic data submission (Windows 10)
- Screen capture
- Geolocation
- Copy and Paste
- Factory reset

To exit the wizard, click Close.

Figure 25: Successful completion (Note: "Allow Cortana" does not mean Cortana is enabled (see Figure A-7); it only means the rule was configured.)



Configuration Items 1 items

Icon	Name	Type	Device Type	Revision	Child	Relationships	User Setting
	BYOD Windows 10 lapt...	General	Mobile	1	No	No	No

BYOD Windows 10 laptop configuration

Configuration Item Properties

Type:	General
Child:	No
Revision:	1
Date Created:	8/7/2017 9:18 PM
Date Modified:	8/7/2017 9:18 PM

Configuration Item Status

Relationships:	No
User Setting:	No
Status:	Enabled

Figure 26: Configuration item available in SCCM for deployment

Part 2: Summary of settings in the "BYOD Program" Configuration Item

The following is the actual summary from the Configuration Item Wizard. There are a significant number of elements to this Configuration Item, especially considering the number of setting groups *not* selected for the wizard. (See Figure A-5.)

✓ Success: The Create Configuration Item Wizard completed successfully.

New device configuration item will be saved as:

- Name: BYOD Windows 10 laptop configuration
- Description: This configuration policy sets the baseline for employee-owned Windows 10 laptops used in Hypergolic's BYOD program. Policy POC: Mr. Christopher Jarko, CISO, christopher.jarko@hypergolicreactions.com, phone: x0240.
- Categories: "BYOD Program"

The following compliance rules are added:

- Rule for Windows Defender Application Guard on or off
- Require password settings on devices
- Minimum password length (characters)
- Idle time before device is locked
- Number of passwords remembered
- Password expiration in days
- Password complexity
- Number of failed logon attempts before device is wiped
- Send password recovery PIN to Exchange Server
- Number of complex characters required in password
- Bluetooth discoverable mode

- Bluetooth advertising
- Voice recording
- Allow Cortana
- Allow diagnostic data submission (Windows 10)
- Screen capture
- Geolocation
- Copy and Paste
- Factory reset
- Bluetooth
- Default browser
- Autofill
- Active scripting
- Plug-ins
- Pop-ups
- Cookies
- Fraud warning
- Manual root certificate installation
- Pre-release features
- Update installation options
- SmartScreen
- User Access Control
- Network firewall
- Virus protection
- Virus protection signatures are up to date
- Lock screen notification view
- Allow Manual Unenrollment
- POP and IMAP email
- Maximum time to keep email
- Allowed message formats
- Maximum size for plain text email (automatically downloaded)
- Maximum size for HTML email (automatically downloaded)
- Maximum size of an attachment (automatically downloaded)
- Calendar synchronization
- Custom email account
- Make Microsoft Account optional in Windows Mail app
- AntiTheft mode
- Unsigned file installation
- Unsigned applications
- SMS and MMS messaging
- Removable storage
- Camera
- Near field communication (NFC)
- Allow USB Connection
- Storage card encryption
- File encryption on device
- Require email signing
- Signing algorithm
- Require email encryption
- Encryption algorithm
- Manual Wi-Fi configuration
- Wireless network connection
- Wi-Fi Tethering
- Offload data to Wi-Fi when possible
- Wi-Fi Hotspot Reporting
- Wi-Fi connection: CLF3
- WIP App Management Mode
- Allowed desktop apps
- Enterprise IP ranges
- Enterprise network domains
- Enterprise protected domains
- Data Recovery Certificate
- Protect app content when the device is in a locked state for the protected apps
- Allow encrypted data and store apps to appear in Windows search
- Revoke encryption keys on un-enroll
- Auto detect proxies
- Auto detect IP ranges
- Show Windows Information Protection icons in Windows Explorer and the Start Menu
- Scan archive files
- Allow behavior monitoring
- Allow cloud protection

- Scan email messages
- Scan mapped drives
- Scan removable drives
- Enable Network Inspection System
- Scan all downloads
- Monitor file and program activity
- Allow realtime monitoring
- Scan files opened from network shared folders
- Allow script scanning
- Allow client UI access
- Potentially Unwanted Application detection
- Files monitored
- Schedule a system scan
- Schedule a daily quick scan
- Day scheduled
- Time scheduled
- Signature update interval
- Prompt users for samples submission
- Days to track resolved malware

The following settings are added:

The following applicability criteria are added:

- All Windows 10 (64-bit)
- All Windows 10 (32-bit)