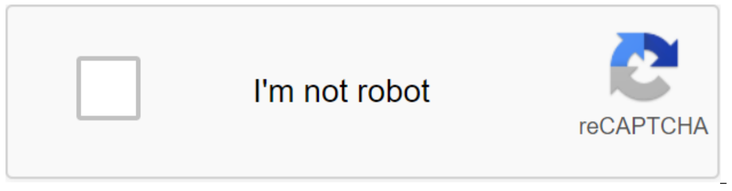
Cisco ise byod deployment guide



Continue

RS0097 - Prime 3.1 Backup and Recovery (Part 2) RS0065 - BGP Multicast (Part 1) RS0129 - SDA Wireless Guest (Part 2) For a standalone or printed copy of this document, just select ⋮ Options's Printer Friendly Pages. You can then print, print on PDF, or copy and paste into any other document format you like. This deployment guide is designed to provide all relevant design, deployment, and operations recommendations for Cisco Identity Services Engine (ISE) to Bring Your Own Device (BYOD), particularly on Cisco Unified Wireless Network (CUWN) controllers. Author: Hosuk Won Table Content Introduction Cisco Identity Services Engine (ISE) is the market leader, based on the identification of network access control system and execution policies. It's a common policy engine for managing, accessing the endpoint, and administering network devices to your business. ISE allows the administrator to centrally monitor the access policy for wired wireless and VPN endpoints on the network. ISE creates context about endpoints that include users and groups (Who), device type (what), access time (when), access location (Where), access type (Wired/Wireless/VPN) (like), threats, and vulnerabilities. By sharing vital contextual data with the integration of technology partners and implementing The Cisco TrustSec policy® defined by segmentation software, Cisco ISE transforms the network from a simple data channel into a security system that speeds up detection time and time for network threats resolution. About this guide, this guide is designed to provide technical advice on the development, deployment and operation of Cisco Identity Services Engine (ISE) to bring your own device (BYOD). Particular attention will be paid to Cisco Unified Wireless Networks controller configurations to handle two BYOD deployment threads; One BYOD and Dual-SSID BYOD. The document contains best practice configurations for a typical environment for the case of BYOD use. Although Cisco ISE BYOD supports wired access, this guide does not cover the BYOD flow through the wired connection. The first half of the document is devoted to planning and design, the other half is devoted to the specifics of configurations and operations. There are four main sections in this document. Initial, defining part of the negotiations on the definition of the problem area, deployment planning and other considerations. Next, in the design section, we'll see how the design is for BYOD. Third, the deployment will provide a variety of configuration recommendations and best practices. Finally, in the exploit section, we learn how to manage BYOD Cisco ISE Identify If you are reading this document, you have already decided to allow users to bring in personal devices or perhaps looking into the resolution of personal devices. The consensus is that BYOD improves user performance because they don't have to be with additional devices for internal access to the network. Before we delve into the details of ISE BYOD, let's discuss what BYOD is. BYOD, as the term says, is to attract and connect personal devices to a managed network. Now, it's a fairly simple concept, but the connection part can have many different meanings for many different customers. For some, this may simply mean connecting to a guest network to access the Internet, for others it may mean providing access to internal resources as well as the Internet, while for others it can mean providing digital certificates and an MDM agent and giving the network administrator some control over the devices, as well as providing access to internal resources not available to guest users. So, as you can see, there may be different GOALS of BYOD based on the customer. However, before you allow personal devices on the network, it's important to determine what requirements you have to access BYOD. Requirements may include who will be allowed to bring in personal devices and how tech-savvy users will be provided by BYOD, what types of devices will be allowed to connect, how are you going to board the end devices on the network to ensure the endpoints are reliably configured? Below is a guide to requirements: Who should be able to bring in personal devices and access the network? The user access network will typically have employees, contractors, and guest users. For typical CASES of BYOD use, BYOD is allowed for employee users and possibly for contractor users. Further control is possible by allowing BYOD for a specific set of users based on user groups if necessary. When users bring in personal devices, what is the role of admin users? What types of devices are allowed into the BYOD network? Are these custom devices where the user can interactively customize devices such as PCs or mobile devices? Or a device that doesn't have a user interface (user interface) such as an IoT device? Does the 802.1X or only PSK support? Are devices personal devices or are you going to treat corporate devices as BYOD? You should also consider how many devices will be tied to one user. Compared to controlled devices, organizations generally do not control BYOD endpoints. Due to lack of control, BYOD endpoints cannot be confirmed as compatible before access is granted, while managed devices can be trusted to have certain elements such as anti-malware, MDM, hotfix, etc. administrators can limit BYOD endpoints to Internet access or a specific set of web applications. Access control can be achieved by assigning various permissions in the form of ACL, VLAN or SGT. Depending on the customer's demand, BYOD may simply allow permission to endpoints connect to the network without an automatic landing process. Which assumes that the end user is responsible for the endpoint configuration to connect and gain access to the network. For many organizations, this level of BYOD can meet their requirements. However, the advantage of the ISE BYOD flow is that ISE can help the end user on board their

endpoints by providing CA with a signed endpoint certificate, as well as customize the network interface and native OS supplicer to use the certificate provided to access the network. Another advantage of ISE BYOD is My Port devices, which allows end users to create/read/update/delete (CRUD) at the endpoints they own. Considering the deployment of solutions As mentioned earlier, there are different ways to be on board endpoints on the network. One way is simply to allow users to connect their personal devices to an existing guest or internal network where the endpoint simply gets access to the Internet only or in the case of an internal network, the endpoint will get the same level of access as managed devices. The other end of the spectrum is where the endpoint is on board through the ISE BYOD stream. When ISE BYOD is on board the endpoint, ISE can issue a Certificate Authority (CA) certificate, as well as automatically set up endpoint network settings to use the endpoint certificate signed to gain access to the network. At the same time, ISE can mark the device as the end point of BYOD, as well as link the endpoint to the user. In addition, the end user can logo on the portal ISE of my devices to control the end point that he/she owns without the need for input from the IT team. When it comes to ISE BYOD, there are two different ways to design user experience threads; Single SSID BYOD and double stream SSID BYOD. If the goal is to minimize the amount of SSID, there is no individual WLAN guest, or if guest access uses access to the access point (rather than named access to a guest account), then a one-SID BYOD is recommended because an open SSID using the hotspot portal cannot be used for the original BYOD portal at the same time. With Single-SSID BYOD, the endpoint associated with the safe WLAN gets on board, then after the endpoint automatically connects the endpoint is granted full access to the network through the same WLAN. If guest access is used by one of these guest accounts, the same guest portal can be used for the employee's BYOD portal. This thread is called Dual-SSID BYOD, where the endpoint is related to WLAN preparation, which is usually transferred to guest access. When ISE that the user is an employee user, the ISE directs the user to the BYOD stream, where the endpoint gets on board. After granting WLAN parameters and possibly a certificate signed by CA, the endpoint reconnects to the secured WLAN for full access to the network. The end point on board When using ISE for BYOD, there are several actions that the endpoint should perform that Start a connection with the appropriate ISE node through the BYOD portal, create digital certificate pairs, submit a certificate signature request and set up a network profile. Some O/S has provisions for such features in their native language, while others require downloading and running the app temporarily to help with the flow. In addition to Apple Mobile Devices (iOS), ISE uses Network Setup Assistant (NSA or AKA Supplicant Provisioning Wizard (SPW) to facilitate the FLOW of BYOD for users. The NSA is an application that is downloaded to the endpoint, either from the ISE itself or from the app store for each of the endpoint types. The NSA helps the user create a couple of certificates, set up a signed certificate, and set up network and proxy settings at the end point. Windows and macOS for Windows and macOS, the NSA is on ISE PSN itself. When the endpoint passes through the onboard stream, ISE instructs the user to download and install the NSA, which in turn directs the user through the BYOD process. Because there are new versions of Windows and macOS that are on the market, the administrator user will need to periodically update the NSA on ISE to support the new OS. Apple's Mobile Devices (iOS) way Apple iOS works is different from other OS in that it doesn't require the NSA ISE app to stream BYOD. Rather, ISE will use existing iOS (Apple Over-the-air (OTA) capabilities to create a key pair, install a signed certificate, and customize WiFi settings. Although ISE uses OTA, iOS receives instructions from ISE in the form of profiles that are installed on iOS. Because there are no download apps, iOS can be on board without access to the Apple App Store. Android devices for Android devices, ISE will force the installation of the NSA during onboard flow, if it is not yet installed. The NSA helps the user create key pairs, set up a signed certificate, and set up Wi-Fi settings. Because Android devices download apps from the Google Play store, the temporary ACL assigned during the onboard stream must be modified to allow such access. Because it's not appropriate to use an ACL IP address to access the game store, it's a good idea to use the DNS ACL on NAD for access. This ensures that access to the game store is allowed even when the IP is changed for services related to access to the game store. In addition to providing access to the game store, it is also recommended that users be sent to pre-load the NSA using other means such as a cellular network or various WLAN to simplify the landing process when the endpoint is connected to the network. The Chromebooks BYOD stream on Chromebook devices is different from other OS. Unlike other OS, where there is no requirement to pre-register endpoints, Chromebook must be registered with Google-Suite before it can pass through the ISE BYOD stream. Teh Teh The administrator needs to set up the Chromebook policy on the G-Suite to get the NSA Chrome extension installed. In addition, the G-Suite administrator needs to set up Wi-Fi settings on the Google Admin console. This is different from other OS, where they get the network settings pushed out of ISE directly. Just like Android devices, Chromebook requires a endpoint to have access to Google resources for BYOD to stream to work. The temporary ACL assigned during the on-board flow must be modified to ensure such access. Because it's not appropriate to use an ACL IP address to access the game store, it's a good idea to use the DNS ACL on NAD for access. This ensures that access to G-Suite resources is allowed even when IP changes are made for services associated with access to the Play Store Unsupported Endpoints As noted above, ISE supports Windows, macOS, iOS, Android and Chromebooks for the BYOD stream. For other OSes, global ISE settings can be switched to determine what access will be given to unsupported devices. You can dictate what level of access will be provided in the event of unsupported devices using a policy or unconditionally provide access to the network. Another option is to manually onboard devices by issuing certificates from the certificate portal and allowing network settings to connect to the network. You can further secure the network by forcing the endpoints to be registered with ISE using the portal of my devices. Finally, if you use a double SSID BYOD thread, you can only allow Internet access if the user chooses not to go through the BYOD stream. After summing up the characteristics of the various endpoints, otherwise through the ISE BYOD thread: The ultimate characteristics of MS Windows NSA located on the ISE PSN site The latest NSA can be downloaded to ISE from ISE GUI Can use the ECC Certificate (Windows 8) As part of the on-board flow the following settings can be configured: - Both wireless and wired interface - web proxies can customize the user, machine, or both for Apple macOS identification Located on the ISE PSN site The latest NSA can be downloaded to ISE from ISE GUI also supports EAP-FAST As part of the onboard flow the following settings can be configured: - Both wireless and wired interface - settings of Apple iOS web proxies Using the native features of iOS (Over-the-Air (OTA)) instead of NSA with iOS 11, and self-signed ID is used for ISE administrator Before the BYOD thread can complete also supports EAP-FAST web proxies settings can be configured along with the wireless profile New iOS may not work if Top Domain Level (TLD) F'D does not valid, such as .local. Google Android NSA located in the Google Play Store the NSA must pre-download or Play Store must be available during the BYOD stream Can use the CERTIFICATE ECC (Android 4.4) Google Chromebook NSA located in the G-Suite Chrome extension Chromebook should be The G-Suite app policy should be configured to force the NSA extension to be preinstalled Other OS In the event of a dual-flow SSID, the BYOD portal can be configured so as to provide guest access if an employee does not want to go through the byOD ISE stream policy can be used to the devices, Profiling Global Settings can be configured to allow access to the network unreservedly My Devices Portal can be used so that the endpoint without the 802.1X ability to connect the Certificate training portal can be used to issue certificates for added security, however the network configuration of the endpoint to use the Digital Certificate While ISE supports different types of EAP to authenticate 802.1X, with ISEOD, there are three types of EAP that can be used; EAP-TLS, EAP-PEAP-MSCHAPv2 and EAP-FAST. With EAP-TLS ISE identifying itself by providing an EAP Identity certificate at its endpoint, once the ISE id certificate is verified by the endpoint, the endpoint will provide its own endpoint id certificate that was previously signed by ISE. Once ISE confirms its validity, the end point will be allowed online. With EAP-PEAP-MSCHAPv2, ISE identifies itself by providing an EAP Identity certificate to the endpoint, once the ISE ID certificate is verified by the endpoint, the endpoint provides a combination of username and password that ISE can verify authenticity. As soon as ISE checks the user, the end point is credited to the network. In both types of EAP, the first ISE provides its own certificate to the end point, and the main difference is whether the endpoint provides a digital certificate or username/password. ISE supports endpoint identification, but it's a good idea to use endpoint certificates for better security and controllability. Password (EAP-PEAP-MSCHAPv2 - EAP-FAST) Digital Certificate (EAP-TLS) Pros Easy to use Certificates are usually valid for a longer period of time than passwords Added Security as a certificate specially built for BYOD only ISE BYOD certificates tied to the end point of MAC address Cons are usually passwords to be changed every X number of days. When the password has been changed, the user must manually change it at all endpoints in short periods of time to avoid connectivity issues. You may need to consider integrating with PKI for a better user experience, THE BYOD Network Access Device ISE BYOD is supported on wireless and wired networks, regardless of the network device provider. However, depending on the feature set available on NAD, deployment may be easier for standards-based. For example, Cisco WLC maintains standards based on coA and RADIUS URL redirection, as well as DNS ACL, making it easier to deploy ISE BYOD. In addition, Cisco WLC is supported by ISE Secure Access Wizard, where ISE can customize WLC and ISE policies for user cases. For other network devices that do not use certain features, ISE can still support the BYOD stream using third-party NAD support. ISE can be configured to take advantage of WebAuth's built-in 3rd-side NAD for BYOD. And for switches that don't have CoA and WebAuth, ISE can be configured to redirect using DNS Sink-holing. Please note that while ISE supports Cisco switches and the 3rd side of NAD for BYOD, this document will focus on deploying BYOD only on the Cisco WLC platform. Below is the table that describes the required NAD feature, and in the case of third-party devices not connected to this feature, as a third-party ISE NAD function can still support network devices. NAD Feature Description ISE 3rd side of the NAD URL redirection feature This allows the endpoints to be redirected to the web portal when the user opens the browser at the end point. This is important for ISE BYOD because ISE needs to interact with the end user to guide through the process. There are two main components to URL redirection. First, the ACL, which dictates that traffic will be allowed without redirection or not, and secondly, the URL destination to direct web traffic when traffic is denied. In addition, there are two different ways to perform URL redirection: - Dynamic URL redirection: When the endpoint is checked through RADIUS, ISE can send back the ACL name and the destination URL as part of the RADIUS response. Most Cisco devices and a limited number of 3rd side NAD supports this method - Static URL redirection: the destination URL and ACL is predetermined by NAD as a static configuration. This is a common URL redirection method in most of the 3rd side of NAD In the case of NAD without a URL redirection function, ISE can be configured to provide URL redirection using DNS-Sinkholing. With DNS-Sinkholing, any direction of web queries is rewritten with an ISE IP address where ISE can provide a CoA web portal Changing authorization is important for BYOD because it provides ways to move from limited access during pre-boarding to full access once boarding is completed. ISE has two different ways of providing CoA: - RADIUS-based CoA: This is the use of RADIUS for communication between ISE and NAD - SNMP Based on CoA: For some third party NAD, which does not support RADIUS based on CoA, ISE can use SNMP to change access. This is done by issuing an ISE SNMP Write command of NAD for the interface to close the interface and immediately return it. As the interface returns, ISE can assign different permissions to the ISE SNMP CoA interface still requires MAB to be configured and On the interface. DNS based on Google Android ACLs and Chromebook requires access to the NSA, which is in the cloud. The NSA can be preinstalled, but if you want to download the NSA during the onboard flow, the ACL must be modified to provide access to cloud resources. Cisco WLC runs 7.6 (8.2 and above supports up up 20 DNS entries on the ACL, while the older version supports 10 entries) and has the function to create an ACL based on F'DN Some 3rd hand NDA supports DNS based on ACLs, for others without function, ISE DNS-Sinkholing can be used to provide the feature. IsE Digital Certificates relies on digital certificates for various aspects of the solution. As noted above, ISE uses certificates to identify itself at endpoints for EAP, but it also uses certificates to identify itself for web portals. In some cases, the EAP certificate and web portal certificate may be different, but in many cases it can use the same certificate to save on management costs. This is especially true when the certificate is signed by the renowned Certificate Authority (CA). One of the main advantages of ISE BYOD is that ISE can provide a signed certificate for endpoints within the BYOD stream. For endpoint certificates, ISE can use an internal CA to issue signed certificates. ISE is already enabled with internal PKI, which can be integrated with the client's existing PKI infrastructure, as well as provide a web portal to manage endpoint certificates. Here are the characteristics of ISE Internal CA: - Usually used for BYOD - Can also be used for other purposes, such as to provide pxGrid communication - Full management of the certificate lifecycle, including multiple templates, expiration date, Annulment (OCSP) - Maintains an expiration date of up to 10 years for endpoint certificates - Supports up to 1 million certificates Integration with MDM/EMM ISE can use MDM/EMM to verify is not in itself providing native MDM/EMM capabilities such as checking on contact lock, encryption, prison broken status, but as end points of connection to the ISE network can refer to the MDM/EMM system. However, if a compatible ISE can provide full access to the network, if the endpoint is not registered with MDM/EMM or does not meet the requirements, ISE can direct the end user to solve the problem without engaging IT. When my Devices is used in conjunction with MSM/EMM, the portal allows the end user to issue MDM/EMM commands, such as remote locking, remote swipe, corporate swipe, etc. When using MDM/EMM to prepare certificates and configuration, the ISE can be configured to trust the mdm/EMM certificate signed to improve the user experience. Below is an example of the attributes of MDM ISE can look for the endpoint Authorization time: MDM Attribute Description DaysSinceLastCheckin How many days have passed since the last MDM check for a specific endpoint DeviceCompliantStatus Attribute check that the complaint status has been confirmed by the MDM server for a specific point point endpoint The endpoint is known to the MDM server and the previously registered DiskEncryptionStatus Disk encryption is not included in the endpoint IMEI. Match-based endpoint IMEI value from MDM server response JailBrokenStatus Match endpoint status JailBroken based on the answer MDM server manufacturer name manufacturer. Match based mobile device manufacturer name from the response of MDM Server MDMFailureReason FailureReason value MDMServerName Match based on MDMServerName from endpoint attributes MDMServerReachable Match achievable status of MDM server MEID MEID Value. Match based mobile endpoint equipment ID (MEID) value from the MDM server response model model value. Match based on the mobile device model from the response mdm server OsVersion OsVersion Value. Match based on the OS version of the mobile device from the response server MDM PhoneNumber PhoneNumber Value. Match based on the phone number of the mobile device PinLockStatus Pinlock is disabled at the end point of SerialNumber SerialNumber Value. The match based on the serial number of the mobile device from the MDM Server server on which the endpoint is registered refers to the type of desktop Device Manager (e.g. Microsoft System Center) or the type of mobile Device Manager (regular MDM server) UDID UDID Value. Match based on the unique device ID (Apple specific) UserNotified User has not previously been notified of the requirement to register the device (Specific check of the desktop manager) Please note that this document will not cover the integration of ISE with MDM/EMM. Design As noted earlier there are two BYOD streams. Here we compare the two BYOD threads. First let's look at the flow of one SSID thread: As its name means, there is only one SSID used for the onboard, which is provided by 802.1X. The user first connects using the username/password and registers, then at will can obtain a signed endpoint certificate issued by the end point, which is used to reconnect to the same SSID and receives increased access. Now let's look at the double stream SSID: In the case of a double SSID thread, the user initially starts on one SSID, which can be shared with the access guest. But once on board, the endpoint is reconnected to the protected SSID to gain increased access. The original SSID can be secured through WPA-PSK if WLC supports WPA-PSK and ISE-NAC (RADIUS-NAC on the same WLAN). Please note that if you use the BYOD guest portal, all employees will go through the same BYOD portal as the BYOD portal tied to the guest portal. Instead of using the BYOD portal, which is tied to the guest portal, as shown above, several BYOD portals can used depending on the state of authorization. This thread allows, for example, different user groups to have different BYOD portals, and allows each group to register devices in different groups of endpoints. Note that in any thread, once the devices have been on board, there is no difference in Network. Here are the pros and cons of various BYOD streams: Single SSID Dual SSID Dual SSID w/ differentiated portal BYOD Pro Custom experience is better for iOS users, as SSID switching from OPEN to SECURED does not require user intervention This is a unique ISE feature where a competitor's solution forces the user to log in twice, while ISE can take user information from session 802.1X without asking the user to log back to the web portal can provide a different BYOD portal based on authorization conditions. The BYOD portal can be tied to another group of endpoints to register. Some organizations prefer to have a special SSID for devices on board. Can provide visible guidance to the user on the BYOD process before entering Better Security: The user can confirm that the BYOD server is legitimate because the user is not asked to manually trust the EAP ID Store certificate is LDAP and cannot begin with PEAP with MSCHAPv2 currently in the LDAP Wired deployment store, Where can not assume the customer already has 802.1X included on the wired interface can be configured to use the protected SSID, which does not broadcast In the case of double flow SSID, the byOD portal can be configured to provide guest access if an employee does not want to go through the BYOD stream Some organizations prefer to have a special SSID for devices on board. Can provide the user with visible recommendations on the BYOD process before entering The Better Security: The user can confirm that the BYOD server is legitimate, since the user is not asked to manually trust the EAP LDAP certificate ID and cannot start with PEAP with MSCHAPv2 currently in the LDAP Wired deployment store, where it cannot assume the customer already has 802.1X enabled on the wired interface can be configured to use a protected SSID that does not broadcast can provide a variety of BYOD portal-based authorization conditions. The BYOD portal can be tied to different groups of endpoints to register. Cons of Fast-SSID settings change should be included on WLC to host iOS devices When end users connect to SSID for the first time there is no easy way to verify whether the server provided a certificate from a trusted source others see double SSID as an additional control burden. The second SSID adds channel overhead and can impair wireless performance Requires iOS users to manually switch SSID Pre-authentication ACL, shared between guest and employee users others see double SSID as an additional control burden. Second SSID adds channel overhead and can impair wireless performance Requires iOS users to manually switch Some client OS may have problems with multiple PKI and ISE Internal CA redirects While issuing signed certificates to the endpoints for BYOD is optional, many customers will consider issuing certificates to the endpoints as this provides better security and user experience for subsequent connections. When installing ISE, the internal internal installed and turned on by default. Here are the characteristics of the domestic CA. - The primary admin node is the root CA - both the primary and secondary admin node is also a sub-CA root called Node_CA. This additional level of hierarchy allows for a single root hierarchy that simplifies deployment when adding new PSNs, while the main node is not an active administrator node - PSN works like CA, RA, and OCSP Respondent When ISE is installed, the first node will become Root_CA. Each of the admin nodes, including the first node, will then become a sub-head of a hierarchy called Node_CA. This additional level of CA hierarchy was made to ensure the installation of the ISE BYOD certificate organ with one root. This makes deployment much easier because it allows you to add PSN at a later time, no matter what admin node is at the time psN is added. In the chart below, although PSN3 was added while the S-PAN (Secondary PAN) was active, the certificate hierarchy is still maintained until Root-CA. This allows PSN3-generated certificates to trust others with NO additional work. Also, note that all nodes operate both RA and CA services along with OCSP. Both the Registration Authority (RA) and the Certificate Office (CA) are required to check requests and issue certificates to the endpoints. Having both services on each node ensures that certificates can be issued autonomously by each PSN. In addition, the Online Certificate Status Service (OCSP) confirms whether the certificate is valid or not, and the presence of the OCSP service locally at PSN nodes ensures that all aspects of BYOD's work can be covered by each PSN. Please note that ISE Internal CA does not support CRL because OCSP is available for CRL verification. When it comes to PKI, ISE can be deployed in 3 variants. The first two levers of CA's internal function are mutually exclusive, while the latter option is simply a proxy request to sign the 3rd side of the CA server, and can also be enabled along with the first or second option. The very signed CA is the initial state of the ISE BYOD setting. The internal CA is enabled by default and is ready to issue certificates for BYOD endpoints. There is no additional action to create the CA. This deployment method would be ideal for PoC, pilot, or if the client intends to separate PKI for BYOD, as opposed to unified PKI for corporate use and BYOD. With individual PKi, it's easier to assign different permissions to BYOD endpoints compared to enterprise endpoints. The subordinate internal CA ISE CA can be integrated with existing PKI customers such as MS CA services. In this mode, ISE will be able to sign BYOD certificates, which are recognized by other organizations that trust the existing CA. If this is the mode of operations that is desired, then the recommendation is to add the initial ISE node as a sub-CA existing PKI before adding a secondary secondary nodes for deployment. SCEP Proxy is an outdated mode of operation where ISE does not use its internal CA, and ISE sends a request to sign a certificate to an external CA. Once signed, ISE sends the certificate to the end point, which is used to identify itself. In this mode, certificate management can only be done with ca itself. For more information about this mode, please refer to the following guide: The following table summarizes 3 ways ISE can issue signed certificates to the end point: SCEP for CA Sub CA Enterprise PKI ISE Self-Signed CA Pros Provide a single point of control for all endpoint certificates; A 3rd side CA console, like ISE, simply proxy all requests to sign certificates to a third party CA ISE Internal Certificates must be overridden if already deployed as a distributed deployment method for The Easiest deployment. No configuration required. ISE is already included with self-signed CA for use with the end point BYOD If there is an existing PKI, ISE Internal CA provides a distinction between the CA enterprise issued certificates for managed devices, compared to BYOD Cons Most complex deployment modes Have only been tested with MS CA (Requires MS Corporate License for SCEP function) There may be licensing costs with a third party CA for each signed certificate endpoint There may be licensing costs with a third party CA for each signed certificate end point of effort may be required to ensure a self-administered CA subscription. Captive Network Assistant Apple CNA (Captive Network Assistant, AKA Apple mini browser) is an Apple iOS feature that allows the browser to like a window, a pop-up whenever you want access to the network, and CNA determines that the network requires user interaction to gain full access to the network. This usually happens when a user contacts an open wireless network, and even if an IP address is provided to the device, the network still restricts the user from taking further action, such as adopting an Acceptable Use Page (AUP), providing a shared password, or logging in as a guest user. This enhances the user experience as it saves the user from manually opening the Safari browser window. It also provides assistance even during a non-initial association with WLAN. For example, if an endpoint device goes to sleep and the session is ripped off on WLC, and then the user tries to use a non-web browser app that requires a network connection, the iOS device may feel that the device in a state of captivating portal and a pop-up mini-browser for the user to take further steps to gain access to the network. As you can see having the iOS CNA feature run on the guest network is a good idea, however, when BYOD is enabled on the same WLAN as in the case of the ISE dual SSID stream, CNA breaks ByOD process. One reason for this is the ISE BYOD process, which causes the CNA mini browser to go into the background because it asks the end user to accept iOS profiles, which includes a CA certificate and a registration package, and when the CNA mini browser moves in the background, it immediately disconnects the device from WLAN, which in turn disrupts the BYOD process. Prior to ISE 2.2, ISE was configured to alert the user that the browser was not supported and the user did not have an easy way to avoid reporting it to the network administrator, and then the administrator had to turn the bypass in captivity on WLC, which disabled the CNA mini browser pop-up window at the controller level. Unfortunately, a bypass function in captivity on WLC 8.3 and below is required for the controller to run wide, which meant that all the WLANs that the controller disabled served the CNA apple. Cisco ISE version 2.2 is the first version to support dual-SSID BYOD stream via Apple CNA. Here's a link to a document that explains how to set up ISE and Cisco WLC, to provide Dual-SSID BYOD, even if the bypass feature of the captive portal is disabled on WLC For other options on how to deal with Apple CNA, please go to the following document: Working with Apple CNA (AKA Mini browser) for ISE BYOD DNS ACL for Android devices and Chromebook, the end point of the OS requires the end point of access to the Google Playback store and Chrome. This is different from apple iOS, macOS and Windows BYOD process. For Apple, iOS ISE leverages OTA's native capabilities to provide certificates and network settings, and for macOS and Windows, ISE provides a network setup assistant that is pushed to the endpoint locally from the ISE site, which does not require access to the endpoint outside the ISE node itself. To allow Android devices and Chromebooks to download Network Setup Assistant, the easiest way to get the NSA uploaded to the end point is to make it through the BYOD stream. This can be done out of range by notifying users to download it from the game store when connected to the Internet by other means. However, if the endpoint going through BYOD does not have the NSA pre-loaded, the way to control access to the Google Play store and Chrome extension through the DNS ACL feature is available on Cisco WLC 7.6 and above. This feature works by tracking the endpoint of the DNS query from the AP and dynamically inserting the IP ACL for the DNS response, which the endpoint gets from the DNS server. Aside from the WLC version, here are additional notes around this feature: ACL pre-retirement and wildcard applications, which means a string value of 0.google.co will match play.google.com and www.google.co.ca not supported by the WLAN WLC auto anchor Version 8.2 and above can support up to 20 20 ACE while previous versions can support up to 10 DNS ACE WLC 8.7 and above supports DNS-ACL with FlexConnect ACL not supported on auto-Anchored WLAN Deployment To understand the configuration required to operate ISE BYOD, this section is broken down into smaller parts. First, it's part of the setup, describing the steps needed to set up WLC and the overall global BYOD settings on ISE. The main part of the configuration will be in the Policy section. ISE uses multiple policies to monitor authentication and authorization flows, and to monitor how endpoints are on the BYOD board. Thus, there are two main policies for change, one of which is a set of policies that includes both authentication and authorization, and the other is a customer assurance policy that monitors which OS is supported for BYOD and how endpoints will receive on board, as well as how certificates will be signed. Below is a table that shows the difference between the two policies: Customer Policy Description Policy This is a control policy that will be pushed by a BYOD profile depending on the type of endpoint or user group. The BYOD profile includes a certificate template, SSID name, proxy settings, etc. Authentication and authorization policy This is a policy to control which portal will be presented to the user going through the BYOD thread. It also dictates how the user will be verified and which network or SSID will be forced to go through BYOD. It can also control what to do if the certificates expire. In addition to policies, there are elements that include policies such as the certificate template and the profile of the indigenous applicants. The certificate template monitors how the endpoint certificate will be signed, including the name of the theme, the size of the key and the duration. NSP controls which certificate template to use and how the network will be configured to the endpoint, including the SSID, EAP-Type, proxy settings, and more. Finally, there are two portals that the end user can use as part of ISE BYOD. The portal of my devices and the certificate preparation portal. This document will describe where the settings for these two portals are located and show access management to the portals. The following diagram shows the relationship between the different elements and the two policies. Setting up a network device This section involves Cisco WLC and the network is already configured with basic settings including IP controls, interfaces and DHCP. This section will run through the WLC/ISE link setup using RADIUS, relative WLANs, and ACLs. For the full Cisco WLC configuration for ISE, please use: Enable the quick change feature (optional) dual-SSID flow for better user experience. The inclusion of this feature allows wireless customers to move from Open SSID to Secured SSID without delay. In the SSID double stream, if From open to secured SSID continues to fail at the end point, then check out the following WLC settings: Access to WLC GUI and go to the controller of the s.a., Click Click And Save the ISE RADIU configuration configuration as THES authentication and accounting server go to security and RADIUS Authentication Click new... in the top right corner to add a new RADIUS authentication server, the RADIUS authentication server settings are listed in the table below (Using the default, if not specified) Attribute Value or description Server Index (Priority) (Index Value) IP Address (ISE PSN IP) General Secret format ASCII General Secret (General Key RADIUS) Port Number 1812 Server Status Included Support RFC 3576 Included (This option enabled CoA) Server Time Out 5 (recommended 5 seconds or above) It can be disabled all over the world) Control is disabled Click Apply and save the configuration. Click Accounting and new... to add RADIUS accounting servers TO RADIUS, the accounting server settings are listed in the table below (Using the default, If not specified) Value or description Server Index (Priority) Available Value Index Server IP Address ISE PSN IP Common Secret format ASCII Total Secret KEY RADIUS Port Port Number 1813 Server Status Included Server Time-Out 5 Network User add as RADIUS authentication and accounting for each PSNs) Create redirection ACL Single ACL will be created for redirection, that applies to both the one SSID flow and the dual SSID flow go to security qgt; Access Control Lists click on New and create ACL_WEBAUTH_REDIRECT ACL with the following parameters. The ACL name 'ACL_WEBAUTH_REDIRECT' is the default ACL name that ISE refers to, so if you use another ACL on WLC, be sure to change it in the ISE Authorization profile. Note that the WLC ACL is aussy, so you need to create a reverse authorized ACE. Action Source IP / Mask Dest. IP / Mask Protocol Source Port Dest Port Direction Permit {ISE}/255.255.255.255 0.0.0.0 / 0.0.0.0 TCP 8443 Any Outbound Permit 0.0.0.0 / 0.0.0.0 {ISE}/255.255.255.255 TCP Any 8443 Inbound Permit {ISE}/255.255.255.255 0.0.0.0 / 0.0.0.0 TCP 8905 Any Outbound Permit 0.0.0.0 / 0.0.0.0 {ISE}/255.255.255.255 TCP Any 8905 Inbound Permit {ISE}/255.255.255.255 0.0.0.0 / 0.0.0.0 TCP 8084 Any Outbound Permit 0.0.0.0 / 0.0.0.0 {ISE}/255.255.255.255 TCP Any 8084 Inbound Note: Even when explicitly not stated, DHCP and DNS is permitted pre-web-authentcation on the WLC. If you want to deny access to DNS servers on the Internet, an ACL can be added to limit on certain servers. Also note that this ACL works with ISE 2.4, however the older version of ISE may require additional TCP ports to be open. Open. Back in the top right corner Click down the arrow next to the ACL and select 'Add-Remove URL' Here enter the following entries one by one .google.co accounts.youtube.com gstatic.com .googleapis.com .appspot.com ggpht.com gvt1.com market.android.com android.pool.ntp.org .googleusercontent.com .google-analytics.com Click Back Click Click Create a Single ACL blacklist will be created for the blacklist of the Go to Security portal. The ACL name 'BLACKHOLE' is the default ACL name that ISE refers to, so use another ACL name in WLC to change it in the ISE Authorization profile. Note that the WLC ACL is aussy, so you need to create a reverse authorized ACE. Please note that this ACL allows full IP access to ISE nodes, but can be modified to limit the impact of ISE from end users. Action Source IP /Mask Dest. IP/Mask Protocol Source Port Dest Port Direction Resolution ISE/255.255.255 0.0.0 / 0.0.0.0 TCP 844 4 Any exit resolution 0.0.0.0.0 / 0.0.0.0 (ISE)/255.255.255.255 TCP Any 8444 Incoming Note: Even if explicitly not stated, DHCP and DNS are allowed pre-web outsourcing on WLC. If you want to deny access to DNS Internet servers, an ACL can be added, to limit DNS to certain servers Click 'Back' in the top right corner Click Apply Secured SSID Go to WLAN Click on Add New and Create WLAN with the following Tab Attribute Value settings or description of General WLAN ID Available WLAN ID Profile Name / SSID Secured Status Included Level Security 2 WPA Security-WPA2 WPA-WPA2 Options WPA2 WPA2 Policy WPA2 Encryption AES Authentication Key Control 802.1X Layer 3 Captive Network Assistant Bypass Enabled AAA Servers Authentication and Accounting Enabled and ISE PSN Nodes Selected (If Multiple PSN Identified, list them here for both authentication and accounting in order) RADIUS Server Accounting Interim Update Included, Intermediate Interval 0 Extended Allow AAA To Redefine Included NAC State ISE NAC (Or RADIUS NAC) RADIUS Customer Profiling HTTP and DHCP Included Open SSID (optional) If there is an existing guest WLAN The same portal can be used for BYOD employees as well. As an employee enters the ISE guest portal, they recognize guest users and employee users and apply different threads. For guest users, ISE automatically applies guest-related access. Only a named guest access portal, such as a self-service or sponsored guest portal, can be used simultaneously as a BYOD portal. If guest access to the hotspot, the same portal cannot be used for both hotspots and byOD portal. To create an open WLAN: Go to WLAN Click on Add New and Create WLAN with the following Tab Attribute Value settings or description of General WLAN ID Available WLAN ID Profile Name / SSID Open Status Included Security Level 2 Security No, MAC MAC Layer 3 Captive Network Assistant Bypass Included AAA Servers Authentication and Accounting Included and ISE PSN Nodes Selected (If Multiple PSN Identified, List Them Here for Authentication and Accounting in Order) RADIUS Server Accounting Interim Update Included, Intermediate Interval 0 Extended Allow AAA Override Included NAC STATE ISE NACE This document assumes that Cisco ISE is installed and the IP management address is available through GUI. Go to the Administration of network resources of the Network Devices Click to Add Name Giving, IP Verification RADIUS Authentication Settings and the section will expand for more options To Provide a Generic Secret Click Save Value Value Value Name NAD IP IP Address NAD IP IP Address Nad RADIUS Common Secret between ISE and NAD Identify Global Settings to Monitor How Many Devices That Can Be Registered by Each User, Go to Work Centers The default is 5 devices, but can be installed between 1 to 999 devices. Please note that this applies to all BYOD users around the world. The Retry URL allows the administrator to set up a URL that ISE will try to force a new URL redirect when the initial thread on board failed for any reason. For example, if a user has abandoned the onboard thread in the middle and returned, the existing session may have been disrupted and the user will need to re-initiate the thread. ISE re-initiates this by forcing the browser to try the URL specified in the settings. By default, if the Retry URL is not specified, ISE will try 1.1.1.1 to force it to redirect. By default, devices without NSA support follow a basic authorization policy for access to the network, but in order to provide unconditional access to the network for unsupported devices, select the Allow Access to network option for the Indigenous PetitionErs' Service Policy Is Unavailable. Managing and defining the certificate template is an optional step if EAP-PEAP-MSCHAPv2 or EAP-FAST are used instead of EAP-TLS. The fresh ISE installation comes with a default certificate template called EAP_Authentication_Certificate_Template, which is used when signing certificates during the BYOD stream. The content of the theme can be filled with the customer's environment in mind, but also note that the content in the object can be used during authorization to assign different permissions. For example, two separate certificate templates can be created for two different groups in the Organization and used to provide certificates to two different OUs. When BYOD devices are connected after boarding, ISE can OU for differentiation and appointment of different ACL or VLANs. The existing certificate template should work for most environments, but it's a good idea to change the theme theme to reflect the site on which ISE is being deployed. In addition, certificate properties, such as key type, key size, and actual period, can also be modified with a template. To change THE CN (organization, organization, city, state and country) and other certificate properties, follow below. Go to the administration of the 'gt; Certificates' Certificates of Certificates' zgt; Certificates Patterns Click on Add (or edit to edit the default 'EAP_Authentication_Certificate_Template') enter specific site information in the theme fields. The CN field is automatically populated by ISE with a user ID that runs through the BYOD ISE process and automatically fills out the MAC endpoint address in the SAN certificate box. The endpoint MAC address is collected during the initial endpoint authentication, either through MAB or through 802.1X and built into the certificate for security reasons. By doing so, the ISE policy can be developed according to the actual MAC endpoint address and the MAC certificate address to prevent the use of BYOD certificates issued for another endpoint, moreover, for which it was issued. The template also allows settings to change key types (RSA and ECC), key size, and actual period. Certificates can be changed from 2 years by default to a maximum of 10 years. Please note that the new client OS requires a key size of 2048 or a larger name for the certificate template attribute attribute. Provide a descriptive name because this field can be used as an AuthC/y cn theme condition is an automatically populated username that passes through the BYOD thread. Other attributes can be entered here to reflect the site. If differentiation of different endpoints or users is required based on the certificate, then any of the attributes here can be changed and can be used during out to ensure differentiated access. For example, if OU'HR, the endpoint may have access to hr resources, while other endpoints may not access hr resources theme Alternative Name (SAN) Currently, the only value available is the MAC address. The MAC address is drawn from the RADIUS session from the end point that triggered the BYOD thread. This is one of the ways in which ISE allows the admin user to link the certificate to the actual end point at which it was signed. The key type is RSA or ECC. EcC is currently only supported by Windows and Android devices. Key size 1024, 2048, 4096. For compatibility, the recommended minimum is 2048. SCEP RA Profile ISE Internal CA. If you use SCEP for a third party CA, this setting can be changed to send a certificate signing request to a third party The actual period is from 1 days to 10 years. A classic security case against convenience. Extended use of keys to use BYOD, only the customer authentication option should be verified ByOD Profile Definition and Resources Here you can manage Windows and macOS Network Setup Assistant (NSA) as well as compile the Profile Native Supplicant (NSP). There are two predetermined NSP; One One Chromebook and another common among all the other supported OS. With Chromebook, most of the network settings are pushed through the G-Suite, so the only setting for the NSP change is which certificate template should be used. For another OS, multiple wireless profiles can be automatically identified and created for any WLANs. In wireless settings, proxies, WPA settings, EAP type, and certificate template are set up. Native Supplicant Profile (NSP) manages the certificate signing pattern, wireless settings, proxy settings, EAP type, and wired network settings. At a minimum, the existing profile of Indigenous applicants (NSP) must be changed to reflect the name of the SSID provided by WLAN, which is used. Follow the steps below to make changes to your existing NSP or create a new NSP. When creating a new NSP, the customer training policy should be changed to use the newly created NSP. Go to the policy of the gt; elements of the policy of the qgt; The Results of the Customer Securing zgt; Resources Edit Cisco-ISE-NSP (Or add a native profile of the supplicant) If NSP editing by default, there is an SSID 'ISE' that can be edited for the safe SSID used on the site. Editing SSID by default by checking it and clicking on SSID Name (Optional) Editing Editing Related Settings It's recommended to leave WPA2 Enterprise security for the permitted protocol, select among TLS (for digital certificate), PEAP (for username and password), or EAP-FAST (for macOS and iOS). Please note that you also need to select a certificate template when using TLS. Expand additional settings can be used to customize additional settings: For Windows endpoints, using a machine or a custom store to customize the certificate of transmission settings SSID can be installed here for iOS devices, SSID broadcast settings can be installed here Click Send If the wired interface should be used, then the 'Wired Profile' checkbox can be enabled for Windows and macOS As part of the customer Resource giving page , an updated NSA version for Windows and macOS can be downloaded. To download the latest NSA, follow the instructions here: Click on Add's Resource Agent from the Cisco site After the screen update will list available agents that can be downloaded from the Cisco site. This includes the NSA as well as the posture of agents (If the ISE node does not have access to the Internet, this page will not be able to download the NSA, in this case, download the NSA manually from cisco.com and add them manually using Add's resource agent from the local drive). Select the latest version of

MacOsXSPWizard x.x.x.x.x and WinSPWizard x.x.x. Click Save After Download, recently downloaded NSA can Used in Customer Management Customer Policy Enforcement Policy Customer Providing Customer Policy Provision Policy dictates that the OS will be supported and which NSP will be used. The NSP designation also controls which certificate template will be used to sign endpoint certificates. Also, if the new NSA was downloaded, the customer's client can be updated to reflect which NSA will be used to assist the user on board the device. This may be necessary when a new version of the os end point has been introduced to the market. Finally, note that this same policy also affects the posture of the customer training as well, which controls what type of posture agent and matching module will apply. Although there are two different customer settings in one rule, ISE can apply different customer settings depending on the flow. The top part, called 'Agent Configuration', controls the posture agent for the rule, while the bottom part, called 'Native Supplicant Configuration', controls the settings for BYOD training. Below is the default customer support policy on the newly installed ISE 2.4 system, which includes a policy rule for ISE. In general, the existing customer training policy should work for most environments, but if a new NSA for Windows or macOS has been downloaded, you will need to update the customer training policy to reflect the changes. In addition, if you use a media profile other than the system, provided it's used, then the customer's giving policy should be updated to reflect the changes. Finally, if a specific set of users requires a separate NSP, Other Conditions can be changed to match certain user groups with specific NSP. To create a new rule of giving customers: Go to the policy of the zgt; Customer Securing All OS policies are already predetermined, however, if a new policy is needed click on the arrow down to the right of any rule and select Insert a new policy ... (Note that the policy works from top to bottom, so if there is a more specific rule that needs to be mapped, make sure the new rule is on top of other rules) Provide the rule name If a specific rule must be in line with a specific internal user or endpoint group, it can be specified here select Operating Systems. If a specific version of Windows or macOS is to be specified, it can be specified here Use other conditions to further qualify the policy rule. AD groups/attributes, location, EAP types, etc. can be used here. The Result section dictates the NSA and NSP version. Please note that the version is only available if Windows and macOS are selected for operating systems, as these two OS download NSP directly from PSN, while the other OS relies on native features or cloud resources. When installing ISE, there is a policy for the Single-SSID BYOD thread, and there are a set of Auth policy rules that were pre-created for the BYOD thread. Despite the fact that politicians already exist, the rules are deactivated. The admin user can simply include two rules to activate the BYOD policy. These two rules are Employee_EAP-TLS and Employee_Onboarding. When a user connects to a protected SSID using a username and password, the endpoint of the user does not have a digital certificate, so the session will comply with the Employee_Onboarding policy rule of Employee_Onboarding makes the endpoint be on board. As the endpoint passes through the onboard stream, the endpoint MAC address is registered in ISE, and the signed certificate is awarded to the end point, at which point the endpoint will be forced to re-stun at the same SSID, where the session will comply with the 'Employee_EAP-TLS' policy, and the endpoint will receive PermitAccesss permission. While pre-configured policy rules work for simple deployments, when you set up an authentication and ISE authentication policy, it's a good idea to create a separate set of policies for each SSID. By doing so, politicians are much easier to view and predictable. Here we are going to create a set of policies for secured SSID used for a single SSID BYOD thread. Initially, endpoints are associated with SSID using a username and password using PEAP-MSCHAPv2. When a user opens a web browser, instead of reaching the user's browser destination or homepage, the user will be redirected to the BYOD portal, where the user is guided to follow the steps to get the end point on board. Go to politics qgt; Policy Sets Click on I Change the New Name Policy Set to Secure SSID Under The Use of Normalized RADIUS : SSID Ends SECURED Click on use Select Access to the Default Network for Permitted Protocols Click Save on qgt;' to authorization policy Click 'x' on denial of access to results: Profiles Column Select NSP_Onboard :EAPAUthentication equals EAP-TLS' such as a match on the SAN certificate with the MAC address extracted from the RADIUS session, and the registered BYOD status can also be used here) For results:Profile Profiles Select Resolution Process Click Saving Creation Policy for dual-SSID BYOD Flow As with a single SSID thread, also for dual SSID, when ISE is installed, there are a set of Auth policy rules that are pre-created for the BYOD thread. Despite the fact that the rules of politics already exist, the rules are deactivated. The admin user can simply include two rules to activate the BYOD policy. These two rules: Employee_EAP-TLS and WiFi_Redirected_to_Guest_Login. The WiFi_Redirected_to_Guest_Login rule is also used for general self-service called guest access. If self-service is not required, it may be disconnected from the guest portal settings. You can do this by visiting a guest portal that is used for BYOD purposes and controlling the Allow the guest to create accounts. To make a guest portal also support BYOD, byOD settings on the portal should be changed. Go to the guest portal and expand the BYOD settings, and then check the Allow employees to use personal devices on the network. Note that once this option is verified, the contextual guest flow chart on the right reflects the change. 'Allow' To Allow Guest-only choice allows employees to bypass the BYOD process and select only guest access. Please note that if you use the BYOD guest portal, all employees will go through the same BYOD portal as the BYOD portal tied to the guest portal. Instead of using the BYOD portal, which is tied to the guest portal, as shown above, several BYOD portals can be used depending on the state of authorization. The instructions for setting up the thread are displayed in the app. In the case of double SSID BYOD, when the user connects to an open SSID, the endpoint is unreservedly authorized for limited access to the network, which provide enough access to get to the guest portal ISE. This is done with advanced MAB authentication options for 'CONTINUE', even if the user is not found. The CONTINUE option in the authentication policy allows unknown MAC addresses to bypass authentication and obtain conditionally permitted limited access, where the endpoint can reach the ISE portal page to log on to the Internet. This allows the user to open the web browser and the user is redirected to the guest portal. When a user logs in using a username and password, ISE identifies the user as an employee because the account used to log in to the portal is not included in the guest user's database, forcing the user to the BYOD portal instead of guest access. As the endpoint passes through the onboard stream, the endpoint MAC address is registered in ISE, and the signed certificate is present to the end point, at which point the endpoint will be forced to connect to the SSID provided, where the session will comply with the 'Employee_EAP-TLS' policy, and the endpoint will receive PermitAccess. If you don't use the default policy set, you can use the following instructions. Here we are going to create a set of policies for Open SSID, used for the double flow of SSID BYOD. Initially, the endpoints are associated with Open SSID. When a user opens a web browser, instead of reaching the user's browser destination, the user will be redirected to the guest portal. When a user enters employee credentials to a guest portal, the user is guided to follow steps to get the end point on board. ISE can distinguish between employees and guests, identifies the store identification that is used during authentication. Because the endpoint will connect to a secured SSID after the landing is complete, you must complete the steps for the SSID flow. Also note that the BYOD portal has nothing to do with dual-SSID, as the BYOD stream is a subset Guest portal. Go to the guest portal, which currently refers to the authorization profile 'Cisco WebAuth' (If it's a fresh ISE setup, it should be a 'Self-registered guest portal (default)) Go to the work centers of the gt; Guest Access portals and components of the guest portals Click on the self-registered guest portal (by default) Scroll down to Settings and click to expand Click Allow employees to use personal devices on the network Scroll up and click Save Go to The Policy Sets of Policies Click on I Change the New Set of Policy Name Open SSID Under the Use of Normalized RADIUS: SSID Ends OPEN Click to Use Select Access to the Default Network for Permitted Protocols Click Save Click on 'Click' , select internal endpoints instead of All_User_ID_Stores Click on "gt; Options' Change if the user is not found from REJECT to CONTINUE (Installing this as CONTINUE allows ISE to unconditionally authentic unknown MAC addresses so that the session can continue through Authorization instead of getting instant REJECT. will be initially unknown isE and yet, ISE should be able to assign limited access to the network so that the user can be directed to the ISE portal page) Click on the authorization policy Click 'x' on Deny Access on Results:Profiles Column Select Cisco WebAuth Click Save (In real deployment, if the same portal is used for guest users, then we will create a guest access rule as above the default rules) Note on the various portals ISE Still document provided however, there are other portals that can be used to provide greater control for end users : Type of portal Config Location used for the guest portal Work Center zgt; Guest Access qgt; Portals and components of the User Portals This is only used for double-flow SSID. The existing guest portal can be used for guests and BYOD at the same time, provided that the customer uses named guest access, as opposed to accessing guests to the hotspot. BYOD Portal Work Center by'gt; Portals and Components by'S byOD Portals or Administration of the Device Portal of the BYD's BYOD Custom Portal that the end user passes through for boarding. This is only used to sing-SSID Stream Blacklist Portal Administration's zgt; the device management portal is a zgt; blacklisting portal users for users with endpoints in the blacklist group. Instead of denying access to the network for blacklisted devices, it can be helpful to provide a visual guide on how to proceed to get the device back into the network when their device is blacklisted. My Portal Devices (MDP) Work Center is a bygt; by're-portals My Devices OrAdministration Portals are used by end-users to control their own devices. Here, users can view on-board devices as well as manually add devices. The user can also flag the devices as stolen or lost, which can affect access to the network. If ISE is integrated with MDM/EMM, the user can also release a lock, a full napkin and a corporate napkin from the portal. The device's certificate portal Used to sign and create certificates manually. Certificates can be signed by importing CSR or a certificate of steam can be obtained from the portal. Access to the portal can be controlled through the ID store and groups. Setting up a blacklist portal (optional) Blacklist portal is already set up, but note that it works on a variety of TCP port 8444 compared to the guest or BYOD portal that runs on 8443. In addition, the blacklist portal uses a variety of ACL on WLC. The policy for blacklisted devices is already in place, but to change the content provided by users when their devices are blacklisted: Go to the administration of the device portal and the Blackist Portal Blacklist (default) Click on the page name of the portal page setting and the message can be changed Click Save Note that the policy for the blacklist has already been set up and included on isE He still requires a 'BLACKHOLE' ACL to attend nad for work. Set up my Devices Portal (optional) My Devices Portal is hosted on PSNs and is already on by default. MDP is commonly used for non-guest users to manage their personal devices. Follow below step to reconfigure the behavior of the portal of my devices Go to work centers of the gt; byOD zgt; Portals and Components of the zgt; My Devices Portal Click on my Devices Portal (default) Expand the Portaign Setting Certificate Group tag Fully Qualified Domain (F'DN) and host names (If F'D configured here, DNS server should be updated to be on PSNs If the portal certificate used is not a wildcard certificate, it must also contain F'D as a SAN to avoid a security pop-up in a web browser, try to access the portal) the Endpoint Identification Group authentication method (there is currently no way to monitor access to MDP based on groups of end users from internal ID or AD. Any user with valid user credentials can access MDP) Scroll up and click on the Page Setting portal under the pages, click on The Office Device Click on settings on the right preview panel You can choose what options are available for end users to set up the certificate preparation portal (optional) The certificate portal is hosted on PSNs, but authorization groups must be assigned before the user can log on to the portal. Follow the step below to reconfigure the behavior of the portal to provide certificates Go to the administration of the zgt; management portal Certificate Giving Click on The Portal of Certificate (Default) Extension Porter Settings Group Tag Group Authentication Method Authorized Groups Fully Skilled Domain (F'D) and Host Names (If F'D configured here, DNS server should be updated to point to PSNs, and in order to make sure F-DN certificate portal users. In addition, if the portal certificate used is not a wildcard certificate, it must also contain F'DN as SAN to avoid a pop-up security in the web browser while trying to access the portal) Work Pitch User Experience Note 1 User connects to secure SSID and provide valid employee credentials to access the network. Because the RADIUS server is unknown to the endpoint, the user is asked to trust the server before submitting the credentials. Although the user is associated with WLAN, the user is limited to the ISE portal and related services to work with the BYOD thread. This includes DHCP, DNS, and access to the G-suite or Google Play store. 2 Once associated with a secure SSID, the user opens the browser and the browser automatically redirects the user to the BYOD portal. Note: If the pseudo (Apple CNA) browser automatically opens, it means that the captive portal bypass function was not enabled on WLC or WLAN. BYOD's 3nd page allows the end user to provide the name and description of the device so that the devices can be identified when multiple devices have been registered by the same user. 4 3rd page portal brokers creating a pair of certificates and signing. It also automatically adjusts the network interface or WLAN profile in the settings listed on ise NSP as an admin user. On iOS, ISE uses iOS to achieve this and forces the user to go through a series of installations of iOS profiles. Depending on the iOS security settings, the user may be asked to enter an iOS PIN to trust the settings and profiles they've downloaded. Note: If a self-recall certificate is used, in connection with XXX, iOS 10.3 and above requires additional steps to trust the ISE certificate. For more information, please visit the app. 5 Once the board is successful, the user is sent back to the Safari browser. The last page of the portal notifies the user that the user has full access now. The user can open the app or view it to another destination. ISE Live magazine Starting from below, the user communicates with SSID Lines only Endpoint ID represents CoA, which has been successful. Multiple CoA can be sent depending on the CoA settings to ensure a proper endpoint session is assigned showing the endpoint of the Authorization Profile has moved from NSP_Onboard to PermitAccess Top Most Lines points to a session that combines THES authentication to information extracted from radius accounting, which includes the endpoint ip address Review dual-SSID BYOD User Experience on iOS Experience 1 The user connects to the open SSID and opens the Safari browser. The user is automatically redirected to the guest portal. If the guest portal certificate is not signed by a known CA, the user can receive the request before proceeding to the guest page of the entrance. The user provides valid employee credentials to log in to the guest portal. 2 ISE sees that the user is not a guest of the user and is directed to the BYOD thread. Byod. that this page shows the 'Guest Portal' in the title because the user is using the guest portal for BYOD. If necessary, you can change this to a different name in the settings of the guest portal. BYOD's 3nd page allows the end user to provide the name and description of the device so that the devices can be identified when multiple devices have been registered by the same user. 4 3rd page portal brokers creating a pair of certificates and signing. It also automatically adjusts the network interface or WLAN profile in the settings listed on ise NSP as an admin user. On iOS, ISE uses iOS to achieve this and forces the user to go through a series of installations of iOS profiles. Depending on the iOS security settings, the user may be asked to enter an iOS PIN to trust the settings and profiles they've downloaded. Note: If a self-recall certificate is used, in connection with XXX, iOS 10.3 and above requires additional steps to trust the ISE certificate. For more information, please visit the app. 5 Once the board is successful, the user is sent back to the Safari browser. The last page of the portal notifies the user that the user must manually transfer to a secure SSID by moving to the settings. This is due to the iOS restriction because it does not automatically allow you to change SSID. Once connected to a secure SSID, the user can open the app or view it to another destination. Please note that the manual transition for SSID security is only required for iOS devices. Another OS can be switched automatically. ISE Live magazine Starting from below, the user is contacted by an open SSID, the user is unknown and identified as a mac address, as the user has not entered the user logs in the guest portal as a user of the Line only Endpoint ID represents CoA, which has been successful. Multiple CoA can be sent depending on the CoA settings to ensure a proper endpoint session is assigned showing the endpoint of the Authorization Profile has moved from Cisco_WebAuth to PermitAccess Top most lines points to a session that combines RADIUS authentication to information extracted from the radius accounting, which includes the end point of the IP address Using a self-recording certificate on ISE if ISE does not use a 3-point signed certificate , Apple iOS 11 and above does not allow the user to accept the registration profile without trusting the ISE certificate as a trusted CA. It is recommended to use an ISE certificate, which is already signed by a well-known CA, to avoid errors during the BYOD flow. In case ISE uses a certificate with self-signed, the user must manually entrust the certificate CA's root in iOS. This is done by tweaking iOS after step 4. Step Custom Experience Note 4a During the last thread step in one or double SSID thread described in previous steps, instead of succeeding in the training thread, the user will receive the next error page: Installing the Failed 4b profile On the iOS iOS iOS iOS iOS click click, go to the settings of the common qgt; about the zgt; the trust certificate settings. Turn on the trust of the certificate as a root CA by moving the options bar to the right and select Continue to accept changes 4c Click Home and open Safari and go through the BYOD stream again. This time the thread should be able to complete without error. Note: If the Retry button doesn't work, enter the external URL in the address rack to initiate the redirection. If the ISE certificate is signed by a well-known third party CA, and iOS10 users still get bugs, this may be due to CSCvk05778 'sISE BYOD with apple devices sending incorrectly ordered certificate chain'. To solve the problem, replace the existing 'USERTrust RSA Certificate Authority' with the one that follows: Device Managers through my Devices Portal My Devices Portal (MDP) can be used to control on-board devices, as well as manually add devices that cannot be on board through the NSP stream. Please note that there is no MDP policy and anyone with an account in a valid identification store can log into MDP. For example, if AD is enabled with MDP, anyone with AD credentials can log into the MDP to manage the endpoints. There are 5 states the device can be installed in my device portal State Status Registered EP has been through the BYOD stream (or NSP or MDP) and has now been registered (HAS has been seen online, a 20-minute delay from PENDING to register because it is done by MnT) While waiting for the EP has been via the BYOD stream (or NSP or MDP) and has now been registered BUT has not yet been seen on the network. A unregistered EP did not pass through the BYOD stream (this is the default for every endpoint in the system) The stolen EP status is changed to Stolen by the owner or administrator. When the device is identified as stolen, the system prevents the device from connecting to the network. Once restored, the status is returned to un-registered status and must be provided before it can connect to the network. For my devices, the device will need to be removed and re-added. Devices registered as stolen are assigned to the blacklist identification group. Lost EP status has been changed to Lost by the owner or administrator. When you identify a lost device when you identify a device as a stolen device, the system prevents the device from connecting to the network. Once restored, the status will return to the previous state before it is reported as Lost. Devices reported as Lost are classified as blacklisted. Manage isse-issued certificates from ISE Admin UI As In the previous section, ISSUED BYOD certificates can be recalled by the end user through MDP when the endpoint is marked as stolen. However, as an ISE administrator user, you can log into the admin's graphical interface, as well as manage endpoint certificates, as well as monitor the status of certificates. Cancel Cancel With the admin console go to the system of zgt; certificates of the Certificate Authority issued certificates, select the certificate that will be revoked, and click recall. The revoked certificate cannot be revoked, and if the endpoint must be re-issued, the user must go through the BYOD thread again. Please note that it takes 30 days for certificates to be revoked from GUI ISE. Managing expired certificates One of the advantages of using endpoint certificates for BYOD is that it is no longer associated with the username and password, which usually has a shorter password update cycle. However, certificates are also created with action dates that can affect access to the end point of the network. In general, it is recommended to provide enough time for the endpoint to live. For example, for clients with higher education, the administrator may set a 4-year endpoint certificate period to cover the student's endpoint at the time of enrollment, or the company may require certificates that will be valid for 2 years to fit the overall life cycle of mobile device purchases on the market. Too often, the requirement to update the BYOD certificate can increase the number of calls to the support base and add to the user's frustration. When dealing with expired or nearly expired certificates, ISE provides several options for solving the issue of renewal certificates. Condition policy: As part of the authentication, ISE can check how many days are left on the certificate that uses the endpoint. Based on the remaining days, ISE can force end users to renew certificates before expiration date. There are two conditions that can be used; CERTIFICATE: Days before expiration and CERTIFICATE: Expired. When allowing authentication of expired certificates, it's a good idea to always use CERTIFICATE: Is Expired in the authorization rule to restrict access to the network for expired certificates. Authorization Profile: The Display Certificate Renewal Messages check allows you to use the portal to renew certificates that the endpoint uses the Authorized Protocol: By default, Cisco ISE rejects a request that comes from a device whose certificate has expired. However, you can change this default behavior and set up ANE to handle such requests and encourage the user to renew the certificate. The EAP-TLS section in the permitted protocols includes an option that allows authentication for an expired certificate. This option is disabled by default because it is not safe to allow an overdue certificate, but if there is Allow an overdue certificate to authenticate, then this option can be enabled. However, when using this option, be sure to use Auth' in conjunction with this option to restrict access for users with an expired certificate. Note: Some devices allow you to renew certificates before and after they expire. But you can only update certificates on Windows devices Expires. Apple iOS, Mac OSX and Android devices allow you to renew certificates before or after they expire. Managing ISE Internal CA You need to back up time Cisco ISE CA certificates and keys securely to be able to recover them back to the secondary administration node in the event of a PAN failure, and you want to promote the secondary administration node to function as a root CA or intermediate CA external PKI. The Cisco ISE configuration backup does not include CA certificates and keys. Instead, you should use the Command Line Interface (CLI) to export CA certificates and keys to the repository and import them. The App Setting team includes export and import options to back up and restore CA certificates and keys. For more information on ISE Internal CA management, please review ise Administrator's Certificate Management Guide at Cisco ISE. ISE Reports Although not part of the reports, ISE Live magazine shows the live status of all authentication requests, including BYOD endpoints. Here you can confirm which policy corresponds to the end point. You can also control which columns are shown as well. Here various attributes can be turned on or disabled to show or can be pulled in a different order as well. ISE also includes several BYOD-related reports that can help in shooting out problems and understand BYOD endpoint stats. Here is a list of reports related to BYOD available to ISE 2.4. Note External Mobile Device Management report shows integration between ISE and external MDM. It also shows the endpoint status of ISE without logging on to the external MDM portal. Manual Certificates Combined Report, which tracks: Login Certificate Requests, made through the Registered Endpoints Displays Certificate Training portal, personal devices registered by employees. Supplicant Provisioning provides detailed information about the applicant and certificates provided on board to employees. My Devices Login and Audit Combined Report, which tracks: Log-up Device related operations performed by users in the MDP app This thread is similar to the double stream SSID, but instead of using the BYOD option in the guest portal, the BYOD portal is used for employees. Once an employee enters the guest portal, the user is presented with the BYOD portal based on the terms of the authorization. In the example below, the user group will be used to provide different BYOD portals. This example uses NAD settings and NSP settings in the main section of the document. Create End Groups Go to the Administration of the Identity Management group Click Endpoint identity groups on the left and click Add Add the name 'EP_Group_A' to the group and click Send Repeat above for 'EP_Group_B' Create a Group of Users Go to the Administration of the Identity Management group Click on Identification groups left on the left and click Add To Provide the name User_Group_A for the group and click Send Repeat above for 'User_Group_B' Create End Users Go to the Administration of qgt; Identity Management, Click on Users on the left and click Add 'User_A' for the name Provide Login Password Select 'User_Group_A' for user groups and click Send Repeat higher for 'User_B' when selecting 'User_Group_B' for user groups instead of creating ByOD portal Go to the work center of the gt; BYOD Portals and Components of the BYOD Portals Click on add use Portal_A as the name of the portal Expand 'Portal Settings' tab and select 'EP_Group_A' as a group identifying the endpoint click Save Repeat above for 'Portal_B' when selecting 'EP_Group_B' for as The Group Identification Endpoint Setting Guest Portal Go to guest portal that currently refers to the 'Cisco WebAuth' Authorization Profile (If it's a fresh ISE setup, then it should be a self-registered guest portal (default)) Go to work centers qgt; Guest Access's Portals and Components of the Guest Portals Click on the self-registered guest portal (default) Scroll down to BYOD Settings and click to make The Settings the success of authentication and click qgt;, to expand Select URL and enter www.cisco.com (Or any site that is marked DNS and on the trusted side of the network) Scroll up and Click Save Create Authorization Profiles Go to The Policy of the zgt; Results Click on Authorization Profiles Click Add 'BYOD_A' as the name Scroll down under the general tasks and check out 'Web Redirect' , MDM, NSP, CPP) Select Native Position Requester Enter ACL_WEBAUTH_REDIRECT as ACL Select Portal_A for the value Click Send Repeat higher for BYOD_B when choosing Portal_B to create a value policy Go to the policy of qgt; Policy sets click on "gt;' for the default policy set name Click on "gt;' for authorization policy to expand Click on cog for Wi-Fi_Guest_Access and select 'Duplicate Above' Rule Duplicate Name Change on Mouse Group_A Hover on terms for rule Group_A and click 'After the studio conditions, click on 'New' in the editor's box on the right Select Grey 'Choose to add the attribute 'Select'InternalUser' zgt; IdentityGroup Select 'User Identification Group 'User_Group_A' Click Use according to the results:Profile column for the rule Group_A click on x on PermitAccess, ask you to choose a new profile, select BYOD_A Repeat steps 4 - 12 for a rule called Group_B when using User_Group_B and BYOD_B instead of choosing Click on the status column for Employee_EAP-TLS, Group_A, Group_B, and Wi-Fi_Redirect_to_Guest_Login to include a set of Policy Rules Resemble the following dual-SSID stream with a separate Android device portal Another case of using a differentiated portal for Android devices. For Android BYOD, you must allow access to Google resources so that the user can download Android NSP. When the same portal is used for both guest users and BYOD employees on board, guest users will also have access to Google resources without logging in. To avoid this, a separate portal can be created for Android, so that only users of employees with Android devices going through BYOD will have access to Google resources. Create an Android logical profile Using a logical profile is necessary so that Android devices can be presented with the proper page for both the original guest portal and the BYOD portal for Android. Make sure to add all Android devices to profiling policies in your newly created logical profile. Go to the work centers of the profiler zgt; Profiling Policy Click on Logical Profiles on the left and click Add Add The Android Name-Logical Profile for the Name and select all Android devices from available policies and add them to the designated policies Click Send Note: Only one logical profile for all Android devices should be created instead of creating multiple logical profiles for individual devices provider Create byOD portal This Android-specific user portal. Go to the work center of the byt; BYOD Portals and Components of the BYOD Portals Click on Add Use Android_BYOD as the name of the portal Click Save Setting Guest Portal Go to the Guest Portal, which currently refers to the Cisco WebAuth Authorization Profile (If it is a fresh ISE installation, then it should be a self-registered guest portal (default)) Go to the work centers of the gt; guest access portals and guest access portals to BYOD Settings and click to expand Make sure employees to use personal devices on the network unverified Scroll down to 'Authentication Success Settings' and click to expand select URL and enter www.cisco.com (Or any site that is solvable DNS and on the trusted side of the network) Scroll up and click Save Create Authorization Profiles. Regular redirection of the ACL ACL_WEBAUTH_REDIRECT will allow access to the ISE portal. The ACL ACL_ANDROID system will allow access to the ISE portal as well as Google resources using the DNS ACL feature on WLC. Go to Politics's Elements of Politics Results Click Authorization (CWA, MDM, NSP, CPP) Select Native Requester Provision Enter 'Android_Redirect' as The Name Scroll Down according to General Tasks and Check 'Web Redirect' (CWA, MDM, NSP, CPP) Select Native Requester Providing ACL_ANDROID as ACL (This ACL should be pre-created on WLC) Select Android_BYOD for value value Send Create a Policy Go to The Politics Go to The Policy Sets Click on the default policy Set name Click on qgt; for authorization policy to expand Click on cog for Wi-Fi_Guest_Access and select Duplicate Above Duplicate Name Change Rules on Android_BYOD Mouse Hover on terms for Android_BYOD rule and click I Once in The Studio , click the New button in the editor's box on the right Select Grey 'Choose, to add the attribute 'EndPoints' to 'Gt; LogicalProfile Select ' Android-Logical-Profile' Click 'Use' Under the results: Column Profiles for the Android_BYOD click on 'x' on 'PermitAccess' when asking you to choose a new profile, select 'Android_Redirect' Click on the status column for 'Employee_EAP-TLS', 'Android_BYOD' and 'Fi_Redirect_to_Guest_Login' :