FAQ Cisco public

The bridge to possible

Cisco User Defined Network Plus

Q: What is Cisco User Defined Network Plus?

A: Cisco® User Defined Network Plus is a Cisco wireless solution that allows IT staff to give each user their very own network partition in an area or building with shared network resources. Users can remotely and securely register their devices on their own personal network. Perfect for university residence halls or extended healthcare stays, Cisco User Defined Network Plus provides the IT team with an easily deployed, managed, and monitored solution that reduces overall IT staff support for dorm connectivity, while simultaneously providing each user with their own personal, homelike network on shared WLAN resources.

Q: How does Cisco User Defined Network Plus work?

A: Users can register their devices remotely through a Splash Access registration page. With a link provided by the institution, the user accesses the Splash Access device registration web portal using a personalized URL to register the MAC addresses of their devices. Splash Access communicates with Cisco's Identity Services Engine (ISE) via pxGrid APIs and stores the MAC addresses in the ISE database. When the user's device connects and authenticates on the organization's Wi-Fi network with User Defined Network Plus enabled, that device is assigned to that specific user's segmented User Defined Network.

Q: What are some examples of areas where User Defined Networking Plus would provide a better user experience with the wireless network?

A: Some typical areas where User Defined Networking Plus would be beneficial include:

- Universities, specifically residential living or dormitories
- Senior living facilities
- Hotels
- Hospitals
- Research teams or departments
- Nonacademic business departments
- Convention centers
- Multitenant environments

Q: What components are needed to deploy this solution?

A: To deploy the User Defined Network Plus solution, we recommend having the following hardware installed: Cisco Catalyst™ 9800 Series Wireless Controllers and Catalyst 9100 Access Points (or Cisco Aironet® 802.11ac Wave 2 access points). All hardware should be updated to Cisco IOS® software version 17.3.1 IOS XE or above. Cisco ISE and Splash Access licenses are needed for the User Defined Networking Plus solution. Cisco Catalyst Center is optional for User Defined Network Plus.

Q: Will the customer need to pay for Splash Access?

A: Splash Access is an essential part of the User Defined Network Plus solution. Splash Access licenses are required and should be purchased. Request a demo account and a quote for Splash Access at https://www.splashaccess.com/udn-request/.

Q: Can you tell me a little more about the new solution with Splash Access?

A. Splash Access is an exclusive Cisco partner that also supplies the registration web portal for the equivalent Cisco Meraki™ solution, Meraki Wireless Personal Network (WPN). Cisco is simplifying and optimizing the on-premises User Defined Networking Plus solution to provide a common workflow regardless of our customers' management preferences, by using Splash Access for both solutions.

Q: What license type is needed to deploy this solution?

A: User Defined Network Plus requires Cisco DNA Advantage with ISE as well as licenses for Splash Access.

Q: What happens when the licenses expire?

A: On expiration of the Cisco DNA licenses, the customer can use the license evaluation period to renew the licenses. If the ISE licenses are active, User Defined Networking Plus will continue to function. If the ISE licenses are not renewed, or if the Splash Access licenses expire, the User Defined Networking Plus solution will not function, as these are critical components.

Q: What scale is supported with User Defined Network Plus?

A: User Defined Network Plus scale is defined by the scale of the Cisco Catalyst 9800 Series controller. Up to 64,000 UDNs are supported for the 9800 Series controller.

Q: Is intercontroller roaming supported?

A: No. Intercontroller roaming is not required.

Q: Are Flex and fabric deployments supported?

A: No. User Defined Network Plus is supported in Local mode access points only.

Q: What level of control does the network administrator have over the devices that users register?

A: Administrators can monitor the devices added by users via the Cisco Catalyst Center Assurance dashboard.

Q: Does User Defined Network Plus require all devices to be on the same SSID?

A: No. Devices using User Defined Network Plus can be on different types of SSID, such as PSK, 802.1X, or even an open SSID if these SSIDs are serviced by the same wireless controller.

Q: Will Cisco create a different SSID or password for all of a user's devices with Splash Access's registration portal?

A: No. Splash Access allows users to securely register their devices' MAC addresses. Once registered, when the device with that MAC address joins the UDN-enabled SSID, the network can group all the user's devices in their own segment so that their personal network or partition can restrict the mDNS and link-local multicast advertisements to those devices.

Q: Will registering with Splash Access automatically connect devices to the Wi-Fi network?

A: No. Splash Access is the registration portal for a user's devices. The device will need to connect to the Wi-Fi or the wireless network through the existing mechanisms already in place.

Q: Will this User Defined Network Plus function if we have mDNS or Universal Plug and Play (UPnP) gateways available in the network?

A: Both mDNS and UPnP gateways are used to advertise and proxy for the mDNS or UPnP across multiple local broadcast domains (VLANs). The User Defined Network Plus solution integrates with the mDNS gateway on the Cisco Catalyst 9800 Series Wireless Controller to provide the User Defined Network Plus functionality. It will operate with an external mDNS gateway. Catalyst 9800 Series Wireless Controllers do not support the UPnP gateway functionality, but the solution works with the UPnP devices in the same broadcast domain VLAN.

Q: Should I disable Peer-to-Peer (P2P) blocking on the wireless SSID?

A: Yes. For the wireless devices to talk to each other, P2P blocking should be disabled. However, the User Defined Network Plus solution offers a similar functionality that lets the administrator disable wireless devices that do not belong to a user to prevent them from talking to each other.

Q: How does User Defined Networking Plus enable secure onboarding and allow for increased protection?

A: **Security and visibility:** User Defined Network Plus enables users to onboard their own devices to the network while giving IT visibility using the wireless controller. Devices are registered with Splash Access, and the existing access policy, enforced by Cisco ISE, is applied. This improves the user experience without compromising protection or increasing organizational risk. Device onboarding is streamlined, policy provisioning is automated, and IT staff can control access to network resources.

Limit the blast radius: User Defined Network Plus confines a user's devices to their partition, separating each user's devices within the same domain. This reduces the attack surface, curtails ransomware spread, and quickens threat containment during security incidents. So, if a user clicks a malicious phishing email, the harmful traffic is confined to their device or network segment, preventing the threat from spreading.