Filtering for eduroam Devices

Table of Contents

ChromeBook Configuration for Eduroam

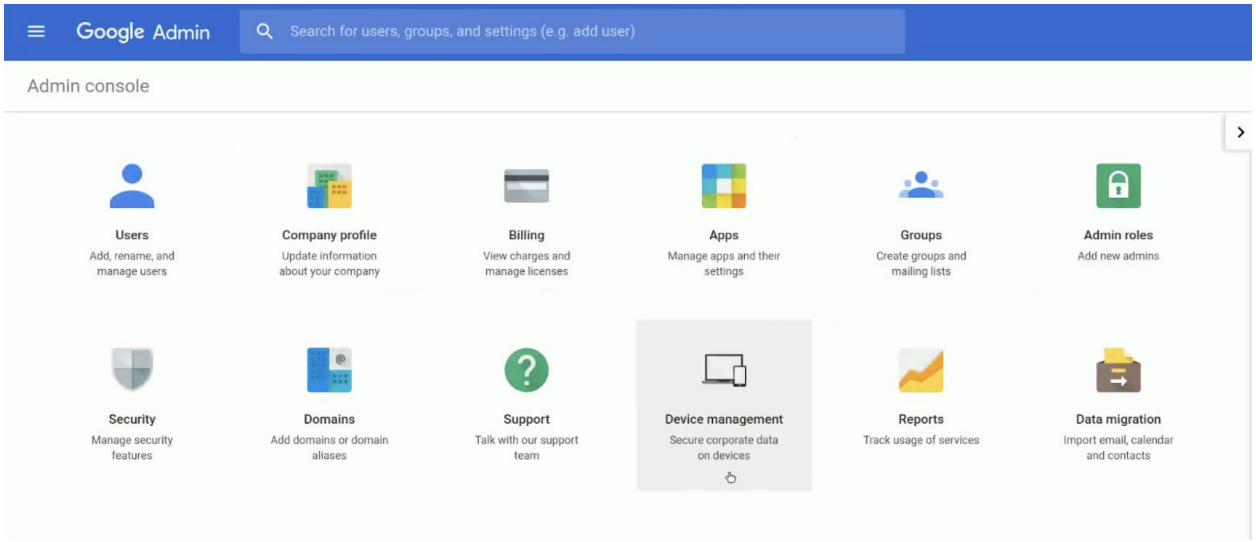
Last updated Feb 22, 2018
Research and testing by Scott Harpster and Josh Kleinke, SEDC
Editing by Pete Kruckenberg, UETN

This tutorial will guide you through configuring district-managed Chromebooks for use by students or staff on eduroam. Filtering is applied at the device using iBossConnect, and access to eduroam uses one set of (secret) credentials. Users are tracked by the Chromebook they are using per Google Admin console.

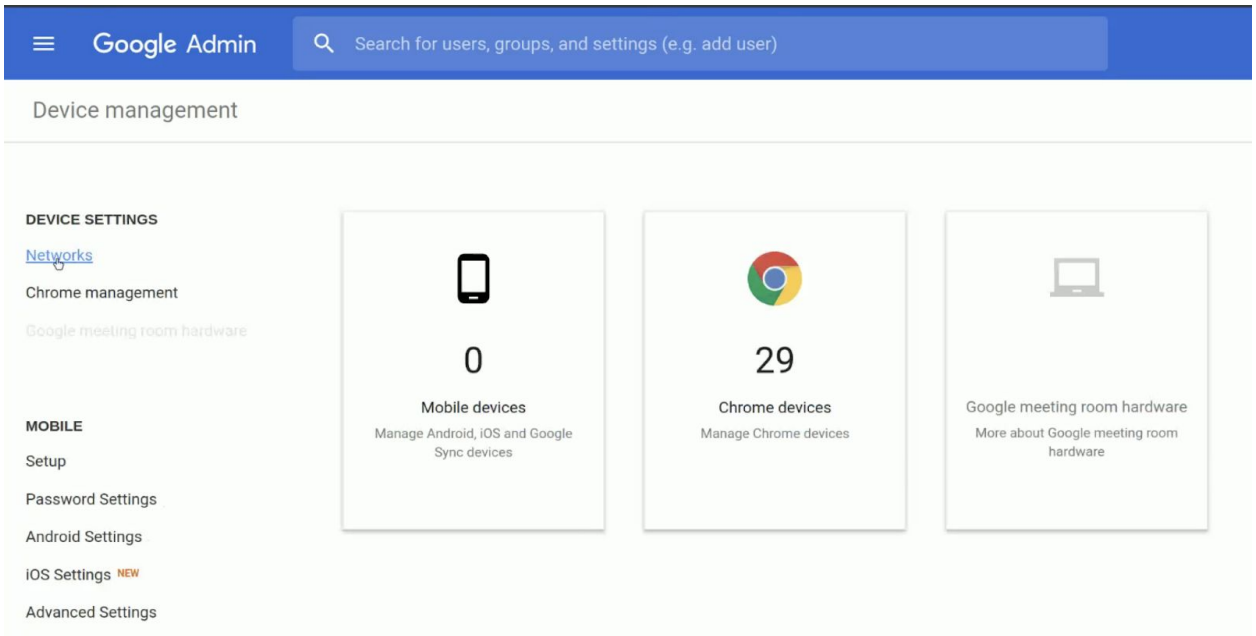
Possible future improvements:

- Use per-user credentials for eduroam, in some sort of automated fashion
- Use certificates (shared, or per-user) to increase authentication security
- Figure out how to have iBoss agent always connect to the home district iBoss, instead of automatically connecting to the local iBoss when visiting other districts

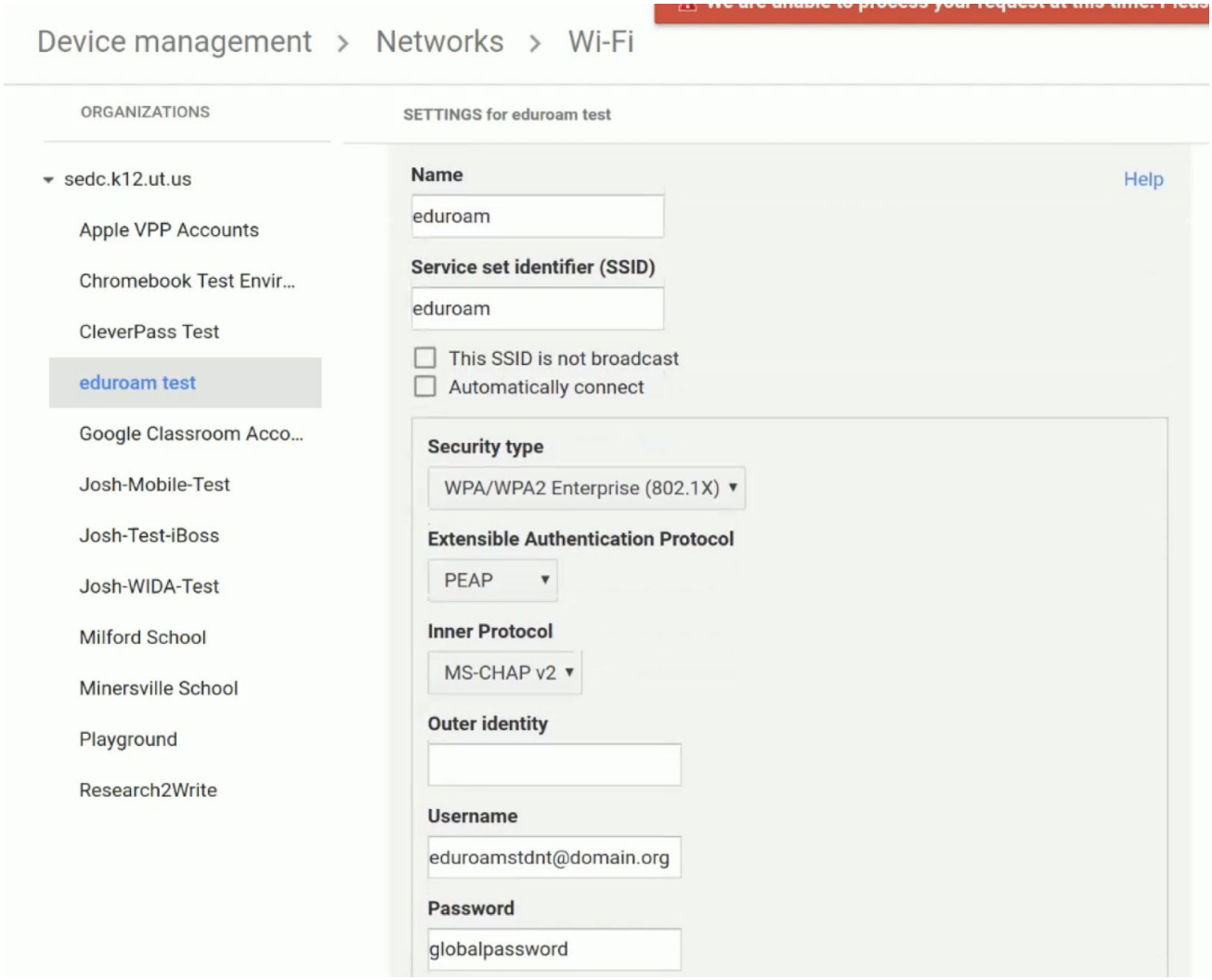
1. Open the Google Admin Console, go to *Device management*



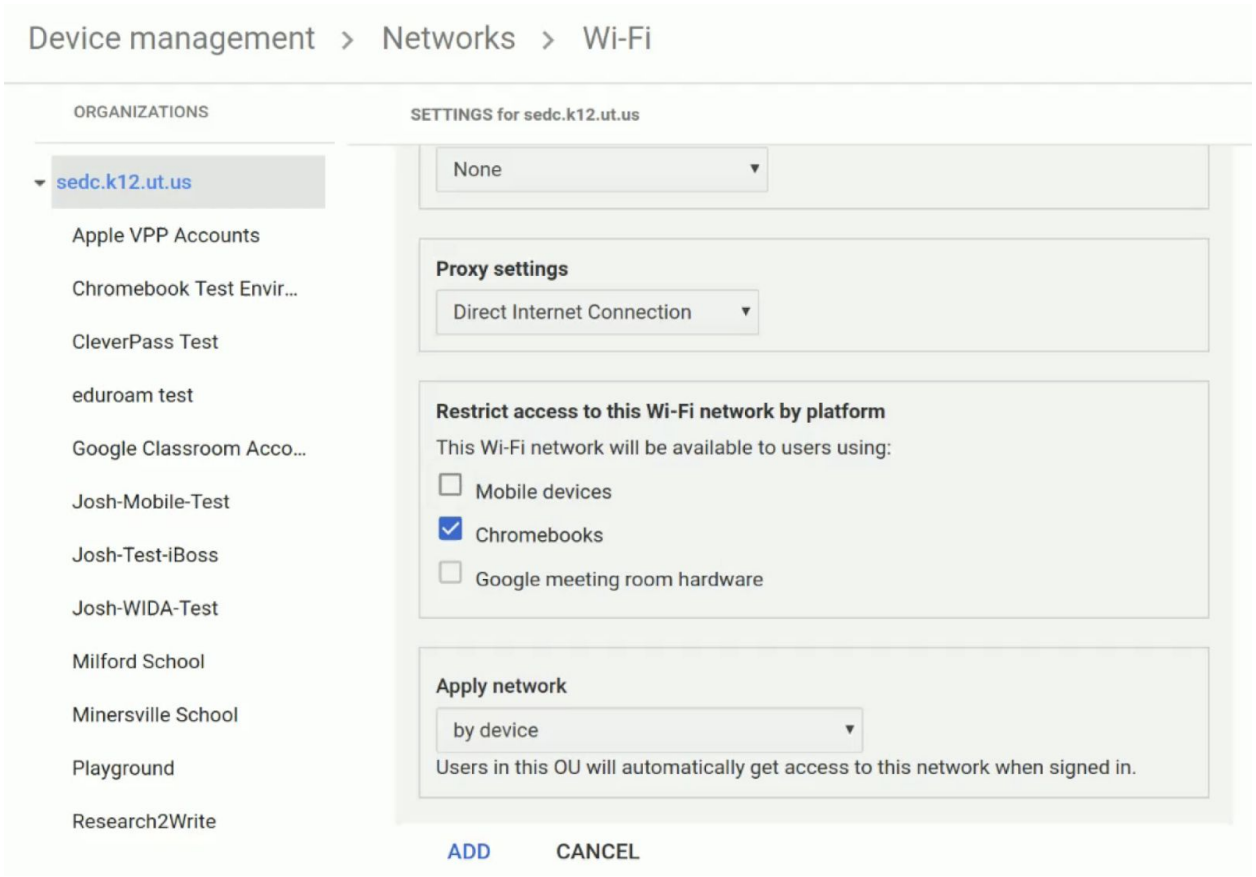
2. Choose *Device Settings* > *Networks*



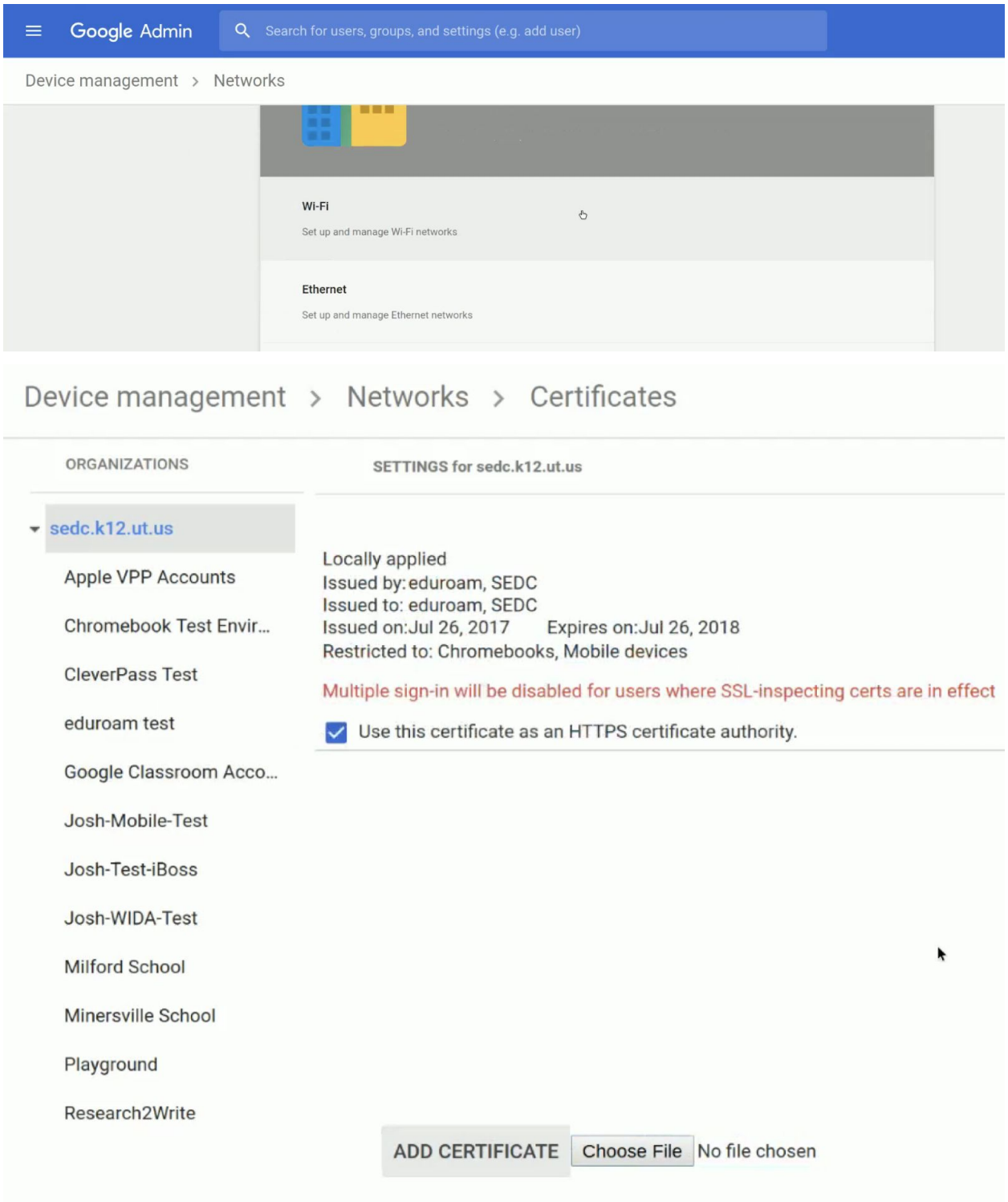
3. Select or add the *eduroam* network. Configure the Security Type, Extensible Authentication Protocol, Inner Protocol, Username and Password. In this tutorial, the same eduroam credentials (which should be kept secret) are used for all Chromebooks, and users are identified by the Chromebook they are using through Google Admin console.



4. Restrict access to eduroam to Chromebooks only. This allows students to only use Chromebooks to access eduroam, it will not be accessible from their mobile phones or other unfiltered devices.



5. If you are using your own encryption certificate (used to encrypt 802.1x authentication), you will need to install your certificate on the Chromebooks. Some platforms do not work well with private certificates, so it is recommended to purchase a certificate from a certificate authority.



6. Install and configure iBossConnect Chromebook filtering software per these instructions https://drive.google.com/open?id=1n4wqRPDBtyRRxehBPeed5KDhkUNGjkrE

Note that the iBossConnect software automatically tries to find a local iBoss appliance, before it connects to the home iBoss appliance. When a Chromebook is used in another school district, the iBoss agent may connect to that district's iBoss appliance, instead of connecting to the home district iBoss appliance.

Setting up iBoss to Filter Windows Devices Connected on Eduroam

Last updated Dec 18, 2018
Research and testing by Jason Eyre, Murray School District
Editing by Pete Kruckenberg, UETN

This tutorial will guide you through configuring district-managed Windows computers for use by staff on Eduroam. Filtering is applied at the device using iBossConnect.

Prerequisites for iBoss:

- iBoss server has to be set up to proxy external traffic (get screenshot, maybe make a recipe for iBoss configuration)

iBoss server has to have a public IP address to listen on, that's externally-accessible

- Under Network > Advanced Settings > General Settings (screenshot "pete1", includes breadcrumbs)
- UDP ports 8025, 8026 (configurable) open externally on a static IP address (firewall needs to be open, needs to be assigned a public IP address and possibly static-NAT'd)
- iBoss agent includes a key for auth. Key can be different for different groups (default, student, staff)

<u>Windows</u>
Download Windows agent
Extract agent
Includes multiple installers, for 32-bit and 64-bit, windows 8
Orca tool - lets you edit the installer, change Properties to set different configuration options for the iBoss agent (ports, IP address/DNS, group key, etc)

- PARAM_OVERRIDE_SETTINGS (default off, recommended enabled "1") allows changes to be pushed dynamically from the iBoss server
- PARAM_GATEWAY_HOST - by default will be a specific iBoss, but can reset to point to a VIP for load-balancing or redundancy
- (would be good to collect people's recommendations for Property settings and other installer settings)

Does Agent read username from windows?
Add installer to whatever deployment system (such as AD Group Policy)

Mac

Generates a pkg file and certificated