

# Filtering for eduroam Devices

## Table of Contents

ChromeBook Configuration for Eduroam	2
Setting up iBoss to Filter Windows Devices Connected on Eduroam	8

# ChromeBook Configuration for Eduroam

Last updated Feb 22, 2018

Research and testing by Scott Harpster and Josh Kleinke, SEDC

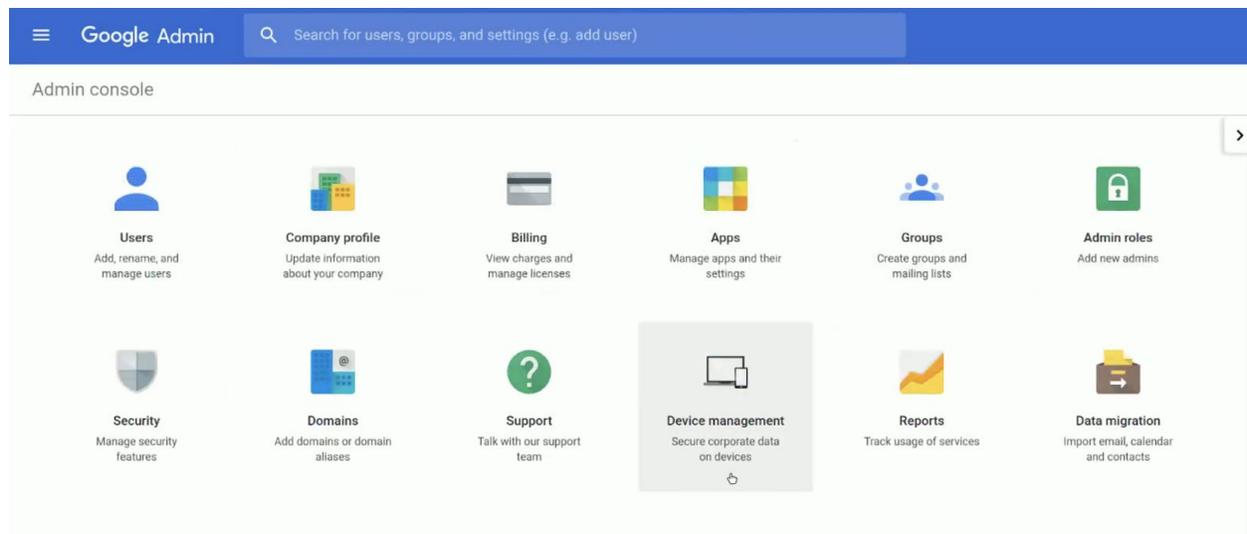
Editing by Pete Kruckenberg, UETN

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*

The screenshot displays the Google Admin console interface. At the top, there is a blue header with the Google Admin logo and a search bar. Below the header, the page title is "Device management". The main content area is divided into a left sidebar and a central grid of three device management cards.

**Left Sidebar:**

- DEVICE SETTINGS**
  - [Networks](#)
  - Chrome management
  - Google meeting room hardware
- MOBILE**
  - Setup
  - Password Settings
  - Android Settings
  - IOS Settings **NEW**
  - Advanced Settings

**Central Grid:**

- Mobile devices:** Represented by a smartphone icon, showing a count of 0. Description: "Manage Android, iOS and Google Sync devices".
- Chrome devices:** Represented by the Chrome logo, showing a count of 29. Description: "Manage Chrome devices".
- Google meeting room hardware:** Represented by a laptop icon, showing a count of 0. Description: "More about Google meeting room hardware".

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.

The screenshot shows the Google Admin console interface for configuring a Wi-Fi network. The breadcrumb navigation at the top reads "Device management > Networks > Wi-Fi". A red error banner at the top right states "We're unable to process your request at this time. Help".

The main content area is divided into two sections: "ORGANIZATIONS" on the left and "SETTINGS for eduroam test" on the right.

**ORGANIZATIONS:** A list of organizations is shown under "secd.k12.ut.us". The "eduroam test" organization is selected and highlighted in blue. Other organizations listed include Apple VPP Accounts, Chromebook Test Envir..., CleverPass Test, Google Classroom Acco..., Josh-Mobile-Test, Josh-Test-iBoss, Josh-WIDA-Test, Milford School, Minersville School, Playground, and Research2Write.

**SETTINGS for eduroam test:**

- Name:** eduroam
- Service set identifier (SSID):** eduroam
- This SSID is not broadcast
- Automatically connect
- Security type:** WPA/WPA2 Enterprise (802.1X)
- Extensible Authentication Protocol:** PEAP
- Inner Protocol:** MS-CHAP v2
- Outer identity:** (empty field)
- Username:** eduroamstdnt@domain.org
- Password:** globalpassword

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.

Device management > Networks > Wi-Fi

---

ORGANIZATIONS

- ▼ **sedc.k12.ut.us**
- Apple VPP Accounts
- Chromebook Test Envir...
- CleverPass Test
- eduroam test
- Google Classroom Acco...
- Josh-Mobile-Test
- Josh-Test-iBoss
- Josh-WIDA-Test
- Milford School
- Minersville School
- Playground
- Research2Write

SETTINGS for sedc.k12.ut.us

None ▼

**Proxy settings**

Direct Internet Connection ▼

**Restrict access to this Wi-Fi network by platform**

This Wi-Fi network will be available to users using:

- Mobile devices
- Chromebooks
- Google meeting room hardware

**Apply network**

by device ▼

Users in this OU will automatically get access to this network when signed in.

[ADD](#) [CANCEL](#)

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.

The screenshot shows the Google Admin console interface. At the top, there is a blue header with the Google Admin logo and a search bar. Below the header, the breadcrumb navigation shows 'Device management > Networks'. The main content area is divided into two sections: 'Wi-Fi' and 'Ethernet', each with a sub-header and a description. Below this, the breadcrumb navigation changes to 'Device management > Networks > Certificates'. The 'CERTIFICATES' section is split into two columns: 'ORGANIZATIONS' on the left and 'SETTINGS for sedc.k12.ut.us' on the right. The 'ORGANIZATIONS' column lists various organizations, with 'sedc.k12.ut.us' selected. The 'SETTINGS' column shows details for a locally applied certificate, including its issuer, recipient, issue and expiration dates, and restrictions. A red warning message is displayed below the certificate details. At the bottom, there is a button labeled 'ADD CERTIFICATE' and a file selection interface with 'Choose File' and 'No file chosen' options.

Google Admin

Search for users, groups, and settings (e.g. add user)

Device management > Networks

Wi-Fi  
Set up and manage Wi-Fi networks

Ethernet  
Set up and manage Ethernet networks

Device management > Networks > Certificates

ORGANIZATIONS

SETTINGS for sedc.k12.ut.us

▼ sedc.k12.ut.us

- Apple VPP Accounts
- Chromebook Test Envir...
- CleverPass Test
- eduroam test
- Google Classroom Acco...
- Josh-Mobile-Test
- Josh-Test-iBoss
- Josh-WIDA-Test
- Milford School
- Minersville School
- Playground
- Research2Write

Locally applied  
Issued by: eduroam, SEDC  
Issued to: eduroam, SEDC  
Issued on: Jul 26, 2017 Expires on: Jul 26, 2018  
Restricted to: Chromebooks, Mobile devices

Multiple sign-in will be disabled for users where SSL-inspecting certs are in effect

Use this certificate as an HTTPS certificate authority.

ADD CERTIFICATE Choose File No file chosen

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)

## Windows

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