

## Smart Proxy - Bug #12578

### Smart-Proxy doesn't enforce ciphersuite ordering

11/24/2015 04:15 AM - Brandon Weeks

<b>Status:</b> Closed	
<b>Priority:</b> Normal	
<b>Assignee:</b> Brandon Weeks	
<b>Category:</b> SSL	
<b>Target version:</b> 1.10.1	
<b>Difficulty:</b>	<b>Fixed in Releases:</b>
<b>Triaged:</b>	<b>Found in Releases:</b> Nightly
<b>Bugzilla link:</b>	<b>Red Hat JIRA:</b>
<b>Pull request:</b> <a href="https://github.com/theforeman/smart-proxy/pull/348">https://github.com/theforeman/smart-proxy/pull/348</a>	
<b>Description</b>	
The SSL settings don't enforce ciphersuite ordering, which may allow the clients to make worse decisions about ciphersuite selection or maliciously downgraded. Enabling the 'SSLHonorCipherOrder' or 'ssl_prefer_server_ciphers' settings for Apache or Nginx is considered a best practice.	

#### Associated revisions

Revision [ec99de99](#) - 11/24/2015 07:19 AM - Brandon Weeks

Fixes #12578 - set SSL\_OP\_CIPHER\_SERVER\_PREFERENCE

#### History

**#1 - 11/24/2015 04:25 AM - The Foreman Bot**

- Status changed from New to Ready For Testing
- Assignee set to Brandon Weeks
- Pull request <https://github.com/theforeman/smart-proxy/pull/348> added

**#2 - 11/24/2015 08:01 AM - Brandon Weeks**

- Status changed from Ready For Testing to Closed
- % Done changed from 0 to 100

Applied in changeset [ec99de9917fcc7ba6e1595d85d508245a3ff6695](#).

**#3 - 11/24/2015 08:08 AM - Dominic Cleal**

- translation missing: en.field\_release set to 104