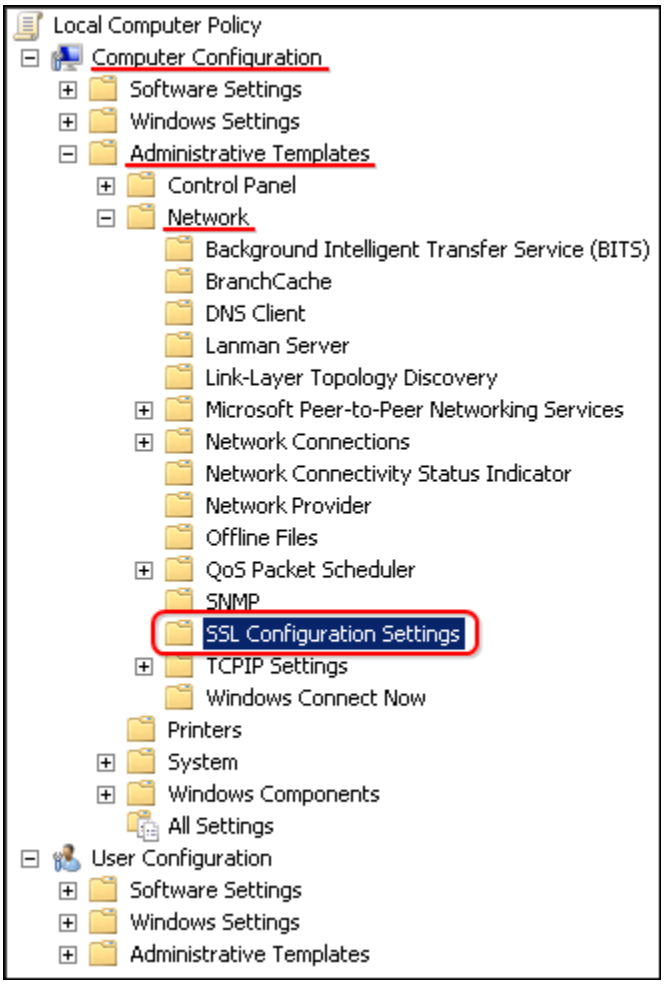
Upgrade Cipher Suite

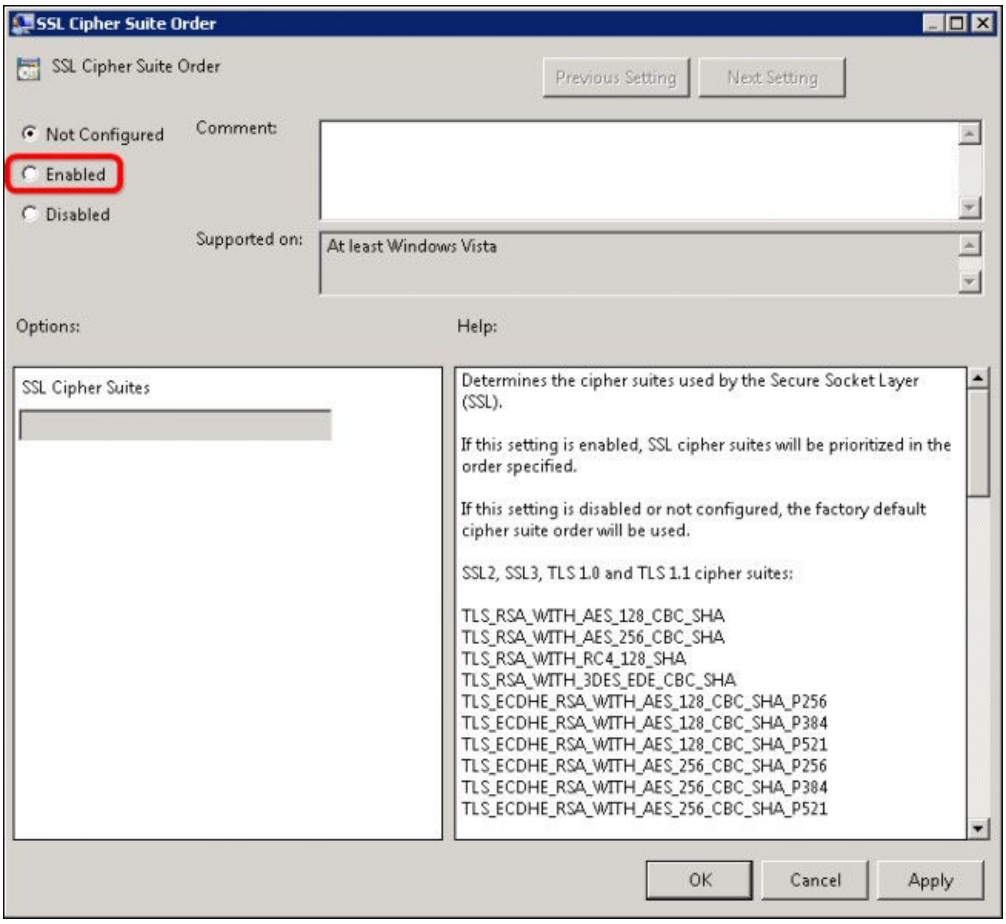
Nâng cấp bộ cipher của Windows không thực sự thấy ngay được sự cần thiết, tuy nhiên nó hoàn toàn không khó.

Đầu tiên, nhấn tổ hợp phím Windows+ R để mở hộp thoại "Run". Gõ "gpedit.msc" và bấm "OK" để mở Group Policy Editor. Đây là nơi chúng ta sẽ thực hiện nâng cấp.

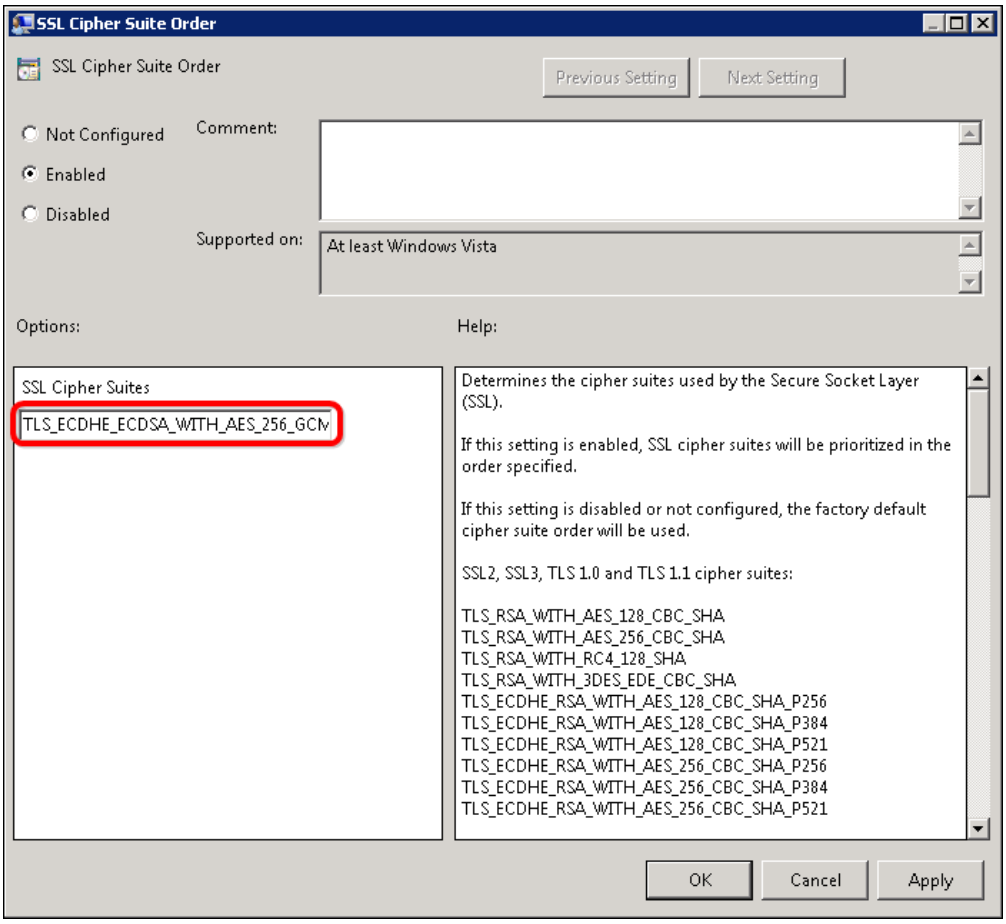


Ở phía bên trái, mở Computer Configuration, Administrative Templates, Network, và chọn SSL Configuration Settings.

Ở phía bên phải, nháy đúp vào SSL Cipher Suite Order.



Mặc định, lựa chọn “Not Configured” được sử dụng. Chọn sang “Enabled” để thay đổi server’s Cipher Suites.



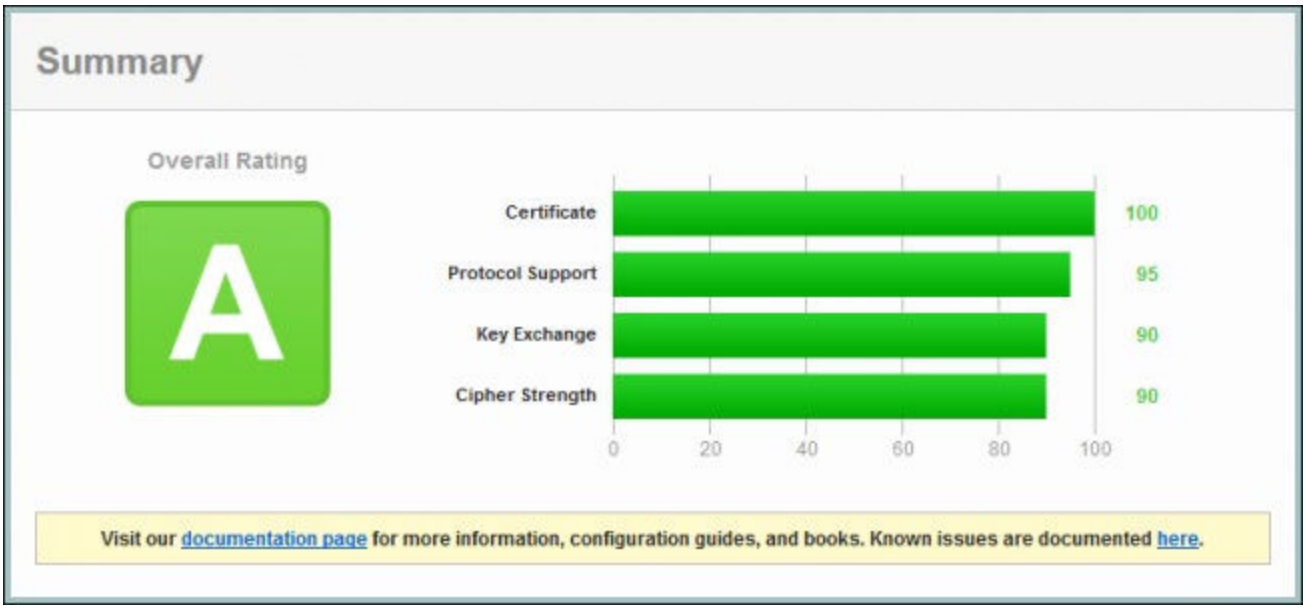
Trường SSL Cipher Suites sẽ được điền thông tin các cipher ngay khi nhấn vào.Nếu bạn muốn xem những bộ cipher nào đang được sử dụng, copy lại nội dung trong trường SSL Cipher Suites và paste chúng ra notepad. Nội dung này được viết trên 1 dòng, mỗi cipher sẽ được phân tách nhau bằng dấu phẩy.

Bạn có thể xem qua toàn bộ danh sách, thêm bớt các bộ cipher, tuy nhiên danh sách không được vượt quá 1023 ký tự. Điều này khá khó chịu bởi nhiều bộ cipher có tên rất dài như "TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384_P384", vì vậy, hãy chọn thật cẩn thận. Chúng tôi đề xuất sử dụng danh sách sau:

```
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384_P384,
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA_P384,
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA_P384,
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA_P256,
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA_P256,
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256_P384,
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256_P384,
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256_P256,
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256_P256,
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA_P384,
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA_P256,
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P384,
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P256,
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256_P384,
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256_P256,
TLS_DHE_DSS_WITH_AES_256_CBC_SHA256,
TLS_DHE_DSS_WITH_AES_256_CBC_SHA,
TLS_DHE_DSS_WITH_AES_128_CBC_SHA256,
TLS_DHE_DSS_WITH_AES_128_CBC_SHA,
TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA,
TLS_RSA_WITH_AES_256_CBC_SHA256,
TLS_RSA_WITH_AES_256_CBC_SHA,
TLS_RSA_WITH_AES_128_CBC_SHA256,
TLS_RSA_WITH_AES_128_CBC_SHA,
TLS_RSA_WITH_3DES_EDE_CBC_SHA,
SSL_CK_DES_192_EDE3_CBC_WITH_MD5
```

Khi đã chọn được danh sách bộ cipher của mình, bạn cần điều chỉnh lại đúng dạng như danh sách gốc, mỗi bộ cipher phân cách nhau bằng dấu phẩy. Copy đoạn danh sách đã được định dạng lại và paste vào trường SSL Cipher Suites và nhấn OK. Cuối cùng, để áp dụng thay đổi, bạn phải khởi động lại server.

Sau khi khởi động lại, bạn có thể vào SSL Labs để kiểm tra, nếu mọi thứ hoạt động tốt, kết quả sẽ đạt điểm A.


Summary
Overall Rating
A
Certificate
100
Protocol Support
95
Key Exchange
90
Cipher Strength
90
0
20
40
60
80
100
Visit our documentation page for more information, configuration guides, and books. Known issues are documented here.