

Blocking Tainted Browser Extensions

The Service Delivery Team has implemented Jamf and SCCM configurations to block tainted browser extensions on our managed machines. We are sharing these configurations here in case Departmental IT administrators may find them helpful.

Windows

Foundations Services Windows customers can use the Group Policy Management tool to link the Policy named "Foundation Services.Edge.Chrome.BlockExtensionList" to the Organization units (OU) where customers would like to block ISO-recommended Google Chrome Web Store extensions in the Chrome and Microsoft Edge browsers.

MacOS

To block the five Chrome extensions in Jamf for the Macs, you will need a Configuration Profile for Chrome applied to the hosts in your site.

Under Configuration Profiles > New

Give it a name, assign it a Category from your site, set Level > Computer Level, Distribution Method > Assign Automatically

For Scope, target all computers or if you have a smart group for hosts with Chrome installed, etc.

For the payload, go to Application & Custom Settings, select Upload

Under Upload, set the Preference Domain to com.google.Chrome

Under Property List you can use the following:

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN"
"http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
  <dict>
    <key>AllowOutdatedPlugins</key>
    <false/>
```

```

<key>DefaultBrowserSettingEnabled</key>
<false/>
<key>MetricsReportingEnabled</key>
<false/>
<key>ExtensionInstallBlocklist</key>
<array>
  <string>mnhffkhmpnefgkIngfmlndmkimimbphc</string>
  <string>bbdnohkpnbkdkmnkddobeafboooipla</string>
  <string>bibjgkidgpfbbllifamdldlhghimfohh</string>
  <string>pkgciiiancapdlpcbppfkmeaieppikkk</string>
  <string>epdjhgbiipbbhoccdeipghoihibnfja</string>
</array>
<key>updatePolicies</key>
<dict>
  <key>global</key>
  <dict>
    <key>UpdateDefault</key>
    <integer>1</integer>
    <key>UpdatesSuppressedDurationMin</key>
    <integer>960</integer>
    <key>UpdatesSuppressedStartHour</key>
    <integer>16</integer>
    <key>UpdatesSuppressedStartMin</key>
    <integer>30</integer>
  </dict>
</dict>
</dict>
</plist>

```

The part in this that blocks the extensions is the following:

```

<key>ExtensionInstallBlocklist</key>
<array>
  <string>mnhffkhmpnefgkIngfmlndmkimimbphc</string>
  <string>bbdnohkpnbkdkmnkddobeafboooipla</string>
  <string>bibjgkidgpfbbllifamdldlhghimfohh</string>
  <string>pkgciiiancapdlpcbppfkmeaieppikkk</string>
  <string>epdjhgbiipbbhoccdeipghoihibnfja</string>
</array>

```

Those strings match the IDs of the five listed extensions. The rest of the settings can be tailored to your preference. If you wish or are requested to block other extensions, you can simply add another string here with the extension ID to block it.