**Important Security Update for Cisco WebEx Locked Down Customers**

**Dear Cisco WebEx Customer,**

Cisco is committed to the security of all Cisco WebEx services and continues to invest in it by providing timely security enhancements, including those which require meeting client downloads and/or updates to Cisco applications and APIs.

We strive to limit business impact to our valued customers whenever possible by providing advanced notifications that include time to align with any required updates. Cisco intends to maintain a vigilant approach toward maintaining the security of our SaaS offerings. Customers can expect future security enhancements to be delivered as often as deemed necessary.

As part of Cisco’s commitment to security, we are rolling out several changes in our environment. In order for these security enhancements to take effect, we require all customers who are using **older versions** of the Cisco applications **listed below to upgrade to the minimum version** **prior to December 5th, 2014**. To limit end user impacts please communicate this change to users who may not be using one of the versions listed below. If any of the following applications are **not in use** by your organization **or if you are currently running the minimum version** then no further action is required.

**UPCOMING WEBEX CLIENT UPDATES**

Security changes impacting Cisco WebEx desktop clients will take effect on **December 5, 2014.**

WebEx sites that are locked down on WBS27 or WBS28 releases must be upgraded to the corresponding desktop clients for the latest WebEx release **prior to December 5, 2014.**

To provide a smooth transition, please contact your Customer Success Manager to coordinate your site upgrade to one of the latest releases shown below as soon as possible. Upgrades can be scheduled to occur as of September 17, 2014.

* **WBS28.12EP19 or higher**
* **WBS27LDSP32EP35**

**UPDATES TO CISCO APPLICATIONS**

On **December 5, 2014,** Cisco WebEx will apply security changes to the applications listed below. After the update, applications older than the minimum version will not function properly. Users should upgrade applications to the minimum version prior to **December 5, 2014**to avoid potential impacts. Basic functionality like starting or joining meetings may be affected for applications which are not updated. Download links for WebEx mobile applications can be found here<http://www.webex.com/products/web-conferencing/mobile.html>

|  |  |  |
| --- | --- | --- |
| **Applications** | **Minimum Version** | **Download Location** |
| **Cisco WebEx Meetings for Apple iPad and iPhone** | 5.1 | Apple App Store |
| **Cisco WebEx Meetings for Android** | 4.0 | Google Play |
| **Cisco WebEx Meetings for Microsoft® Windows Phone® 8** | 2.1 | Microsoft Windows® App Store |
| **Cisco WebEx Meetings for BlackBerry** | 3.0 | BlackBerry App world |
| **Cisco Jabber for iPhone and iPad** | 9.6.2 | Apple App store |
| **Cisco Jabber for Android** | 9.6.1 | Google Play |
| **Cisco Jabber Video for iPad** | 9.3.6 | Apple App store |
| **Cisco Jabber for Apple Mac** | 9.6.0 | Org Admin |
| **Cisco Jabber for Windows** | 9.7.4 (for 9.7 release) | Org Admin |
| **Cisco Jabber for Windows** | 9.6.3 (for 9.6 release) | Org Admin |
| **Cisco Jabber for Windows** | 9.2.7 \* (for 9.2 release) **See Note Below** | Org Admin |
| **Cisco WebEx Connect** | Cisco.com |  |
| **Cisco Unified Personal Communicator** | 8.6.4 | [Cisco.com](http://software.cisco.com/download/type.html?mdfid=280455801&flowid=45924&softwareid=282074306) |

**Note:** At this time Cisco Jabber 9.2.x customers are requested to upgrade to Cisco Jabber 9.6.3 or 9.7.4 for full compliance. Alternatively, customers can upgrade to 9.2.7 for mandatory security compliance, but the WebEx Audio Conference functionality in Jabber will not work in this case.

**All  CISCO WEBEX CENTERS – SECURITY ENHANCEMENT AVAILABLE**

* **Cisco WebEx Meeting Center**
* **Cisco WebEx Training Center**
* **Cisco WebEx Event Center**
* **Cisco WebEx Support Center**

**STRONG USER PASSWORD**

* **Strong User Password** – Functionality is available from the site administration page to give administrators the option to **enable strong password requirements** for their users at any time. Cisco WebEx recommends sites take advantage of this functionality to help protect against unauthorized access to meetings and information.  For more information refer to [**WBX48733: How Do I Edit Strong Password Criteria** **in Site Admin**](http://kb.webex.com/WBX48733) found in the Cisco WebEx Knowledge Base.