Engineering Advisory 74074

Security Advisory on Vulnerability with the SIP Registration Credentials

This engineering advisory describes a security vulnerability in certain releases of the Polycom® UC Software with the SIP registration credentials on the Polycom phones.

This engineering advisory applies to Polycom® SoundPoint® IP, SoundStation® IP, and VVX® 1500 phones running Polycom UC Software 3.3.2 and SoundPoint® IP phones and SpectraLink® 8400 Series handsets running UC Software 4.0.0.

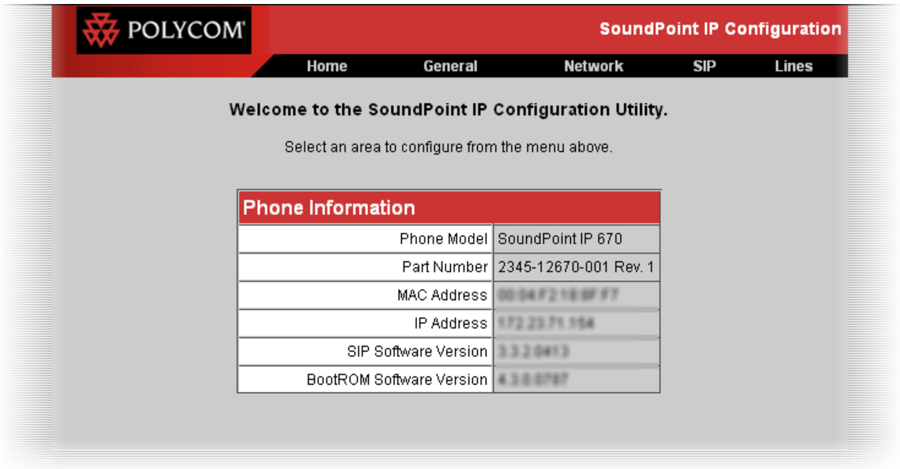
Identifying the Issue

When your Polycom phones are running UC Software 3.3.2 or 4.0.0, anyone who knows the administrative password can log in and access the phone's web interface.

If users view the page source from a browser or 'sniff' the browser traffic from the phone, they will see the password fields in clear text. All password fields should appear as ????.

Phones Running UC Software 3.3.2

If users log into the phone's web interface with the administrative password and the phone is running UC Software 3.3.2, the following page will display in the browser.

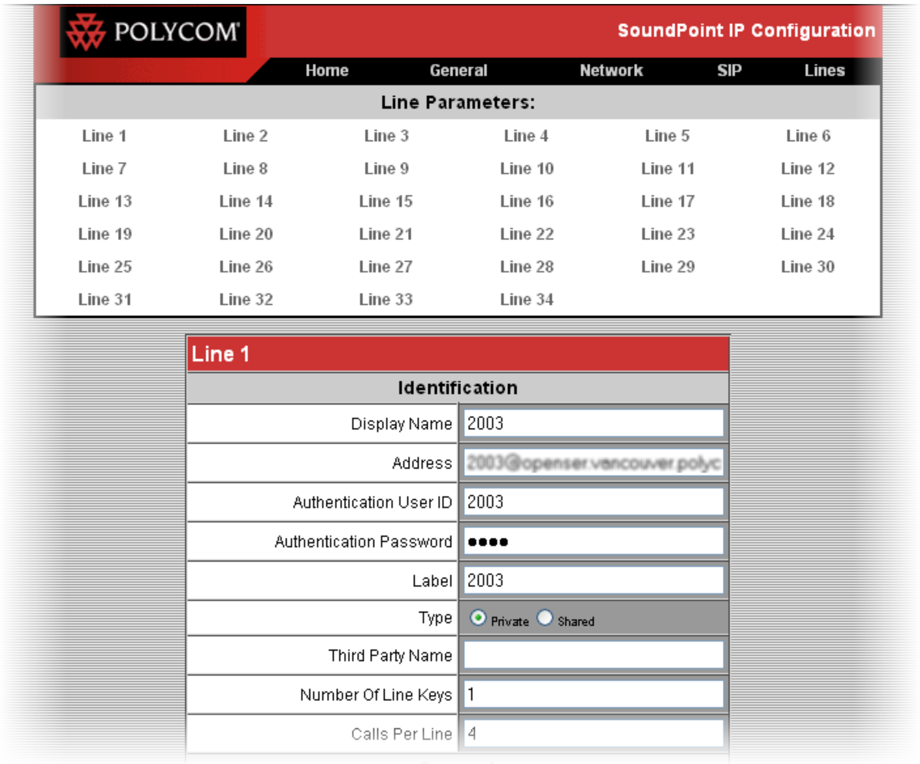


Welcome to the SoundPoint IP Configuration Utility.

Select an area to configure from the menu above.

Phone Information	
Phone Model	SoundPoint IP 670
Part Number	2345-12670-001 Rev. 1
MAC Address	[redacted]
IP Address	[redacted]
SIP Software Version	[redacted]
BootROM Software Version	[redacted]

If users navigate to the Lines page, the following page will display in the browser.



Line Parameters:

Line 1	Line 2	Line 3	Line 4	Line 5	Line 6
Line 7	Line 8	Line 9	Line 10	Line 11	Line 12
Line 13	Line 14	Line 15	Line 16	Line 17	Line 18
Line 19	Line 20	Line 21	Line 22	Line 23	Line 24
Line 25	Line 26	Line 27	Line 28	Line 29	Line 30
Line 31	Line 32	Line 33	Line 34		

Line 1

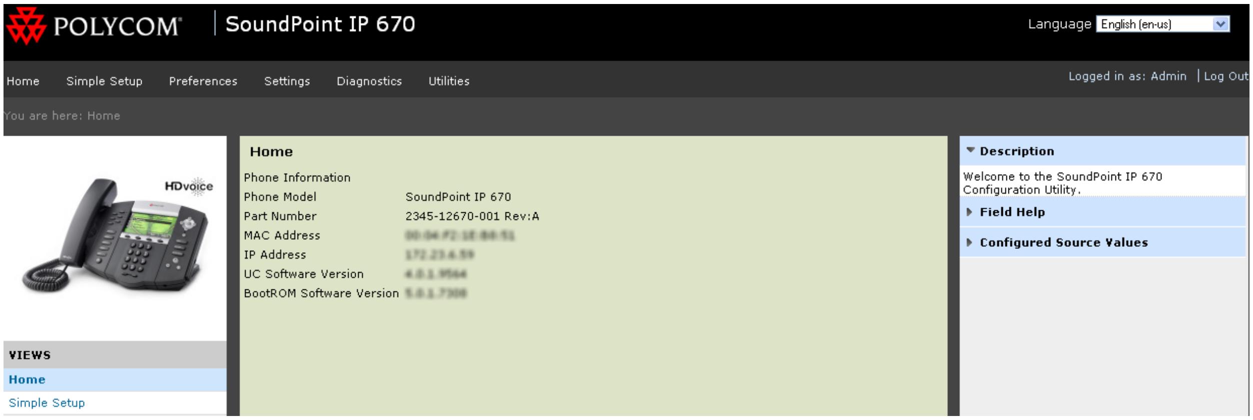
Identification

Display Name	2003
Address	[redacted]
Authentication User ID	2003
Authentication Password	●●●●
Label	2003
Type	● Private ○ Shared
Third Party Name	
Number Of Line Keys	1
Calls Per Line	4

If users view the page source from a browser, they will see the password fields in clear text.

Phones Running UC Software 4.0.0

If users log into the Web Configuration Utility with the administrative password and the phone is running UC Software 4.0.0, the following page will display in the browser.

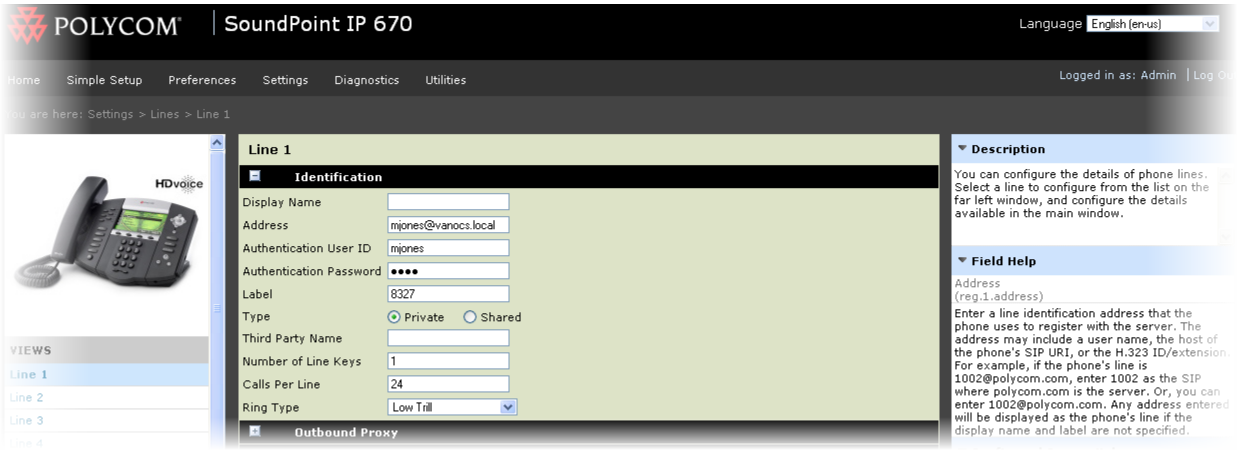


Home

Phone Information	
Phone Model	SoundPoint IP 670
Part Number	2345-12670-001 Rev:A
MAC Address	[redacted]
IP Address	[redacted]
UC Software Version	[redacted]
BootROM Software Version	[redacted]

Welcome to the SoundPoint IP 670 Configuration Utility.

If users navigate to the **Settings > Lines** page, the following page will display in the browser.



Line 1

Identification

Display Name	
Address	mjones@vanocs.local
Authentication User ID	mjones
Authentication Password	••••
Label	8327
Type	● Private ○ Shared
Third Party Name	
Number of Line Keys	1
Calls Per Line	24
Ring Type	Low Trill

Outbound Proxy

Description

You can configure the details of phone lines. Select a line to configure from the list on the far left window, and configure the details available in the main window.

Field Help

Address
(reg.1.address)

Enter a line identification address that the phone uses to register with the server. The address may include a user name, the host of the phone's SIP URI, or the H.323 ID/extension. For example, if the phone's line is 1002@polycom.com, enter 1002 as the SIP where polycom.com is the server. Or, you can enter 1002@polycom.com. Any address entered will be displayed as the phone's line if the display name and label are not specified.

If users view the page source from a browser, they will see the password fields in clear text.

Admin Tip: Using HTTPS Access

If you require the use of a secure tunnel to access the Web Configuration Utility, the vulnerability is removed.

Workaround

To work around this issue, do one of following:

1. Disable the web interface. This solves both the page source viewing issue and the 'sniffing' issue.

   To disable the web interface, set `httpd.cfg.enabled` to 0.

   For more information on changing configuration parameters, see the *Polycom UC Software 3.3.0 Administrator's Guide* or the *Polycom UC Software 4.0.1 Administrator's Guide*.

2. Change the administrative password from the default. This means only authorized people can access the web interface. This solves the issue of viewing the page source from a browser.

   The administrative password can be changed by changing the configuration parameter or through the phone's user interface under **Settings > Advanced**.

   This is not a complete workaround, but it mitigates the issue by removing the ability for an attacker to use a well-known default password.

3. If your phones are running UC Software 4.0.0, set `httpd.cfg.secureTunnelRequired` to 1. All communications with the web interface are now secure.

   This is not a complete workaround, but it mitigates the issue of an attacker sniffing packets.

4. Use the HTTPS protocol for all communications.

This is not a complete workaround, but it mitigates the issue by removing the ability for an attacker to use a well-known default password.

5 Downgrade the phones running UC Software 3.3.2 to 3.3.1 . The UCS Software 3.3.1 does not have the issue.

6 Upgrade the phones running UC Software 3.3.2 to 3.3.3 or upgrade the phones running UC Software 4.0.0 to 4.0.1 . See Resolution.

Resolution

This issue is fixed in UC Software 3.3.3 (see VOIP-74074), which was released in November 2011, and is fixed in UC Software 4.0.1 (see VOIP-74167), which was released in December 2011.

Trademarks

Disclaimer

While Polycom uses reasonable efforts to include accurate and up-to-date information in this document, Polycom makes no warranties or representations as to its accuracy. Polycom assumes no liability or responsibility for any typographical or other errors or omissions in the content of this document.

Limitation of Liability

Polycom and/or its respective suppliers make no representations about the suitability of the information contained in this document for any purpose. Information is provided "as is" without warranty of any kind and is subject to change without notice. The entire risk arising out of its use remains with the recipient. In no event shall Polycom and/or its respective suppliers be liable for any direct, consequential, incidental, special, punitive or other damages whatsoever (including without limitation, damages for loss of business profits, business interruption, or loss of business information), even if Polycom has been advised of the possibility of such damages.

Customer Feedback

We are constantly working to improve the quality of our documentation, and we would appreciate your feedback. Please send email to VoiceDocumentationFeedback@polycom.com.

POLYCOM® | Support

Visit support.polycom.com for software downloads, product document, product licenses, troubleshooting tips, service requests, and more.