SURECOM

Connecting Clarity

Security Guidelines for Surecom Customers

Contents

1. Document Purpose

The purpose of this document is to provide guidelines around the setup of passwords and logins for systems that Surecom installs and maintains to ensure that all systems are kept secure from unauthorised access.

2. Executive Summary

There has been a noticeable rise in cyber security breaches in recent times and as a result it has become necessary to ensure that any systems that Surecom install or are provided access to, are to be kept as secure as possible to prevent any unauthorised access.

In some extreme cases phone systems have been accessed illegally and used for overseas phone calls. In some cases this has resulted in the businesses incurring costs in excess of $80,000.00.

Each section of this document will provide guidelines on the minimum security and login measures that should or will be implemented with each of the systems Surecom installs.

3. Avaya IP Office Platform

The Avaya IP Office has many different passwords that can be set up to prevent access to the various parts of the solution. Below are each of the sections that secure passwords should be set up and what the minimum password strength should be:

3.1 Manager Logins

With all systems that Surecom installs all default passwords will be changed to ensure that anyone that has knowledge of the systems cannot access them using the default logins.

A login called Surecom is always created on systems installed by Surecom to allow an audit to be done on any changes made to the system by any other user. If the customer requires a login to the system then a user called 'Engineer' should be created.

All passwords for any users on the Avaya IP Office Manager application will be a minimum of 8 characters and contain at least one of each the following characteristics:

- A capital letter
- A number
- A special character e.g. !@#$%^&*
- No password is to contain sequential numbers or letters of the alphabet

3.2 SIP extension logins

As SIP extensions are one of the most common methods to gain access to a phone system if there are open ports on the firewall it is necessary to ensure the complexity of the passwords used for any SIP extension created on the Avaya systems is as secure as possible.

As only numeric digits can be used for SIP extension logins, the only way to better secure this login is to make it as long as possible. The Avaya IP Office allows for up to a 13 digit login code to be set for this and the maximum number of digits (13) must be used when setting passwords up on the SIP extension with non-sequential numbers.

3.3 IP extension logins

Whilst not as susceptible as the SIP extensions we need to ensure that these login codes are also kept secure.

As this login is usually a code that a user needs to input each time they login we cannot make it 13 digits long but each login code should be set to at least 6 digits and should not be sequential numbers.

3.4 Voicemail logins

Voicemail box logins is another method that can be used to access phone systems but as with the IP extension logins it is a code that users will need to input on occasion so we cannot make these 13 digits long but each login code should be set to at least 6 digits and should not be sequential numbers.

As this login can also be changed by the users themselves we recommend that users change their passwords to 6 digit passwords when changing them.

3.5 User logins

With the availability of more CTI applications such as One-X Portal and One-X mobile it is necessary to set a password on the user within the IP Office to access these applications.

Surecom recommends that the passwords for the users requiring access to these applications to be a minimum of 8 characters and contain at least one of each of the following characteristics:

- A capital letter
- A number
- A special character e.g. !@#$%^&*

3.6 Application logins

There are a number of applications available for IP Office such as One-X portal, CCR, IPOCC etc. that all have administrative and user logins.

All passwords for any administrative and user logins should be set to a minimum of 8 characters and contain at least one of each of the following characteristics:

- A capital letter
- A number
- A special character e.g. !@#$%^&*

3.7 Scopia platform

The Scopia Video Conferencing platform also has logins for the codec unit itself as well as the Desktop Server software.

Both systems need to have their default passwords changed and should be a minimum of 10 characters and contain at least one of each of the following characteristics:

- A capital letter
- A number
- A special character e.g. !@#$%^&*

As some customers maintain their own logins for these platforms, Surecom recommends that the logins conform to the above standards to ensure security.

3.8 3rd Party IP endpoints

Avaya IP Office has the ability to make use of 3rd party hardware such as Polycom IP conference phones and Spectralink Wi-Fi handsets.

These handsets all have web interfaces with default logins which need to be set to be at least 10 non-sequential digits or where possible 13 alphanumeric characters.

4. Other platforms

Surecom also installs and maintains many other platforms that need to be secured from unauthorised access. Below is a summary of those systems and the minimum password requirements for each of them.

4.1 Aruba Wi-Fi

The Aruba Wi-Fi solution consists of several components and will need secure passwords set for each of them to ensure no unauthorised access. Below are a list of those components and there password requirements:

4.1.1 Aruba Controllers

The controller's password needs to be set to a minimum of 10 characters and contain at least one of each of the following characteristics:

- A capital letter
- A number
- A special character e.g. !@#$%^&*

4.1.2 Aruba Instant AP's

The Aruba instant AP's needs to be set to a minimum of 10 characters and contain at least one of each of the following characteristics:

- A capital letter
- A number
- A special character e.g. !@#$%^&*

4.1.3 SSID passwords

Where RADIUS is not possible the security on any SSID should be set to WPA2 and should have a password of a minimum of 10 characters and contain at least one of each of the following characteristics:

- A capital letter
- A number
- A special character e.g. !@#$%^&*

5. CTI/Nurse call servers and client PC's

Surecom on occasion are provided with remote access to client's servers and PC's for various applications such as nurse call, Avaya applications etc.

Where a server or PC is supplied by Surecom or remote access is provided to a server or PC by a client we recommend that a password of a minimum of 10 characters be used and contain at least one of each of the following characteristics is set:

- A capital letter
- A number
- A special character e.g. !@#$%^&*

6. Summary

While this document covers the major platforms that Surecom install there are many other systems that have logins that may be implemented by Surecom.

As a general rule these must have their default passwords changed where possible to a minimum of 10 characters and contain at least one of each of the following characteristics:

- A capital letter
- A number
- A special character e.g. !@#$%^&*