Security Checklist Frequently Asked Questions

1. Q: Is drive encryption required?
A: Mobile devices such as tablets, phones, notebooks and laptops must have their drives encrypted. For desktop devices (and servers), while not required, it is a good idea to have the drives encrypted. If you need assistance with getting your devices' drive encrypted, please ask Entreda to assist you with this service.

2. Q: How does Entreda Unify determine a device's drive encryption status?
A: The Unify applet detects if an approved full disk encryption software is installed on an end-point (which will be categorized as a "pass"). If an encryption software package is installed, but is no longer supported, this check will be flagged as a "warning." Anything outside of this will be categorized as a "fail." Entreda Unify performs a check to verify that specific signatures are found to validate the drive encryption.

For the list of approved full disk encryption packages, please refer to the "Compliance Summary" document.

3. Q: How does Entreda Unify determine if a device is using WIFI connectivity that is using WPA2 encryption?
A: If WPA2 encryption is used for the WIFI connectivity and/or Wired Ethernet, this status check is categorized as a "pass." However, if at any time, Entreda Unify determines that any other connectivity is being used, it will flag this as a "fail" and specify the reason why and the network name (WIFI SSID). Entreda Unify programmatically interfaces with the underlying operating system (Windows or MAC OS X) and continuously monitors the device's local area network interfaces (WIFI and Wired Ethernet). Examples of "failing" WIFI networks includes those that are encrypted with WPA+AES, WPA+TKIP and WEP.

Assuming the device user has subscribed to the Entreda Unify VPN service, if Entreda Unify detects that a non-secure WIFI network is used, the device user will be prompted to enable a secure encrypted tunnel (VPN) for their browsing/internet access. This auto-remediation feature is not enabled by default.

4. Q: How does Entreda Unify enforce use of a strong password and aging policy?
A: The Entreda "Computer Device Password Policy" feature enforces a password policy for all your devices (Windows PC and Mac OS) automatically. This feature uses the existing user login on your device. Password policy enforcement includes: complexity (strength), aging (expiration) and length.

The following are requirements for the password policy to be "passing" (in accordance to SEC/FINRA guidelines):

A) **Password "complexity"** (or "strength") must be high and contain at least 3 of the following elements:
- Lowercase letter (a through z)
- Uppercase letter (A through Z)
- Numbers (0 through 9)
-Symbols (#$%&, etc.).

B) **Password Length** has to have a minimum length (default is 8 characters)

C) **Password Aging Policy**: Password has to change periodically (at least every 90 days)

D) **Password History Length:** Has to be greater than or equal to 5. Need to ensure same password is not "recycled"

NOTE: We are unable to check the password itself. We monitor the policies, which get set on the device instead**.**

The password policy can be changed by system administrator and/or compliance enforcement organization. This auto-remediation feature is disabled by default and can be enabled through the Entreda Unify cloud console.

For devices that utilize a Windows "live" login (available in Windows 8 and 10), the password policy needs to be maintained manually.

5. Q: Do I still need a router/firewall on premise at my office if my client device has its firewall enabled?
A: Yes. The client firewall and on premise firewall/router serve different roles - both are required. Each provides a different layer of protection.

6. Q: How does Entreda Unify determine if a device is protected by a client firewall?
A: If the device's firewall is enabled, this will be flagged as a "pass." If not enabled, this will be flagged as a "fail." Entreda Unify interfaces with the underlying operating system (Windows or MAC OS X) to determine if a device has the firewall enabled or disabled.

If Entreda Unify detects that the device's firewall is not enabled, it will automatically remediate this. In such a case, the device user will be prompted to enable the client firewall. This auto-remediation feature is enabled by default and can be disabled through the Entreda Unify cloud console.

7. Q: If I have Anti-malware software, do I still need Anti-Virus software?
A: Yes both are needed as each serve a different purpose. Typically, anti-virus software protects against viruses (including worms, and Trojans) whereas anti-malware software detect malicious software (such as unwanted programs).

8. Q: How does Entreda Unify determine if a device is utilizing anti-virus software?
A: Entreda Unify has a "white-list" of supported anti-virus packages and if any of these are found, the check will be categorized as a "pass." If no anti-virus software is found or if the anti-virus package in use is not part of the "white-list," then this would be categorized as a "fail."

The "white-list" of anti-virus packages can be found in the "Compliance Summary" document. New anti-virus software packages can be added to the white-list by the system operator or compliance enforcement organization.

If Entreda Unify detects that a device doesn't have anti-virus software installed, it will automatically remediate this condition. In such a case, the device user is prompted to install an Entreda approved Anti-virus packaged. This auto-remediation feature must be enabled on a per device basis from the Entreda Unify cloud console.

9. Q: How does Entreda Unify determine if a device's anti-virus software is set to automatically update?
A: Entreda Unify has a "white-list" of supported anti-virus packages (refer to above for list) which will report as a pass. Otherwise, this will be categorized as a "fail." Entreda Unify programmatically interfaces with the Windows operating system determine if automatic updates have been enabled. For MAC OS X this requires a manual check by the user as this capability is not currently supported by the anti-virus APIs.

10. Q: How does Entreda Unify determine if a device's Operating System is set to automatically update?
A: If the device's operating system is set to automatically update, this will be categorized as a "pass." If not enabled, this will be categorized as a "fail." Entreda Unify interfaces with the operating system (Windows or MAC OS X) to determine the status of this function.

If Entreda Unify detects that a device doesn't have its operating system set to automatically update, this will be remediated automatically. In such a case, the device user is prompted to have their Operating System set to auto-update. This auto-remediation feature must be enabled on a per device basis from the Entreda Unify cloud console.

11. Q: How does Entreda Unify determine if a device has the appropriate screen-lock settings?
A: A "passing" screen-lock setting is defined as having the screen lock function enabled with a screen-lock timeout of 15 minutes (or less). If the screen lock is not enabled and/or the timeout is set to greater than 15 minutes, this is categorized as a "fail." Entreda Unify interfaces with the underlying operating system (Windows or MAC OSx) to determine status. Some devices can have multiple User Accounts / logins, and in this case, Entreda Unify will check each user account and if any of these User Accounts / Logins are not set accordance to the above criteria, it will be categorized as a "fail." Conversely, if all the User Account / Logins are set correctly, Entreda Unify will report this as "pass."

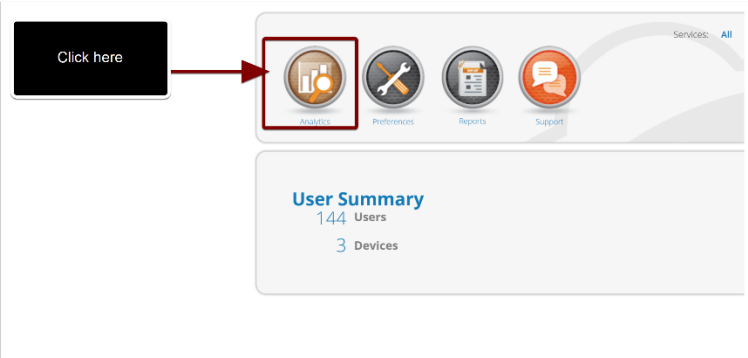
If Entreda Unify detects that a device doesn't have its screen-lock function enabled, it will be remediated automatically. In this case, the device user is prompted to enable the screen-lock function. This auto-remediation feature must be enabled on a per device basis from the Entreda Unify cloud console. On Mac OS the timeout will be set 10 minutes and for Windows, the timeout is 15 minutes.

12. Q: How does Entreda Unify determine if P2P (peer to peer) file-sharing software is installed?
A: Entreda Unify performs a forensic check to look for signatures of P2P (peer to peer) file-sharing software packages on the computer. If any of these packages/signatures are found, this will be categorized as a "fail." However, if these application signatures are not found, this will be categorized as a "pass." The signatures vary from time to time, and we do our best to provide updates in a timely manner. The "black-list" of peer-to-peer packages can be found in the "Compliance Summary" document.

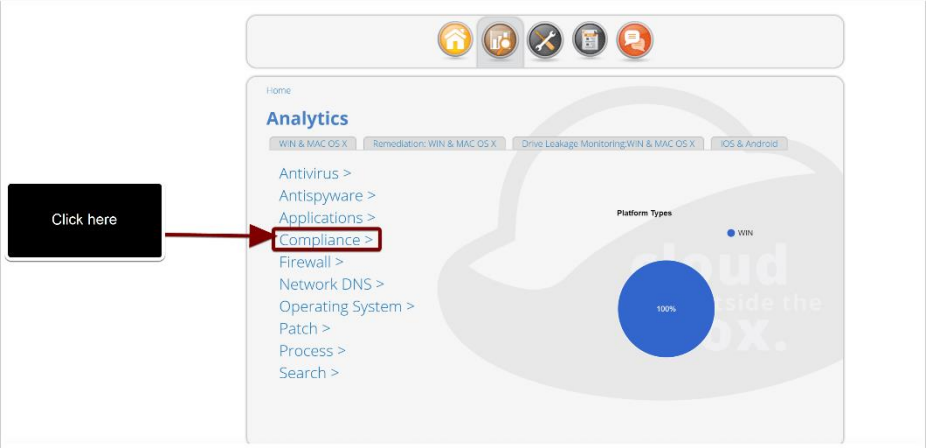
13: How to find all the security checklist data?
A: All of this information can be found within the Entreda Unify Web Console at by login with your credentials at: https://nhld.entreda.com

In reference to ***items (above) #2 (Drive Encryption), #3 (WIFI Connectivity), #8 (Ant-Virus package),and #13 (Peer-to-peer/file-share software),*** details for these can be found on the following widget on the compliance section of the Entreda Unify Web console:

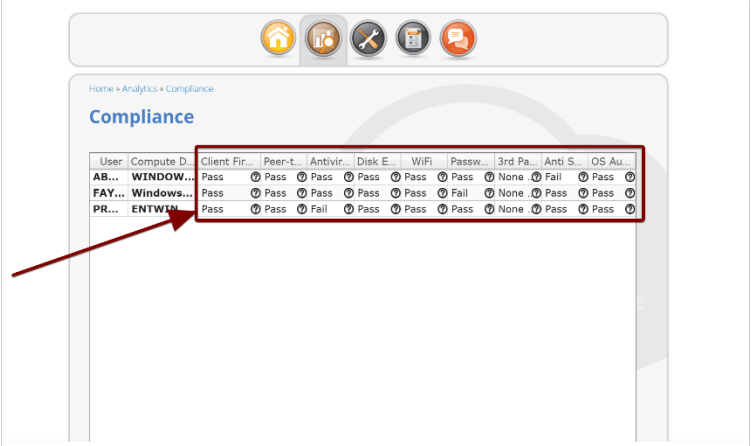
1) Click on Analytics



2) Click on Compliance



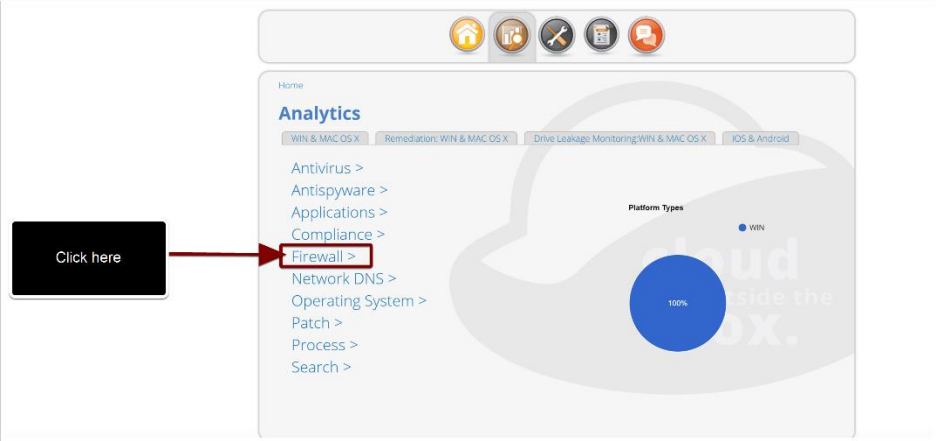
Sample screenshot of the Compliance page below:



In reference to item **#7 (Client Firewall),** details for this can be found by going to: "Analytics" → "Client Firewall."

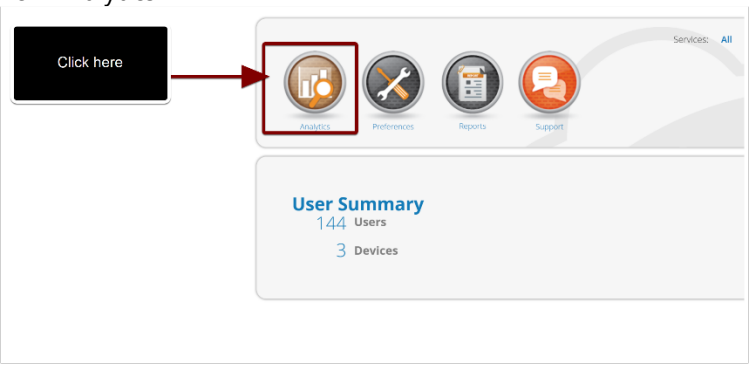
1) Click on Analytics

2) Click on Firewall

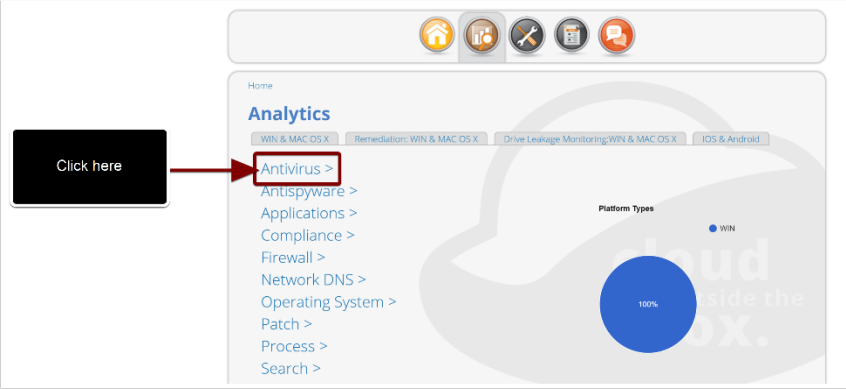


In reference to item **#10 (Ant-virus set to update automatically),** details for this can be found by going to: "Analytics" →Antivirus."

1) Click on Analytics



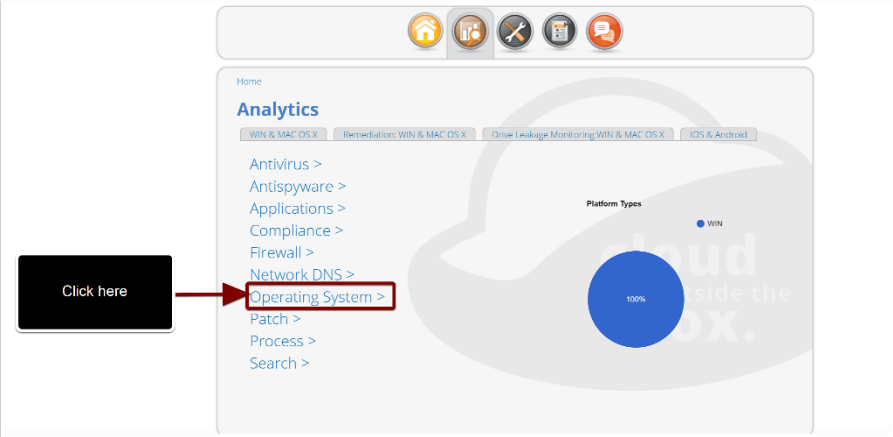
2) Click on Antivirus



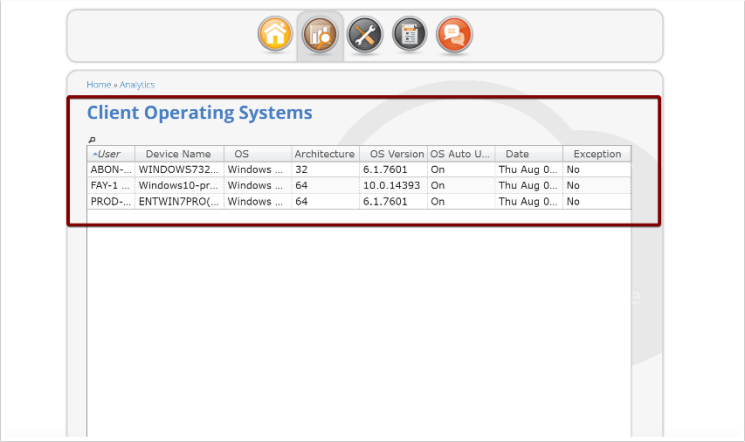
In reference to items **#11 (Operating System set to update automatically)**, details for this can be found by going to: "Analytics" → "Operating System."

1) Click on Analytics

2) Click on Operating System



3) Here you will find all details on Operating System including whether Operating System is set to update automatically



14: How often does the data get refreshed in the Entreda Unify Console after a setting change on a device?
A: It will take approximately 3-4 minutes for the data to appear in the Entreda Unify Web console. You will need to refresh the page.

15: How often will the auto-remediation retry?
A: The retry timer for the auto-remediation settings is configurable to be between 0-30 days. This applies to screen-lock, Operating System updates, client firewall, password policy and anti-virus, where if the user selects "no" they will get prompted again in 0-30 days, depending on the configuration. However, in the case of WIFI remediation, this is checked each time a device is connected to a different network.

16: How often does the Security checklist report go out?
A: The report gets sent out on a bi-weekly basis.