Guidance

End User Devices Security Guidance: Chrome OS

Published 10 June 2014

Contents

1. Changes since previous guidance
2. Usage scenario
3. Summary of platform security
4. How the platform can best satisfy the security recommendations
5. Network Architecture
6. Deployment process
7. Provisioning steps
8. Policy recommendations
9. Enterprise considerations

This guidance is applicable to devices running Chrome OS 32 and later. This guidance was developed following testing performed on Samsung Chromebooks running Chrome OS version 32.0. All device management services are provided by Google Infrastructure. This guidance was prepared with the provided versions as of February 2014.

1. Changes since previous guidance

This document updates the previous guidance to cover Chrome OS 32. Some changes to the recommended configuration have been made to take account of new features and changed behaviours in the platform. The risk information given below has been updated to reflect that.

Deployments which followed the previous recommended configuration will need to be updated with the new configuration to take advantage of the enhanced platform features.

2. Usage scenario

Chrome OS devices will be used remotely over any network bearer, including Ethernet, Wi-Fi and 3G, to connect back to enterprise services over a VPN. This enables a variety of remote working approaches such as:

- accessing OFFICIAL email through an enterprise-provided web portal

- creating, editing, reviewing and commenting on OFFICIAL documents through an enterprise-provided web portal
- accessing the OFFICIAL intranet resources, the internet and other web-resources

To support these scenarios, the following architectural choices are recommended:

- All data should be routed over a secure enterprise VPN to ensure the confidentiality and integrity of the traffic, and to benefit from enterprise protective monitoring solutions
- Users of Chrome OS devices should not use unaccredited enterprise or Internet services to store or process OFFICIAL email, documents or web applications
- Arbitrary third-party application installation by users is not permitted on the device. A list of allowed trusted apps and extensions can be configured within the Google Admin console

3. Summary of platform security

This platform has been assessed against each of the 12 security recommendations, and that assessment is shown in the table below. Explanatory text indicates that there is something related to that recommendation that the risk owners should be aware of. Rows marked [!] represent a more significant risk. See How the platform can best satisfy the security recommendations for more details about how each of the security recommendations is met.

Recommendation	Rationale
1. Assured data-in-transit protection	The VPN can be disabled by the user. The built-in VPN has not been independently assured to Foundation Grade, and no suitable third-party products exist.
2. Assured data-at-rest protection	The built-in data encryption has not been independently assured to Foundation Grade.
3. Authentication	Chrome OS relies on Google online services for user management and authentication. [!] There is no ability to automatically lock a user account after a number of failed logon attempts when the device has no Internet connection.
4. Secure boot	
5. Platform integrity and application sandboxing	
6. Application whitelisting	
7. Malicious code detection and prevention	
8. Security policy enforcement	
9. External interface protection	Radio interfaces such as Wi-Fi and Bluetooth cannot be controlled by policy.
10. Device update policy	
11. Event collection for enterprise analysis	[!] There is no facility for collecting security logs remotely from a device, such as failed logins.

3.1 Significant risks

The following significant risks have been identified:

- The VPN has not been independently assured to Foundation Grade, and does not currently support some of the mandatory requirements expected from assured VPNs. The VPN can be disabled by the user and some Google traffic is sent prior to the VPN being established resulting in potential for data leakage onto untrusted networks. Without assurance in the VPN there is a risk that data transiting from the device could be compromised
- Chrome OS data encryption has not been independently assured to Foundation Grade, and does not support some of the mandatory requirements expected from assured full disk encryption products. Without assurance there is a risk that data stored on the device could be compromised
- There is no account lockout to prevent brute force password attacks when the device is offline. Logon attempts are hardware rate-limited when the user is fully logged off but not when a user session is still active and the screen has been locked. There is therefore potential to guess a user's password on a stolen device
- Collection of events for enterprise analysis is limited, meaning protective monitoring and forensic analysis following any compromise may be much harder than on other platforms
- Only limited policy controls are available to restrict the external interfaces a user can enable, meaning that external interfaces may be accidentally or deliberately enabled by the end-user
- Management of Chrome OS devices via Google Admin console, and authentication of users to devices are intrinsically dependent on Google's online services. Trust in Google's online services is essential for enterprise deployments of Chrome OS devices. Users can authenticate against the account from unmanaged devices with risk of credential theft

4. How the platform can best satisfy the security recommendations

4.1 Assured data-in-transit protection

Use the native IPsec VPN client.

4.2 Assured data-at-rest protection

Use the native Chrome OS data encryption without additional configuration.

4.3 Authentication

Use a strong 9-character password to authenticate to the device. It is not possible to technically enforce some aspects of password complexity on Chrome OS, hence the increased password length versus some platforms.

Enterprises can choose to enable two-factor authentication on Chrome OS which will require the user to enter the second factor the first time they log in to their device, and after any subsequent password changes.

4.4 Secure boot

This requirement is met by the platform without additional configuration. Users should be educated to recognise when secure boot has failed and respond appropriately.

4.5 Platform integrity and application sandboxing

This requirement is met by the platform without additional configuration.

4.6 Application whitelisting

Authorised apps and extensions can be managed using a whitelist in Google Admin console.

4.7 Malicious code detection and prevention

Chrome does not support side-loading of applications. Content-based attacks can be filtered by scanning on the email server.

4.8 Security policy enforcement

The security policy can be managed in Google Admin console to centrally enforce security settings, however some security related settings are configured only by the user, including those for Bluetooth.

4.9 External interface protection

No technical controls exist to prevent users from enabling Wi-Fi and Bluetooth, or using certain USB devices. The use of USB storage devices can be disabled by policy.

4.10 Device update policy

Operating system security updates can be configured via the Google Admin console to be either automatically or manually applied. Using the recommended automatic setting, updates are installed automatically when the device is switched on and logged in. System updates are applied when the user restarts their Chrome OS device.

4.11 Event collection for enterprise analysis

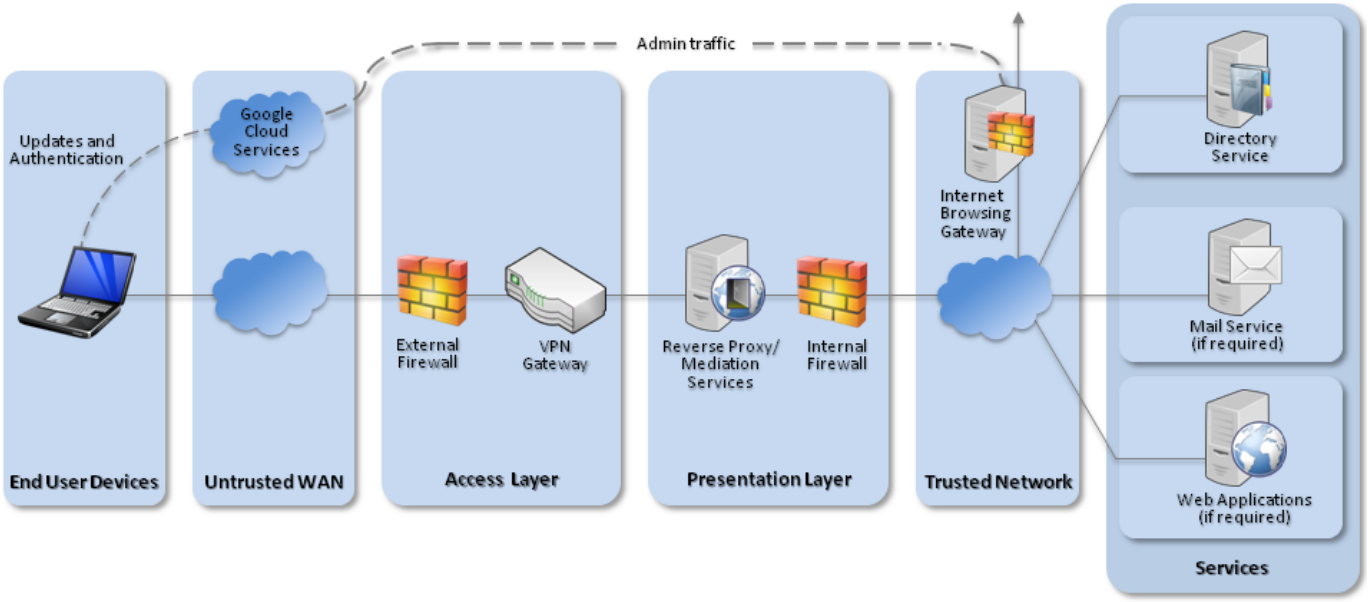
The Google Management Console shows a limited amount of information about enrolled Chrome devices. It is not possible to display or collect many security related events, including failed logins.

4.12 Incident response

Cached user data can be wiped from the device after each sign-out (it is retained in the cloud). User accounts can be disabled or suspended from within the Google Admin console. Access to the enterprise network can be prevented by revoking the VPN client certificate associated with a lost or stolen device. Additionally, the client certificates for any other enterprise servers (such as email) that are stored on the device should be revoked.

5. Network Architecture

All remote or mobile working scenarios should use a typical remote access architecture based on the Walled Garden Architectural Pattern. The following network diagram describes the recommended architecture for this platform.



Recommended network architecture for deployments of Chrome OS devices

6. Deployment process

The following steps should be followed to prepare the enterprise infrastructure for hosting a deployment of these devices:

1. Procure and provision a Google Apps for Business account which also creates the Administrator account for use by the enterprise.
2. Procure and provision a Google Enterprise Management Console Account using the previously created

Administrator account.
3. Purchase device licenses for the Google Management Console from the Google store
4. Change the temporary password for the account.
5. Recommended: Enable Google two-factor authentication for Admin account.
6. Verify domain ownership.
7. Setup Google Apps and Enterprise accounts according to requirements.
8. Create profiles as defined in the Policy Recommendations section below.

7. Provisioning steps

The following steps should be followed to provision each end user device onto the enterprise network to prepare it for distribution to end users:

1. Enrol Chrome OS device
2. Add users to your domain

8. Policy recommendations

The following settings can be applied from the Enterprise Management Console:

Configuration Rule	**Configuration Setting**
Device Settings → Enrol Devices Automatically	Enrol Devices Automatically
Device Settings → Allow Guest Mode	Do not allow Guest Mode
Device Settings → Sign-In Restriction	*@{company domain}
Device Settings → Sign-in Screen	Never show usernames and photos
Device Settings → Public Session Kiosk	Do not allow Public Session Kiosk
Device Settings → Single App Kiosk	Do not all Single App Kiosk
Device Settings → Auto Update	Allow auto-updates
Device Settings → Restrict Google Chrome version to at most	No Restriction
Device Settings → Auto reboot after updates	Allow auto-reboots
Device Settings → Anonymous Metric Reporting	Never send metrics to Google
Device Settings → Device State Reporting	Enable device state reporting
User Settings → Allowed Apps and Extensions	Block all apps and extensions except the ones I allow
User Settings → Safe Browsing	Always enable Safe Browsing

User Settings → Screen Lock	Always automatically lock screen on idle
User Settings → Malicious Sites	Prevent user from proceeding anyway to malicious sites
User Settings → Policy Refresh Rate	30
User Settings → Spell Check Service	Disable the spell checking web service
User Settings → Google Translate	Never offer translation
User Settings → Google Cloud Print Submission	Disallow submission of documents to Google Cloud Print
User Settings → Google Cloud Print Proxy	Disallow using Chrome as a proxy for Google Cloud Print

In addition the following settings and steps must be performed manually on each device to be deployed. The settings are applied per-user, and therefore the person setting up the device must log into the Chrome device as the user to be set up. This may require resetting the user's password before and after deployment.

Configuration Rule	**Value**
Settings → Advanced Settings → Bluetooth	Off (unless required)

8.1 VPN profile

Setting	**Value**
IKE DH Group	2 (1024-bit)
IKE Encryption Algorithm	AES-128 CBC
IKE Hash Algorithm	SHA-1
IKE Authentication Method	RSA X.509
IPsec Encryption	AES-128 CBC
IPsec Auth	SHA-1
SA Lifetime	24 hours

8.2 Enterprise firewall

To facilitate connections to Chrome OS devices and services, the following steps should be followed:

- Firewall rules should be configured to allow users to access the VPN terminator.
- If SSL intercepting proxies are used within the environment they should be configured to whitelist Google services as these services often use certificate pinning and fail to work when intercepted.

9. Enterprise considerations

9.1 Secure boot

The Chrome Secure Boot process alerts a user when an attempt to subvert the security controls has taken place. It is important to ensure users know how to identify and respond to this alert.

9.2 Enterprise services

Users of Chrome devices should not use unaccredited enterprise services to store or process OFFICIAL email, documents or web applications, which may include the default public Google services. As with any online service, enterprises should ensure that the services used by the platform for storing or processing OFFICIAL information are appropriately accredited.

9.3 Cloud integration

Chrome OS relies on Google services to authenticate users to the device, and to manage the device. Trust in Google's online services is essential for enterprise deployments. Features such as the 'Spell Check Service' and translation services rely on data being sent to a Google web service. Such features should not be used when handling OFFICIAL information as it could be processed by unaccredited systems.

It is possible for users to log in to enterprise Google accounts from unmanaged devices. Users should only log in to their enterprise Google account from enterprise managed devices to reduce the risk of credential theft.

9.4 Chrome web store

The configuration above prevents users from installing apps and extensions from the Chrome web store, but an organisation can host a private Chrome app collection to distribute in-house applications to their employees if required.

If the Chrome web store is enabled, authorised apps and extensions can be managed using an allow list in the Google Admin console.

Legal Information