Google Chrome

Przewodnik wdrażania urządzeń z Chrome

Konfigurowanie i wdrażanie urządzeń z Chrome w organizacji

Enterprise i Education

Spis treści

Informacje o tym przewodniku

Ten przewodnik stanowi uzupełnienie pięciokrokowego przewodnika Konfigurowanie urządzeń z Chrome. Szczegółowo opisuje te zagadnienia:

- najważniejsze decyzje podejmowane podczas wdrażania urządzeń z Chrome w dużej szkole lub firmie;
- zasady w chmurze, aplikacje Chrome i określone przypadki użycia. Bardziej szczegółową dokumentację znajdziesz w Centrum pomocy Chrome Enterprise.

Kwestie opisane szczegółowo w tym przewodniku:

- **Konfigurowanie i wdrażanie** – jak połączyć wszystkie urządzenia z siecią, zarejestrować je w domenie i zaktualizować do najnowszej wersji Chrome OS.
- **Zarządzanie** – jak przekazywać zasady w domenie, aby spełniały wymagania, oraz jak konfigurować urządzenia obsługujące najnowszą wersję Chrome OS i nimi zarządzać.

Uwaga: zalecenia dotyczące wdrażania urządzeń z Chrome zebraliśmy podczas współpracy z szerokim gronem klientów i partnerów ze środowisk szkolnych i biznesowych. Jesteśmy im wdzięczni za podzielenie się doświadczeniami i uwagami. Informacje dotyczące wdrażania zarządzanej przeglądarki Chrome znajdziesz w artykule Zarządzanie przeglądarką Chrome.

Opisane treści	Instrukcje, zalecenia i najistotniejsze uwagi dotyczące wdrażania urządzeń z Chrome w środowisku szkolnym lub biznesowym
Główni odbiorcy	Administratorzy IT
Środowisko IT	Chrome OS, środowisko w chmurze
Wnioski	Sprawdzone metody działania związane z najistotniejszymi kwestiami i decyzjami dotyczącymi wdrażania urządzeń z Chrome

Ostatnia aktualizacja: 10 września 2019 r.
Lokalizacja dokumentu: https://support.google.com/chrome/a/answer/6149448

Wprowadzenie

Urządzenia z Chrome to komputery z systemem Chrome OS zaprojektowane przez Google. Są unikalne, ponieważ w pełni działają w środowisku internetowym i automatycznie się aktualizują, dzięki czemu nie trzeba regularnie instalować łatek ani ponownie wdrażać na nich obrazów systemu. Te komputery szybko się uruchamiają i mają wbudowane różne funkcje zabezpieczeń.

Urządzeniami z Chrome można zarządzać centralnie w konsoli administracyjnej Google. W tej internetowej konsoli możesz skonfigurować ponad 200 ustawień związanych na przykład z siecią Wi-Fi, aplikacjami do wstępnego zainstalowania czy wymuszaniem automatycznej aktualizacji urządzeń do najnowszej wersji Chrome OS.

Wymagania wstępne

1. Chociaż tożsamość Google (konto Google Workspace) nie jest wymagana do korzystania z zarządzanego urządzenia z Chrome, zalecamy udostępnienie użytkownikom kont Google. Więcej informacji znajdziesz w artykule Dodawanie nowych użytkowników lub adresów e-mail.
2. W przypadku każdego samodzielnego urządzenia z Chrome, którym chcesz zarządzać, potrzebujesz urządzeń Chromebook Enterprise lub licencji – np. na Chrome Enterprise lub na Chrome Education. Licencje możesz kupić dla szkoły lub firmy. Organizacje w Stanach Zjednoczonych i Kanadzie mogą też kupić licencję na Chrome Enterprise online.
3. Jeśli chcesz wdrożyć dużą liczbę urządzeń z Chrome lub po raz pierwszy wdrożyć je razem z Google Workspace, zalecamy skontaktowanie się z Partnerem Google Cloud.

Zarządzanie urządzeniami z Chrome

Urządzenia z Chrome można tak skonfigurować, aby działały w niemal każdym środowisku szkolnym lub biznesowym. Podczas ich wdrażania możesz (jako administrator) zarządzać dostępem do sieci Wi-Fi, filtrowaniem sieciowym, zainstalowanymi wstępnie aplikacjami oraz szeroką gamą innych ustawień, takich jak:

- **Zasady dotyczące urządzeń** – umożliwiają wymuszanie ustawień i zasad na zarządzanych urządzeniach z Chrome w Twojej organizacji, niezależnie od tego, kto się na nich loguje. Możesz np. umożliwić logowanie tylko określonym użytkownikom, zablokować tryb gościa czy skonfigurować ustawienia automatycznych aktualizacji. Więcej informacji
- **Zasady dotyczące użytkowników** – umożliwiają wymuszanie ustawień i zasad u użytkowników w organizacji, niezależnie od używanego przez nich urządzenia z Chrome. Administrator IT może na przykład wcześniej zainstalować aplikacje u określonych użytkowników, wymusić Bezpieczne przeglądanie, skonfigurować logowanie jednokrotne (SSO), blokować określone wtyczki, dodawać do czarnej listy wybrane adresy URL, zarządzać zakładkami oraz stosować dziesiątki innych ustawień u użytkowników w całej organizacji. Więcej informacji
- **Zasady dotyczące zarządzanych sesji gościa** – umożliwiają konfigurowanie zasad na urządzeniach współdzielonych w domenie. Zarządzane sesje gościa umożliwiają wielu użytkownikom używanie tego samego urządzenia z Chrome bez konieczności logowania się czy uwierzytelniania. Możesz wymuszać ustawienia, takie jak wylogowywanie użytkownika po upływie określonego czasu. Więcej informacji

Łączność

Podczas konfigurowania sieci bezprzewodowej w klasie lub firmie upewnij się, że sieć ma wystarczający zasięg w całym budynku oraz że przepustowość połączenia internetowego jest odpowiednia do tego, aby wszystkie urządzenia mogły działać online.

Najważniejsze funkcje

Urządzenia z Chrome obsługują wszystkie najczęściej używane protokoły Wi-Fi: WEP, WPA, WPA2, EAP-TLS, EAP-TTLS, EAP-PEAP i LEAP. Dodatkowo niektóre są też wyposażone w sprzęt umożliwiający łączenie się z internetem mobilnym 3G lub 4G. Korzystanie z tej opcji wymaga dostępu do sieci komórkowej i abonamentu obejmującego komórkową transmisję danych.

Wskazówki dotyczące oceny i wdrażania

Odpowiednia ocena i przygotowanie infrastruktury sieciowej organizacji stanowią ważny krok do zapewnienia użytkownikom najlepszej jakości usług. Administratorzy IT powinni upewnić się, że połączenie z internetem i przepustowość sieci są wystarczające, szczególnie w takich miejscach jak biuro czy szkoła, gdzie wiele urządzeń z Chrome jest używanych jednocześnie.

- **Przetestuj zasięg i zagęszczenie sieci Wi-Fi**, aby ocenić, czy konieczne będą dodatkowe punkty dostępu. Możesz to zrobić przy użyciu zewnętrznej aplikacji Wifi Analyzer na urządzeniu z Androidem.
- **Wykonaj przegląd infrastruktury bezprzewodowej i topologii** we wszystkich budynkach, zanim dokonasz wdrożenia w całej szkole lub firmie, aby mieć pewność, że zasięg sieci bezprzewodowej jest wystarczający. Zazwyczaj najlepiej jest skorzystać z usług partnera, który specjalizuje się w topologii sieci bezprzewodowej i wykonuje te czynności:
    - **Analiza lokalizacji** – najpierw musisz przeanalizować istniejącą sieć Wi-Fi oraz zakłócenia z okolicznych urządzeń i innych sieci Wi-Fi.
    - **Wdrażanie** – wdróż lub zmień położenie punktów dostępu, odpowiednio konfigurując ich zabezpieczenia, numery kanałów oraz siłę sygnału.
- **Upewnij się, że urządzenia z Chrome mają dostęp do wymaganych adresów URL.** Aby urządzenia z Chrome działały poprawnie, muszą mieć dostęp do sieci Google oraz muszą otrzymywać aktualizacje zasad i zabezpieczeń. Jeśli w swoim środowisku ograniczysz dostęp do internetu, musisz dopilnować, aby wdrożone urządzenia nadal miały dostęp do tych określonych adresów URL Google bez konieczności używania uwierzytelnionego serwera proxy ani kontroli SSL.

Więcej szczegółowych informacji znajdziesz w artykule Sieci korporacyjne dla urządzeń z Chrome.

Zarządzanie profilami sieciowymi

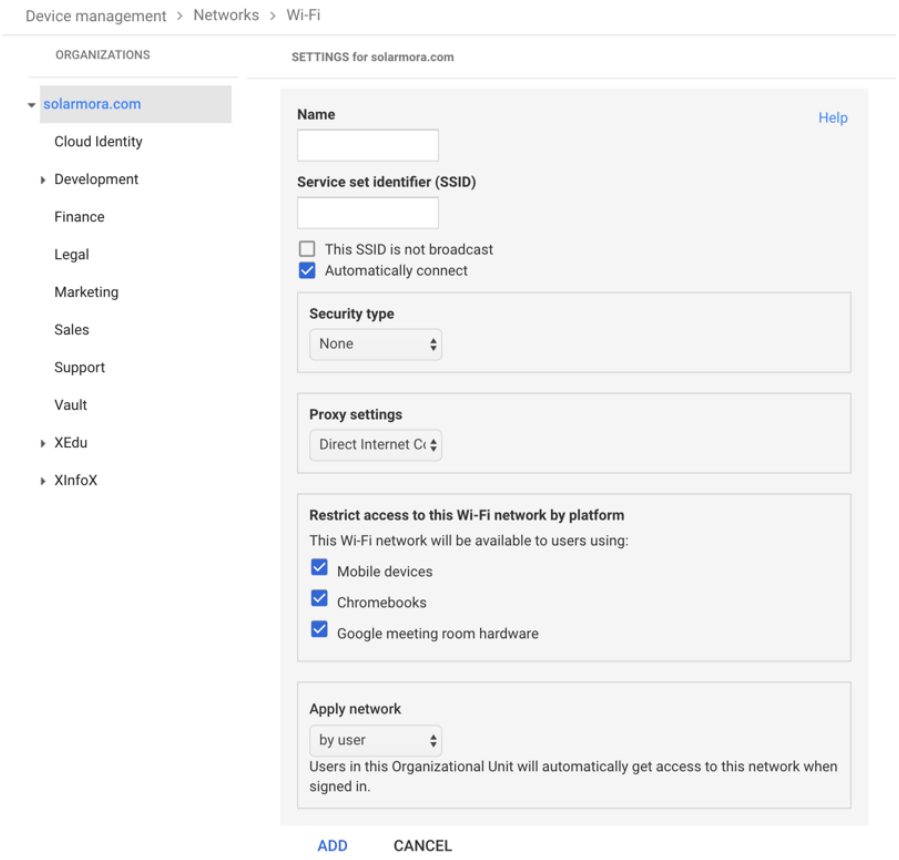
Sieci Wi-Fi można dodawać ręcznie na urządzeniu z Chrome w dowolnym momencie, ale Google zaleca korzystanie z konsoli administracyjnej do przekazywania profili sieci Wi-Fi. Te profile są pobierane i stosowane na urządzeniu z Chrome podczas procesu rejestracji. Aktualizacje profili sieci Wi-Fi są również przekazywane podczas automatycznego odświeżania zasad na urządzeniu z Chrome. Dzięki przekazywaniu tych konfiguracji przy użyciu konsoli administracyjnej klucz PSK może być wystarczająco złożony i nigdy nie trzeba go udostępniać użytkownikom.

Konfigurowanie Wi-Fi

Wielu użytkowników urządzeń z Chrome korzysta ze standardu WPA2-PSK ze względu na łatwość konfiguracji. Urządzenia z Chrome mogą jednak działać w wielu środowiskach edukacyjnych i biznesowych – w tym w złożonych sytuacjach dotyczących wdrażania, które wymagają certyfikatów klienta, logowania jednokrotnego i kiedy wdrażane są rozwiązania do filtrowania sieciowego. Poniżej znajdziesz wskazówki dotyczące konfigurowania Wi-Fi i opcjonalnych ustawień sieci.

Dodawanie konfiguracji Wi-Fi na poziomie urządzenia

Podrzędne jednostki organizacyjne dziedziczą profile sieci Wi-Fi z organizacji nadrzędnej. Aby skonfigurować profil, musisz mieć informacje o sieci, takie jak identyfikator SSID oraz rodzaj zabezpieczeń. Zwróć szczególną uwagę na identyfikator zestawu usług (SSID) oraz hasło – w obu przypadkach wielkość znaków ma znaczenie. Podczas określania nowego profilu sieci Wi-Fi musisz zaznaczyć też pola **Łącz automatycznie** i **Chromebooki** w sekcji **Ogranicz dostęp do tej sieci (Wi-Fi) dla określonych platform**. Dodatkowe szczegóły techniczne dotyczące konfigurowania siedzi znajdziesz tutaj.



Konfiguracja Wi-Fi

Aby zarejestrować urządzenia z Chrome i po raz pierwszy zsynchronizować zasady zarządzania, często najłatwiej jest użyć sieci otwartej lub niefiltrowanej. Ta konfiguracja zezwala urządzeniu z Chrome na otrzymywanie profili sieci określonych przez administratora IT. Po skonfigurowaniu urządzeń z Chrome usuń tę tymczasową sieć rejestracyjną z listy preferowanych sieci. Zobacz Zapominanie sieci.

Wdrażanie uwierzytelniania 802.1x

Urządzenia z Chrome obsługują uwierzytelnianie 802.1x. Skontaktuj się ze swoim dostawcą sieci, aby dowiedzieć się, jak skonfigurować urządzenia z Chrome z certyfikatami klienta. Na przykład rozszerzenie ClearPass Onboard firmy Aruba Networks obsługuje rejestrację urządzeń z Chrome i instaluje certyfikat w bezpieczny sposób.
Administratorzy systemu i partnerzy Google Cloud mogą skorzystać z Google Cloud Connect, aby znaleźć dokumentację zaawansowanej konfiguracji sieci firmowej Wi-Fi 802.1x.

Do pobrania certyfikatu 802.1x wymagane jest połączenie z siecią. W związku z tym musisz skonfigurować otwartą sieć WPA/WPA2-PSK lub użyć konwertera USB na Ethernet, aby wczytać certyfikat na urządzenie. Zobacz Zarządzanie sieciami.

Więcej informacji na ten temat znajdziesz w artykule Zarządzanie certyfikatami klienta na urządzeniach z Chrome.

Filtrowanie sieciowe

Organizacje używające urządzeń do filtrowania sieciowego wykonujących kontrolę Secure Socket Layer (SSL) zwykle wymagają dodania niestandardowego certyfikatu głównego na karcie **Wystawcy** na stronie `chrome://settings/Certificates`. Sprawdza się to w przypadku większości żądań internetowych inicjowanych przez użytkowników, ale niektóre żądania na poziomie systemu nie używają tego certyfikatu do ochrony użytkownika przed określonymi rodzajami zagrożeń. Zapoznaj się z tą listą hostów, które należy wykluczyć z kontroli SSL

Jeśli chcesz, żeby urządzenia z Chrome działały w sieci z kontrolą SSL, zapoznaj się z informacjami na stronie Konfigurowanie sieci z filtrami treści SSL. Znajdziesz tam wyjaśnienia dotyczące instalowania niestandardowego certyfikatu głównego u wszystkich użytkowników domeny, którzy zalogowali się na zarejestrowanych Chromebookach należących do Twojej organizacji.

Konfigurowanie kont i zasad Chrome OS

Za pomocą konsoli administracyjnej Google możesz centralnie organizować swoje urządzenia z Chrome i nimi zarządzać. Gdy zarządzasz użytkownikami przy użyciu konsoli administracyjnej, w sekcji Zarządzanie urządzeniami z Chrome możesz ustawić urządzenia i zasady dotyczące użytkowników według jednostki organizacyjnej.

W konsoli administracyjnej możesz zobaczyć listę swoich urządzeń z Chrome, wyszukiwać urządzenia i wyświetlać informacje na ich temat (np. numer seryjny, status rejestracji, datę zakończenia świadczenia pomocy technicznej, nazwę użytkownika wykorzystaną do rejestracji i ręcznie wprowadzone uwagi, takie jak lokalizacja). Wyświetlenie szczegółowych informacji o urządzeniu na podstawie jego numeru seryjnego pozwala sprawdzić wersję zainstalowanego na urządzeniu systemu operacyjnego, adres MAC i nazwę ostatniego zalogowanego użytkownika.
Te zasady dotyczące urządzeń są wymuszane na wszystkich urządzeniach Chrome, które zostały zarejestrowane do zarządzania w Twojej domenie.

Zasady dotyczące użytkowników są stosowane wszędzie tam, gdzie użytkownik się zaloguje, niezależnie od tego, czy urządzenie z Chrome jest zarejestrowane, czy nie. Te ustawienia obejmują możliwość konfigurowania zasad zabezpieczeń i kontrolowania, które aplikacje mogą pobierać użytkownicy i do których mają dostęp. Więcej informacji znajdziesz w artykule Informacje o zarządzaniu urządzeniami z Chrome OS.

Najistotniejsze kwestie dotyczące zasad

Aby ustawić poprawne ustawienia dla Twojej szkoły lub firmy:

1. Określ, jak ma być skonfigurowane modelowe urządzenie z Chrome w Twoim środowisku.
2. Ustaw te same ustawienia jako zasady w konsoli administracyjnej w przypadku jednej jednostki organizacyjnej (na potrzeby testu).
3. Gdy ustawienia (takie jak strona domyślna do załadowania po uruchomieniu, aplikacje internetowe, które mają zostać wcześniej zainstalowane, czy adresy URL, które mają zostać zablokowane) zostaną ustawione i sprawdzone na urządzeniach z Chrome w tej jednostce organizacyjnej, możesz powielić je w całej domenie.

Więcej informacji na temat używania jednostek organizacyjnych na urządzeniach z Chrome znajdziesz w artykule Przenoszenie urządzenia z Chrome do jednostki organizacyjnej.

Zalecane ustawienia

W konsoli administracyjnej kliknij **Zarządzanie urządzeniami > Zarządzanie urządzeniami z Chrome**, aby uzyskać dostęp do ustawień w obszarach **Ustawienia użytkownika** i **Ustawienia urządzeń**. Chociaż większość organizacji decyduje się korzystać z ustawień domyślnych, poniżej znajdziesz najczęściej dostosowywane ustawienia.

Zezwalaj użytkownikom zalogowanym na urządzeniu na zmienianie kont w oknie przeglądarki	Możesz dać lub zablokować użytkownikom możliwość logowania i wylogowywania się z kont Google w przeglądarce. Możesz też zezwalać im na logowanie się tylko w określonych domenach Google Workspace. Dowiedz się więcej o logowaniu w przeglądarce.
Wymuszona ponowna rejestracja	Google zaleca niewyłączanie tego ustawienia. To ustawienie wymusza na wyczyszczonym urządzeniu ponowną rejestrację w Twojej domenie. Jeśli nie chcesz, aby urządzenie z Chrome było ponownie rejestrowane w domenie, musisz je wyrejestrować. Dowiedz się więcej o wymuszonej ponownej rejestracji.
Blokada ekranu	Wybierz ustawienie **Zawsze blokuj ekran po pewnym okresie nieaktywności**, aby poprawić bezpieczeństwo i zmniejszyć prawdopodobieństwo sytuacji, w której ktoś skorzysta z komputerów Twoich użytkowników pod ich nieobecność.
Wstępnie zainstalowane aplikacje i rozszerzenia	Wybierz aplikacje internetowe odpowiednie dla użytkowników – takie jak Gmail offline czy Dysk Google. Możesz też dodawać aplikacje do czarnej i białej listy, aby mieć większą kontrolę nad tym, które aplikacje z Chrome Web Store użytkownicy mogą instalować.
Przypięte aplikacje	Wybierz aplikacje, które mają być ukryte lub widoczne na pasku zadań w systemie. **Uwaga:** to ustawienie zezwala wyłącznie na aplikacje określone przez administratora. Użytkownicy utracą możliwość wyświetlania na pasku zadań własnego zestawu aplikacji.
Strony do załadowania podczas uruchamiania	To ustawienie stosuje się często do portalu intranetowego lub strony głównej. Niestety powoduje ono, że urządzenia z Chrome nie będą mogły przywracać kart przeglądarki z ostatniej sesji po zrestartowaniu urządzenia.
Ograniczenie logowania do listy użytkowników	Ograniczenie logowania do użytkowników w domenie **@twojadomena.com* uniemożliwia użytkownikom logowanie się za pomocą osobistego konta Google lub innego konta spoza domeny. Możesz kontrolować, kto może logować się na zarządzanym (zarejestrowanym) urządzeniu z Chrome.

Usuwanie wszystkich lokalnych danych, ustawień i informacji o stanie użytkowników po każdym wylogowaniu	Nie włączaj tego ustawienia, jeśli czynności wykonane przez użytkowników nie muszą być usuwane pomiędzy sesjami. Powoduje ono, że zasady dotyczące użytkowników będą pobierane ponownie po każdej sesji logowania.
Ustawienia automatycznej aktualizacji	Ustawienia automatycznej aktualizacji pozostaw domyślne. Aktualizacje urządzeń z Chrome odbywają się co 6–8 tygodni i obejmują nowe funkcje, naprawę błędów oraz łatki usuwające luki w zabezpieczeniach. Zalecamy też, aby 5% użytkowników w Twojej organizacji korzystało z wersji beta i deweloperskiej na potrzeby testowania działania przyszłych wersji Chrome OS w Twojej organizacji. Pełną listę zaleceń znajdziesz w artykule Wdrażanie aktualizacji automatycznych na urządzeniach z Chrome. **Uwaga:** aby zatrzymać pobieranie aktualizacji w tle przed zarejestrowaniem i ponownym uruchomieniem urządzenia, naciśnij Ctrl+Alt+E na ekranie umowy licencyjnej użytkownika. Jeśli tego nie zrobisz, pobrane aktualizacje, które powinny zostać zablokowane zgodnie z zasadami, mogą zostać zastosowane, gdy użytkownik ponownie uruchomi urządzenie.
Logowanie jednokrotne	W przypadku organizacji korzystających z logowania jednokrotnego (SSO), zanim wdrożysz to ustawienie w całej organizacji, wykonaj test z udziałem niewielkiej liczby użytkowników, aby upewnić się, że mogą oni zalogować się na swoich urządzeniach z Chrome. Jeśli używasz logowania jednokrotnego w Google Workspace na już posiadanych urządzeniach, rozważ korzystanie z funkcji Password Sync.

Przygotowywanie urządzeń do wdrożenia

Zanim rozdzielisz urządzenia z Chrome wśród użytkowników, muszą zostać one właściwie przygotowane, aby działały optymalnie. Musisz przynajmniej zarejestrować urządzenia z Chrome w domenie na potrzeby zarządzania nimi. Dzięki temu wszystkie przyszłe aktualizacje zasad dotyczących urządzeń będą stosowane na Twoich urządzeniach.

Jeśli wdrażasz małą liczbę urządzeń, zapoznaj się z krótkim przewodnikiem, w którym znajdziesz uproszczone instrukcje dotyczące rejestrowania i wdrażania urządzeń. Jeśli wdrażasz urządzenia dla większej grupy użytkowników, np. w kilku klasach, szkołach lub biurach, zapoznaj się z instrukcjami poniżej.

Aktualizowanie urządzeń z Chrome do najnowszej wersji

Urządzenia z Chrome OS automatycznie sprawdzają dostępność aktualizacji i pobierają je przez sieć Wi-Fi lub Ethernet. Urządzenia są aktualizowane do najnowszej wersji, o ile administrator nie ustawił ograniczenia w ustawieniach aktualizacji urządzeń. Jeśli jednak musisz zaktualizować wiele urządzeń i chcesz zachować przepustowość sieci, możesz użyć dysku USB przywracania, na którym znajduje się najnowsza wersja Chrome OS.

Aktualizacje z dysków USB stanowią najbardziej efektywną i wydajną metodę instalacji systemu na setkach lub tysiącach urządzeń z Chrome. Aktualizowanie przez USB to świetny sposób na oszczędność przepustowości sieci. Każde urządzenie musi pobrać pełną aktualizację systemu operacyjnego, która może przekroczyć rozmiar 400 MB na urządzenie.

Tworzenie obrazu Chrome OS

Aby ręcznie zaktualizować urządzenia z Chrome do najnowszej wersji Chrome OS za pomocą dysku USB, potrzebne będą:

1. informacje o producencie i modelu urządzenia z Chrome, które chcesz zaktualizować;
2. port USB 2.0 (lub nowszy), dysk flash o pojemności co najmniej 4 GB;
3. przeglądarka Chrome uruchomiona w systemie Chrome OS, Microsoft Windows lub macOS.
4. Zainstaluj aplikację Chromebook Recovery Utility i wybierz odpowiednią markę i model urządzenia, aby utworzyć dysk USB przywracania.

Kliknij tutaj, aby zapoznać się z dodatkowymi informacjami dotyczącymi aktualizowania, przywracania i czyszczenia urządzeń.
Uwaga: może minąć tydzień, zanim aktualizacja będzie dostępna w narzędziu do nagrywania obrazu.

Przygotowywanie urządzeń do wdrożenia

Aby przygotować i wdrożyć urządzenia:

1. Utwórz dyski USB przywracania lub zaktualizuj urządzenia bezprzewodowo. W przypadku więcej niż 10 urządzeń zalecana jest aktualizacja przez USB.
2. Po ponownym uruchomieniu urządzenia wybierz język, typ klawiatury i sieć Wi-Fi.
3. Po zaakceptowaniu Warunków usługi, a *przed zalogowaniem się na urządzeniu z Chrome*, naciśnij **Ctrl+Alt+E**. W lewym górnym rogu pojawi się napis „Rejestracja w firmie”.
4. Wpisz nazwę użytkownika i hasło (administratora lub użytkownika w domenie) i kliknij **Zarejestruj urządzenie**.

   Po zarejestrowaniu urządzenia wyświetli się komunikat „Urządzenie zostało zarejestrowane do zarządzania w firmie”.
5. Kliknij **Gotowe**, aby powrócić do początkowej strony logowania. U dołu strony powinien wyświetlać się komunikat „Tym urządzeniem zarządza *twoja_domena.com*”.

Powtórz te kroki na wszystkich urządzeniach z Chrome w organizacji. Więcej informacji na temat rejestrowania urządzeń znajdziesz w artykule Rejestrowanie urządzeń z Chrome.

Dodatkowa usługa („white glove”) przygotowania urządzenia (opcjonalna)

Dodatkowa usługa („white glove”) przygotowania umożliwia wdrożenie urządzeń z Chrome bez konieczności angażowania specjalistów IT. Zaletą umożliwienia sprzedawcy dokonania takiego przygotowania jest fakt, że dostarczone do Ciebie Chromebooki będą od razu gotowe do użycia. Użytkownicy będą sami mogli odpakować swoje urządzenie z Chrome lub wziąć je z koszyka, a następnie zacząć z niego korzystać bez konieczności konfiguracji. Podobnie jak w przypadku innych urządzeń komputerowych, z których korzystają użytkownicy, urządzenia z Chrome wymagają pewnej konfiguracji, aby zostały powiązane z odpowiednimi zasadami zarządzania w konsoli administracyjnej. Wielu oficjalnych sprzedawców urządzeń z Google Chrome świadczy taką usługę przed dostawą urządzenia.

Sprzedawca lub inna organizacja świadcząca dodatkową usługę („white glove”) przygotowania urządzenia w swojej siedzibie może uzyskać dostęp do konta innego niż konto administratora w Twojej domenie Google Workspace. Takie konto do rejestracji można nawet umieścić w jednostce organizacyjnej, w której wszystkie usługi są wyłączone.

Kroki, które należy wykonać po dodatkowej usłudze („white glove”) przygotowania, mogą obejmować:

- aktualizację Chrome OS;
- rejestrację w usłudze zarządzania Chrome OS;
- weryfikację zasad, w tym wstępnie skonfigurowanych sieci Wi-Fi;
- tagowanie zasobów;
- grawerowanie laserowe;
- pakiet urządzeń peryferyjnych.

Aby dowiedzieć się więcej, skontaktuj się ze sprzedawcą Twojego urządzenia z Chrome. Jeśli nie współpracujesz z partnerem, możesz wyszukać Partnera Google Cloud w Twoim regionie.

Wdrażanie aplikacji na Androida na urządzeniach z Chrome

Jeśli Twoja organizacja korzysta z urządzeń z Chrome obsługujących aplikacje na Androida, możesz wymusić instalację lub zdecydować, które aplikacje na Androida mogą pobierać użytkownicy. Aplikacje możesz udostępnić użytkownikom na 3 sposoby:

- Możesz wymusić instalację aplikacji na urządzeniach.
- Możesz wybrać zestaw aplikacji, które będą mogli pobierać użytkownicy.
- Możesz przyznać użytkownikom dostęp do wszystkich treści z zarządzanego Sklepu Google Play (ta opcja nie jest dostępna w przypadku Chrome Education).

Więcej informacji na temat włączania aplikacji na Androida na urządzeniach z Chrome w Twojej domenie i zatwierdzaniu aplikacji dla użytkowników znajdziesz w artykule Korzystanie z aplikacji na Androida na urządzeniach z Chrome OS.

Zanim zaczniesz

- Przed wdrożeniem aplikacji u wszystkich użytkowników Google zaleca przetestowanie aplikacji na Androida na urządzeniach z Chrome w pilotażowej jednostce organizacyjnej. Jeśli zdecydujesz, że nie chcesz już używać tej aplikacji, możesz ją wyłączyć i korzystać z urządzenia w ten sam sposób co wcześniej.
- Zapoznaj się z najczęstszymi pytaniami dotyczącymi aplikacji na Androida na urządzeniach z Chrome, aby uzyskać więcej informacji, które mogą Ci się przydać podczas wdrażania.

Uruchamianie aplikacji na Androida w trybie kiosku

Przy użyciu konsoli administracyjnej Google możesz instalować aplikacje na Androida na zarządzanych urządzeniach z Chrome w trybie zablokowanego kiosku. Umożliwia to wdrażanie aplikacji na Androida na urządzeniu kiosku i skonfigurowanie jej tak, aby uruchamiała się automatycznie.

Natywne drukowanie przy użyciu urządzeń z Chrome

Chrome OS obsługuje natywne drukowanie, co umożliwia użytkownikom łatwe i bezpośrednie łączenie się z drukarkami i serwerami drukowania bez dostępu do jakiejkolwiek infrastruktury opartej na chmurze. Chrome używa systemu CUPS (Common UNIX Printing System) do obsługi natywnego drukowania oraz protokołu IPP (Internet Printing Protocol) do obsługi drukarek lokalnych i sieciowych.

Jako administrator w konsoli administracyjnej Google możesz skonfigurować system CUPS. Gdy dodasz drukarkę, automatycznie pojawi się ona na liście drukarek Chrome użytkowników. Przed rozpoczęciem drukowania nie będzie potrzebna żadna dodatkowa konfiguracja. Więcej informacji znajdziesz w artykule Zarządzanie drukarkami lokalnymi i sieciowymi.

System CUPS obsługuje drukarki szerokiej gamy producentów, jak również drukowanie przy użyciu drukarek lokalnych i sieciowych.
Więcej informacji na temat dodatkowych opcji drukowania w Chrome OS znajdziesz w artykule Drukowanie na urządzeniach z Chrome.

Dostęp zdalny i wirtualizacja (opcjonalne)

Urządzeń z Chrome możesz używać do uzyskiwania dostępu do starszych wersji aplikacji w sytuacjach, gdy użytkownicy wymagają dostępu do:

- starszych aplikacji klienckich, takich jak Microsoft® Office®;
- stron internetowych wymagających starszych rozwiązań lub wyłącznie technologii firmy Microsoft (np. Internet Explorer);
- wtyczek innych niż Flash (np. Java® lub Silverlight) w przypadku aplikacji internetowych.

Najważniejsze funkcje

Aplikacje do wirtualizacji umożliwiają uruchamianie starszych wersji aplikacji na urządzeniach z Chrome lub używanie urządzeń z Chrome w już istniejącej zwirtualizowanej infrastrukturze aplikacji. Istnieje kilka rozwiązań wykorzystujących popularne protokoły zdalnego dostępu. Przykłady:

- Citrix Workspace
- VMware Horizon Client for Chrome
- ChromeRDP

Istnieją również takie aplikacje do wirtualizacji, jak Chromotif i Fra.me, które dobrze działają w Chrome OS.

Istotne kwestie dotyczące hostowania aplikacji

Jeśli aplikacje, do których chcesz mieć dostęp, znajdują się poza siedzibą organizacji (np. Microsoft® Office 365, aplikacje Oracle® Cloud czy hostowane aplikacje SaaS), zazwyczaj najłatwiej jest wdrożyć hostowane rozwiązanie – nie wymaga ono również konfigurowania serwera.

Jednak jeśli aplikacja, do której chcesz mieć dostęp, musi być hostowana w ramach Twojej zapory sieciowej lub jeśli chcesz wykorzystywać już istniejące serwery albo rozwiązania infrastruktury pulpitu wirtualnego (VDI), te rozwiązania mogą okazać się lepsze:

- VMware Horizon™ DaaS®
- Pulpit zdalny Chrome

Szczególne sytuacje związane z wdrażaniem urządzeń z Chrome

Urządzeń z Chrome można używać w różnych sytuacjach, a biorąc pod uwagę ich niski koszt, zdalne zarządzanie i rzadką konieczność serwisowania (lub nawet jej brak), zyskały popularność w określonych przypadkach użycia w firmach i szkołach. Obejmują one sytuacje od wyświetlania szkolnego kalendarza na wyświetlaczu cyfrowych treści informacyjno-reklamowych, przez współdzielenie laptopów w bibliotece, aż po zarządzanie egzaminami uczniów. Zapoznaj się z linkami poniżej, aby uzyskać dostęp do dodatkowych materiałów na temat wdrażania urządzeń z Chrome, które będą najlepiej dostosowane do Twoich potrzeb.

Osoba pracująca w chmurze

Urządzenia z Chrome stanowią świetne rozwiązania dla pracowników. Urządzenie z Chrome można przypisać do użytkownika, aby było ono jego głównym narzędziem uzyskiwania dostępu do aplikacji internetowych, narzędzi biurowych oraz do współpracy z innymi pracownikami.
Aby dowiedzieć się więcej o wykorzystaniu Chrome Enterprise na potrzeby osób pracujących w chmurze, obejrzyj te filmy na stronie Cloud Worker Live.

Jednofunkcyjna aplikacja kiosku

Możesz utworzyć aplikację kiosku obsługującą jedną funkcję, np. wypełnianie przez klienta wniosku o kredyt lub ankiety w sklepie albo danych potrzebnych do rejestracji przez ucznia. Więcej informacji

Kioski z zarządzaną sesją gościa

Możesz utworzyć kioski z zarządzaną sesją gościa do użytku w takich miejscach jak pokój socjalny dla pracowników czy wystawy sklepowe. Kiosk może też działać na współdzielonym urządzeniu w bibliotece – tam, gdzie użytkownicy nie muszą się logować, aby używać urządzenia z Chrome. Więcej informacji

Treści informacyjno-reklamowe

Możesz używać Chromeboksów jako wyświetlaczy treści informacyjno-reklamowych, takich jak szkolne kalendarze, tablice cyfrowe, menu restauracji czy interaktywne gry. Możesz utworzyć aplikację hostowaną lub aplikację w pakiecie i uruchomić ją na pełnym ekranie w trybie kiosku z pojedynczą aplikacją. Więcej informacji

Egzaminowanie uczniów

Chromebooki są bezpieczną platformą do egzaminowania uczniów, a po prawidłowej konfiguracji urządzenia te spełniają normy dotyczące testów w szkołach podstawowych i średnich. Chromebooki umożliwiają wyłączenie dostępu uczniów do internetu podczas egzaminu, a także wyłączenie obsługi zewnętrznych urządzeń do przechowywania danych oraz funkcji wykonywania zrzutów ekranu i drukowania.

Chromebooki możesz konfigurować na wiele sposobów na potrzeby testów, zależnie od rodzaju egzaminu – jako kiosk z pojedynczą aplikacją w domenie udostępnionej przez dostawcę testu lub przy użyciu kiosków z zarządzaną sesją gościa. Więcej informacji znajdziesz w artykule Używanie Chromebooków do egzaminowania uczniów.

Lista kontrolna gotowości do wdrażania

☐	**Infrastruktura sieciowa**	Czy masz odpowiednią infrastrukturę Wi-Fi i wystarczającą przepustowość sieci, aby wszystkie urządzenia mogły łączyć się z internetem w tym samym czasie? • Jakie jest dziś Twoje wykorzystanie przepustowości (przed dodaniem urządzeń z Chrome)? Czy sieć obsłuży szacowane zapotrzebowanie? • Czy w Twoim budynku są miejsca bez zasięgu sieci Wi-Fi?
☐	**Porównanie liczby starszych wersji aplikacji z aplikacjami internetowymi**	Ilu użytkowników wymaga korzystania ze starszych wersji aplikacji (w stosunku do aplikacji internetowych)? Czy rozważasz przejście na szersze wykorzystanie aplikacji internetowych i zasobów online przez użytkowników? Jeśli tak, kiedy to planujesz?

▢ Wykorzystanie wtyczek	Czy wiesz, jakie wtyczki są wymagane do uzyskiwania dostępu do stron, których muszą używać Twoi użytkownicy? Czy musisz skonfigurować rozwiązanie zdalne, aby sprostać tym potrzebom? Więcej informacji
▢ Drukarki	Czy Twoje drukarki zostały skonfigurowane na potrzeby natywnego drukowania (CUPS)? Zezwolisz na drukowanie wszystkim użytkownikom czy tylko niektórym?
▢ Urządzenia peryferyjne	Czy urządzenia peryferyjne, których Twoi użytkownicy potrzebują do pracy, współpracują z urządzeniami z Chrome? Przetestuj na przykład zestawy słuchawkowe, skanery kodów kreskowych i inne urządzenia peryferyjne, które musisz wdrożyć, zanim przekażesz je użytkownikom.
▢ Schemat uwierzytelniania	W jaki sposób użytkownicy będą logować się na komputerach? Jak będziesz zarządzać hasłami do Wi-Fi i dostępem do sieci Wi-Fi? Czy stosujesz logowanie jednokrotne jako metodę uwierzytelniania na urządzeniach z Chrome? Czy używasz też funkcji Google Workspace Password Sync (GSPS)? Czy korzystasz z Cloud Identity?
▢ Daty ważnych etapów projektu	Czy postępy wdrażania są zaplanowane? Czy użytkownicy mają zapewnioną możliwość dzielenia się opiniami na temat doświadczeń związanych z używaniem urządzeń z Chrome? Jak długo będzie trwał okres oceniania, jakie rodzaje ankiet otrzymają Twoi użytkownicy i jak często będziesz gromadzić ich opinie oraz dane dotyczące użytkowania?
▢ Szkolenie użytkowników	Jeśli przejście na Chromebooki odbywa się z innej platformy, czy przeprowadzisz szkolenie dla użytkowników? Jeśli masz dział ds. szkoleń, możesz samodzielnie zorganizować szkolenie. Jeśli nie, niektórzy Partnerzy Google Cloud Premier oferują szkolenia dotyczące Chromebooków.
▢ Przygotowanie zespołu pomocy	Czy Twój zespół pomocy zaznajomił się z Centrum pomocy Chrome Enterprise? Zapoznanie się z materiałami wymienionymi na kolejnej stronie i uczestnictwo w szkoleniach może pomóc Twojemu zespołowi pomocy i działowi IT szybko odpowiadać na pytania związane z Chromebookami.

Dodatkowe materiały i pomoc

Aktualności dotyczące urządzeń z Chrome

- Regularnie czytaj bloga Google Chrome i bloga poświęconego wersjom Chrome.
- Śledź informacje o wersjach Chrome Enterprise.

Klienci Google Workspace mogą też odwiedzić:

- stronę Co nowego w Google Workspace,
- bloga Google Cloud.

Materiały w Centrum pomocy

- Chrome Enterprise
- Chromebook (dla użytkowników)
- Chromebox wideokonferencje
- Jak zalogować się w konsoli administracyjnej

Wskazówki dotyczące samodzielnego rozwiązywania problemów

- Pobieranie dzienników urządzenia z Chrome
- Rozwiązywanie problemów z Chromebookiem (dla użytkowników Chromebooków)
- Znane problemy (Chrome Enterprise)
- Analizator logów (Zestaw narzędzi Google Workspace) – analiza katalogów **/var/log/messages** i **/var/log/chrome/** w poszukiwaniu błędów
- Zarządzanie egzaminami na Chromebookach

Uzyskiwanie pomocy

Pomoc związaną z problemami, które mogą wystąpić podczas korzystania z oprogramowania i usług na urządzeniach z Chrome, świadczymy przez telefon i e-mail. Zobacz opcje pomocy związane z urządzeniami z Chrome.