# Introduction to Declarative MDM

**DDM** 

Declarative Device Management

**MDM** 

Mobile Device Management

## What is MDM?

## • API for sending device management commands

- For iOS, usable on iOS 4.x and later.
- For macOS, usable on 10.7.x and later.
- For tvOS, usable on tvOS 10.x and later.
- Not all MDM commands are backwards-compatible







## Why use it?







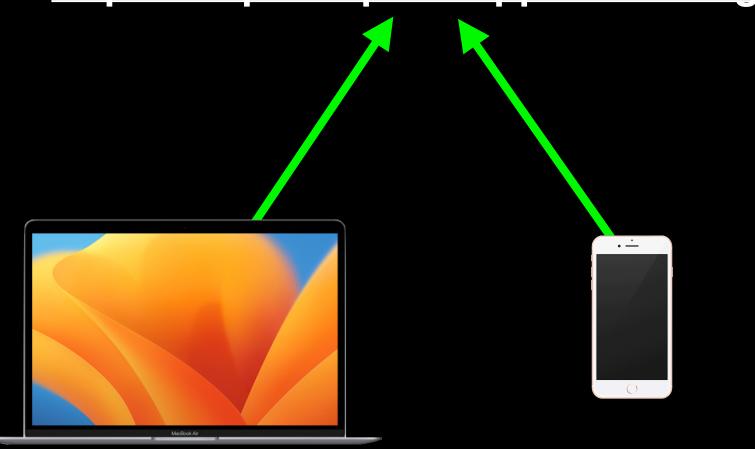
## How does MDM management work?

- Apple's push notification services (APNS)
- Mobile device management (MDM) server





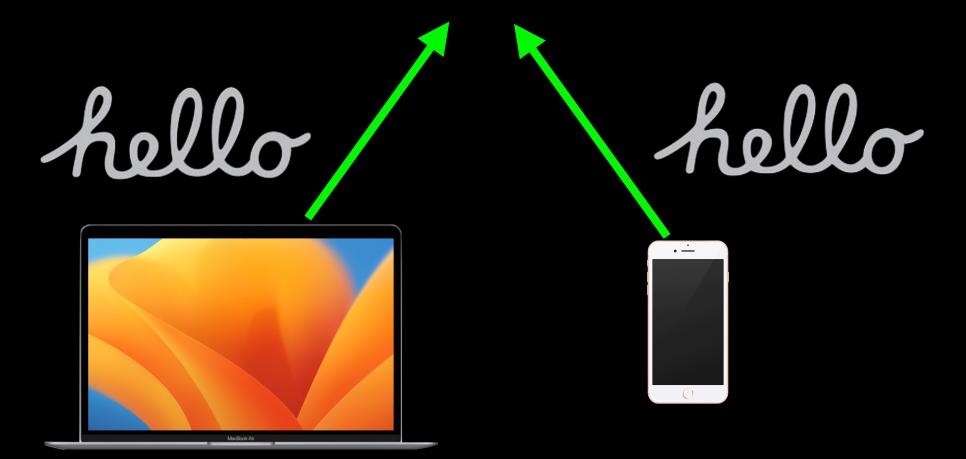
#### http://init-p01st.push.apple.com/bag



```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<pli><pli><pli><pli>version="1.0">
    <dict>
        <key>signature</key>
<data>BflfmeYAToSiBTn0AlHGE91F5uL4cdULBy4YLkpftLJ9A2qX4Z7ljxd6ZykCtwsm66/JAhjVKqmG3/505gvXpkRB7r0VJfyx1tZ9zyXqAiMNBdqoKd+62NK+N50WAitKgi5gRdQMraL/Wsx3aNY/7za+
PvyzxSAsaWMFgp0RP/j8sQL7lVp2KyF6AyygS0N3NursZKDqNHM5qHNeVo/xoJ0aYI9LZ/
Mrwc8EU4m8wUA6cjeHBIiy5Z2JImxOEPaYABeMpCJ98PVfqvqa9bOmaqPmPKnWscdzMzw0asJJDb7sQXY55lymwnh1vYccutGQWrSChZ8pBXbnj4lu+RDBDw==</data>
        <key>certs</key>
        <array>
MIIFRİCCBCGaAwIBAgIOXguİPtScX2cAAAAAUN5PkzANBakahkiG9w0BAOsFADCBuİELMAkGA1UEBhMCVVMxFİAUBaNVBAoTDUVudHJ1c3OsIEluYy4xKDAmBaNVBAsTH1N\ZSB3d3cuZW50cnVzdC5uZXQvbGVnYWwt
dGVybXMxOTA3BqNVBAsTMChjKSAyMDEyIEVudHJ1c3QsIELuYy4qLSBmb3IqYXV0aG9yaXplZCB1c2Uqb25seTeUMCwGA1UEAxMlRW50cnVzdCBDZXJ0aWZpY2F0aW9uIEF1dGhvcml0eSAtIEwxSzAeFw0xNzA5Mjkx
NZAVMTNAFwØxDTASMigxNZMVMTJAMG8xCZAJBgNVBAYTALVTMŔMwEQYDVQQÍEwpDYwxóZm9ybmlhMRIwEAYDVQQHEwlDdXBlcnRpbm8xEZARBgNVBAOTCKFwcGxlIEluYy4xIjAgBgNVBAMTGWluaXQtcDAxc3QucHVZ
aC5hcHBsZS5jb20wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKA0IBAQDZcQxsOe+k06rGzjHosZBbaLBoiwmVhbXTs60Zbz2YAwT/
1qJeToldRnGWks7TafG6Nhfme0QH2gYYf11NUyC65z6rx0Gnhqe94sp4TD4ueawAYnsn+bzkC8VPQuP7KGM6Kvk4lL5EimA09vh0STYmKESe0YqupHCEy+J9zfHR/
pSqDhRhVXHNpLqm4Hmr4H0eebulfKaCQIBAwaVwhAvfMNl3U5Lp00EsFCiUyhFgdvyR8l9Y68MU9ITft042z9+Dc+LG4sGjiWVlL3nOyuqAyElcvDBillzVxjdnPHbU8ip9VhBaaIsQzpq8GxdYZodt+
r3\dkU0pNu7uE9AIKWZAgMBAAGiggG0MIIBiDA0BgNVH08BAf8EBAMCBaAwH0YDVR0\BBYwFAYIKwYBB0UHAwEGCCsGA0UFBwMCMDMGA1UdHw0sMCowKKAmoCSGImh0dHAGLy9icmwuZW50cnVzdC5uZX0ybGV2ZWwxa
y5jcmwwSwYDVR0gBEQw0jA2BgpgnKgBhvpsCgEFMCgwJgYIKwYBBQUHAgEWGmh0dHA6Ly93d3cuZW50cnVzdC5uZXQvcnBhMagGBmeBDAECAjBoBggrBgEFBQcBAQRcMFowIwYIKwYBBQUHMAGGF2h0dHA6Ly93V3NwL
mVudHJ1c3QubmV@MDMGCCsGAQUFBzAChidodHRwOi8yVWlhLmVudHJ1c3QubmV@L2wxaý1jaGFpbjI1Ni5jZXIwJAYDVR@RBB@wG4IZaW5pdC1wMDFzdC5wdXNoLmFwcGxlLmNvbTAfBqNVHSMEGDAWgBSConB@3bxTP
8971PfNf6dgxgpMvzAdBqNVHQ4EFqQUhhd/lweSvsZr6D0kMcH+ZuKwtvswCQYDVR0TBAIwADANBqkqhkiG9w0BAQsFAA0CAQEAWkt4Jb9WrYCMIfW/+
imgU8f3Eb3KSbw08jrvtVmV08De22USIb9I5HbNzXZEld6uD3VAMixAf0riEfev1T0D3v00cti8pp7peAU5U05zvDa8WJmgSlvdsZe7WIdlkMi2YuFY21lhxhHLgaaeWuePv+wbd720H0IxCf1m20v7/
hozOW7xlz9mD00obgrBG0BUQw0TxtycmLI5FycYhw53MaJlsKm7Y5nliCPziqHL5zSSBMf35MEQwffdGpp/YM/Nz8YZQXqV02gFFvAJoiSdZE4A2bm+dMHIzR6PGy1imoBcsPqmwssk4/
q0qrC0pSZhs3buInq2FnxQGaWv8YFobg==</data>
<data>MIIE/jCCA+agAwIBAgIEUc4A/jANBgkqhkiG9w0BAQsFADCBtDEUMBIGA1UEChMLRW50cnVzdC5uZXQxQDA+
BQNVBASUN3d3dy5lbnRydXNØLm5ldC9DUFNfMjA00CBpbmNvcnAuIGJ5IHJlZi4qKGxpbWl0cyBsaWFiLikxJTAjBqNVBASTHChjKSAxOTk5IEVudHJ1c3QubmV0IExpbWl0ZWQxMZAxBqNVBAMTKkVudHJ1c3QubmV0
IENlcnRpZmljYXRpb24qQXV0aG9yaXR5ICqyMDQ4KTAeFw0xNDEwMTAxNTIzMTdaFw0yNDewMTEwNjIyNDdaMIG6MQswCQYDVQQGewJVUzEWMBQGA1UEChMNRW50cnVzdCwgSW5jLjEoMCYGA1UECxMfU2VlIHd3dy5l
bnRydXN0Lm5ldC9sZWdhbC10ZXJtczE5MDcGA1UECxMwKGMpIDIwMTIgRW50cnVzdCwgSW5jLiAtIGZvciBhdXRob3JpemVkIHVzZSBvbmx5MS4wLAYDVQQDEyVFbnRydXN0EnltcRpZmljYXRpb24gQXV0aG9yaXR5
ICOgTDFLMIIBIjANBgkghkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA2j+W0E25L0Tn2zlem1DuXKVh2kFnUwmgAJgOV38pa9vH4SEkgjrOjUcj0u1yFvCRIdJdt7hLgIOPt5EyaM/
OJZMSsn2XyP7BtBe6CZ4DkJN7fEmDImiKm95HwzGYei59QAvS7z7Tsoyqj0ip/wDoKVqG97aTWpRzJiatWA7lQrjV6nN5ZGhTJbiEz5R6rqZFDKNrTdDGvuoYpDbwkrK6HIiPOlJ/915tqxyd8B/
lw9bdpXiSPbBtL0rJz5RBGXFEaLpHPATpXbo+8DX3Fbae8i4VHi9HvMqdp3NFXU2w07G0Fvk36t0FASK7lDYqiV$1/lMZLwhGwSqzGmIdTivZGwIDA0ABo4IBDiCCAOowDqyDVR0PA0H/BA0DAqEGMBIGA1UdEwEB/
wOIMAYBAf8CAOAwMwYIKwYBBOUHAOEEJzAlMCMGCCSGAOUFBzABhhdodHRwOi8vb2NzcC5\bnRvdXN0Lm5\dDAyBaNVHR8EKZApMCegJaAihiFodHRwOi8vY3JsLmVudHJic3OubmV0LzIwNDhiYS5icmwwOwYDVR0gB
D0wM] AwbgRVHSAAMCgw)gYTKwYBBQUHAgEWGmh0dHA6Ly93d3cuZW50cnVzdC5uZXQvcnBhMB0GA1UdDgQWBB5ConB03bxTP8971PfMf6dgxgpMvzAfBgNVHSMEGDAWgBRV51HREYC+21m5CKMx+
aEkCRa5cDANBgkqhkiG9w0BAQsFAAOCAQEAWEJxwT4pFm51WHe1ZU2eKfWuCxwY+aMIQ3XvfW3xkur+zmhc4h++pa8aTKqD01+iR0b3fJ7Bg8R6JLDpz0mimgcJ6B4dd1ZJ/
FNzqEfMyS1aYDSnGgvlK7jf74JK3XBeEBg1013cioQ9aNgAtMSeQ3hLXvBiaoyQZlOKrMV9WP90qa3XpMoSRynl8yIhQDJg2jr+klQeQ6ENqVI3YL+HxKHHeWWHHuV3419b3HFtukSHMQWAWAvF3nQogYMIhNDIRlr+
isa9q047ZHhtJtw8TPeBXDwRfyU6k2Klo5EFJSNztM30zDmkA3qwZkZeqXWwtGcDqbGfV/DTds/hk+iAoq==</data>
        </array>
        <key>bag</key>
<data>PD94bWwqdmVvc2lvbi0iMS4wIiBlbmNvZGluZz0iVVRGLTqiIHN0YW5kYWxvbmU9InllcvI/
Pgo8IURPQ1RZUEUgcGxpc3QgUFVCTE\DICItLy9BcHBsZS8vRFREIFBMSVNUIDEuMC8vRU4iICJodHrw0i8vd3d3LmFwcGxlLmNvbS9EVERzL1Byb3BlcnR5TG\zdC0xLjAuZHrkIj4KPHBsaXN0IHZ\cnNpb249IjEu
Cgk8ZGljdD4KCQk8a2V5PkFQTlNDb3VyaWVySG9zdG5hbWU8L2tleT4KCQk8c3RyaW5nPmNvdXJpZXIucHVzaC5hcHBsZS5jb208L3N0cmluZz4KCgkJPGtleT5BUE5TQ291cmllckhvc3Rjb3VudDwva2V5PgoJCTxp
bnRlZ2VyPjUwPC9pbnRlZ2VyPgoKCQk8a2V5PkNsaWVudENvbm5lY3Rpb25SZXRyeUF0dGVtcHRzPC9rZXk+CgkJPGludGVnZXI+MTAwPC9pbnRlZ2VyPgoKCQk8a2V5PkFQTlNDb3VyaWyyU3RhdHVzPC9rZXk+
CakJPHRVdWUvPaoKCOk8a2V5Pm1pbkNvbnNlY3V0aXZlS2VlcEFsaXZlc01haW50YWluaW5nV2lGaUNvbm5lY3Rpb248L2tleT4KCOk8aW50ZWdlc14XMDwvaW50ZWdlc14KCakJPGtleT5taW51dGVzRGlzYWJsZVN3
aXRjaGlúZ1RvVŽlGaUZyb21DZWxsdWxhcjwva2V5PqoJCTxpbnRlZ2VyPj61PC9pbnRlZ2VyPqoKC0k8a2V5PkF0TlN0dW1iZXJPZkNyaXRpY2FsTWVzc2FnZUtlZXBBbGl2ZXNCZWZvcmVEaXNjb25uZWN0aW5nPC9r
ZXK+CqkJPGludGVnZXI+MzwvaW50ZWdlcj4KCqkJPGtleT5BUE5TQ3JpdGljYWxNZXNzYWdlS2VlcEFsaXZlVGltZXJEdXJhdGlvbjwva2V5PqoJCTxyZWFsPjEwLjA8L3JlYWw+CqoJCTxrZXK+
QVBOUΘNyaXRpY2FsTWVzc2FnZVRpbwVvdXQ8L2tleT4KCQk8cmVhbD4xMC4wPC9yZWFsPgoKCQk8a2V5PkFQTlNXV0F0VHJhY2tlZ€xpbmtRdWFsaXR5VGltZUludGVydmFsPC9rZXk+CgkJPHJlYWw+
NiAwLiA&L3JlYWw+CgoJCTxrZXk+0VB0U1dX0U5UcmFia2VkTGlua1F1YWxpdHlPZmZUcmFuc2l0aW9uczwya2V5PgoJCTxpbnRlZ2VyPiI&L2ludGVnZXI+CgoJCTxrZXk+
QVBOU0FXRFNsb3dSZWNlaXZlVGhyZXNob2xkPC9rZXk+CqkJPHJlYWw+NjAuMDwycmVhbD4KCqkJPGtleT5BUE5TTG93UHJpb3JpdHlNZXNzYWdlQmF0Y2hTaXplPC9rZXk+CqkJPGludGVnZXI+NTA8L2ludGVnZXI+
CgoJCTxrZXK+QVB0U0FjdGl2ZUlúdGVydmFsPC9rZXk+CgkJPGludGVnZXI+NTwvaW50ZWdlcj4KCgkJPGtleT5BUE5TRm9ÿY2VkU2hvcnRUaW1lb3V0SW50ZXJ2YWw8L2tleT4KCQk8cmVhbD4yLjA8L3JlYWw+
CgoJCTxrZXk+QVB0U0Nvc3REcml2ZWSEdWFsQ2hhbm5lbEF0dGVtcHRzPC9rZXk+CgkJPGludGVnZXI+MTAwPC9pbnRlZ2VýPgoKCQk8a2V5PkFQTlNQaWdneWJhY2tEdWFsQ2hhbm5lbEF0dGVtcHRzPC9rZXk+
CgkJPGludGVnZXI+NTA8L2ludGVnZXI+CgoJCTxrZXk+QVB0U01heGltdW1Mb3dQcmlvcml0eUJhdGNoZXNQZXJIb3VyPC9rZXk+CgkJPGludGVnZXI+
MzwvaW50ZWdlcj4KCqkJPGtleT5BUE5TRGlzYWJsZUNvc3REcml2ZW5EdWFsQ2hhbm5lbDwva2V5PqoJCTxmYWxzZS8+CqoJCTxrZXk+
QVBDUØxvd1ByaW9yaXR5QnVyc3RXaW5kb3c8L2tleT4KCQk8cmVhbD4zMC4wPC9yZWFsPgoKCQk8aZV5PkFQTlNMb3dQcmlvcml0eUJ1cnN0RGVsYXk8L2tleT4KCQk8cmVhbD4xMjAwLjA8L3JlYWw+CgoJCTxrZXk+
QVBOUØxvd1ByaW9yaXR5QnVyc3RTZW5kUHJvYmFiaWxpdHk8L2tleT4KCQk8cmVhbD4wLjg8L3JlYWw+CgoJCTxrZXk+S2VlcEFsaXZlVjJUaW1lRHJpZnRNYXhpbXVtPC9rZXk+CgkJPGludGVnZXI+
MDwvaW50ZWdlcj4KCqkJPGtleT5LZWVwQWxpdmVwMlrobWVEcmlmdE1heEFsbG93ZW08L2tleT4KCQk8aW50ZWdlcj4zMDwvaW50ZWdlcj4KCqkJPGtleT5BUESTSVBDYWNoaW5nYFRMTWludXRlczwva2V5PqoJCTxp
bnRlZ2VyPjE0NDA8L2ludGVnZXI+CqoJCTxrZXk+QVB0U0lQQ2FjaGluZ1BlcmNlbnRhZ2U8L2tleT4KCQk8aW50ZWdlcj4wPC9pbnRlZ2VyPqoKCQk8a2V5PkVudmlyb25tZW50PC9rZXk+
CakJPHN0cmluZz50cm9kdWN0aW9uPC9zdHJpbmc+CqoJCTxrZXk+0VB0U05hZ2xlRW5hYmxlZDwva2V5PqoJCTxmYWxzZ58+CqoJCTxrZXk+
OVBOU01pbmltdW1JbnRlcnZhbEZhbGxiYWNrRW5hYmxlZDwva2V5PgoJCTx0cnVlLz4KCqkJPGtleT5BUESTSVBDYWNoaW5nVFRMTWludXRlc1YvPC9rZXk+CqkJPGludGVnZXI+
MTQ0MDwvaW50ZWdlcj4KCgkJPGtleT5BUE5TV2lGaUtlZXBBbGl2ZUVhcmx5RmlyZUNvbnN0YW50SW50ZXJ2YWw8L2tleT4KCQk8aW50ZWdlcj4xMjA8L2ludGVnZXI+CgoJCTxrZXk+
QVBOU0NvdXJpZXJIb3N0c1ByaW1hcnlJUHY0PC9rZXk+CgkJPGFycmF5PgoJCTwvYXJyYXk+CgoJCTxrZXk+QVB0U0NvdXJpZXJIb3N0c1ByaW1hcnlJUHY2PC9rZXk+CgkJPGFycmF5PgoJCTwvYXJyYXk+
CgoJCTxrZXk+QVB0U0NvdXJpZXJIb3N0c1NlY29uZGFyeUlQdjQ8L2tleT4KCQk8YXJyYXk+
CgkJPC9hcnJheT4KCgkJPGtleT5BUE5T0291cmllckhvc3RzU2Vjb25kYXJ55VB2Njwva2V5PgoJCTxhcnJheT4KCQk8L2FycmF5PgoKCQk8a2V5PkFQTlNDb3VyaWVySG9zdHNEZWZhdWx0SVB2NDwva2V5PgoJCTxh
cnJheT4KCQk8L2FycmF5PgoKCQk8a2V5PkFQTlNDb3VyaWVySG9zdHNEZWZhdWx0SVB2NjwvaZV5PgoJCTxhcnJheT4KCQk8L2FycmF5PgoKCQk8a2V5PkFQTlNCYWdfeHBpcnk8L2tleT4KCQk8aW50ZWdlcj4xMDgw
MDwvaW50ZWdlcj4KCgkJPGtleT5BUE5TRGVmZXJyZWRIb3NÓVGltZW91dDwva2V5PgoJCTxpbnRlZZVyPjM2MDA8L2ludGVnZXI+CgoJCTxrZXk+
OVBOU0ZpcnN0VW5sb2NrRGVsaXZlcnlTdGF0dXN0cm9iYWJpbGl0eTwva2V5PqoJCTxpbnRlZ2VyPjE8L2ludGVnZXI+CqoJPC9kaWN0Pqo8L3BsaXN0Pqo=</data>
```



#### **APNS**



## hello APNS hello







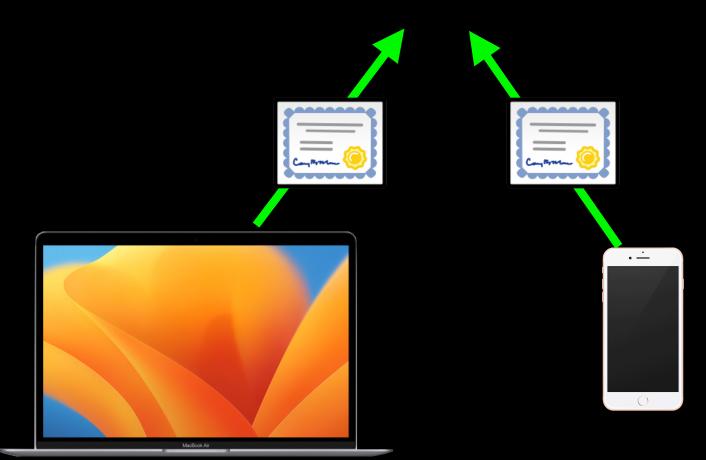






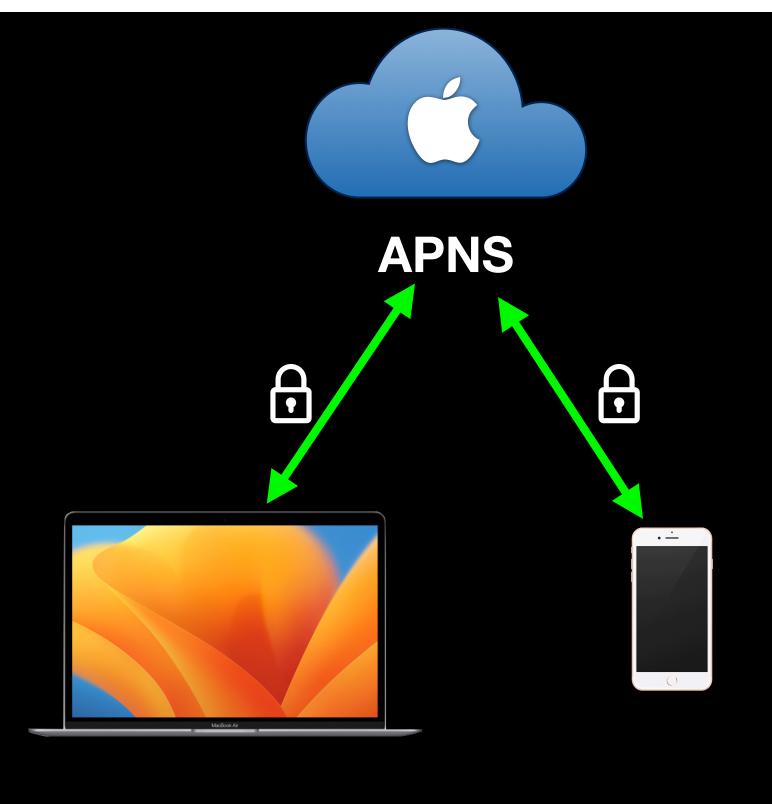


## **APNS**

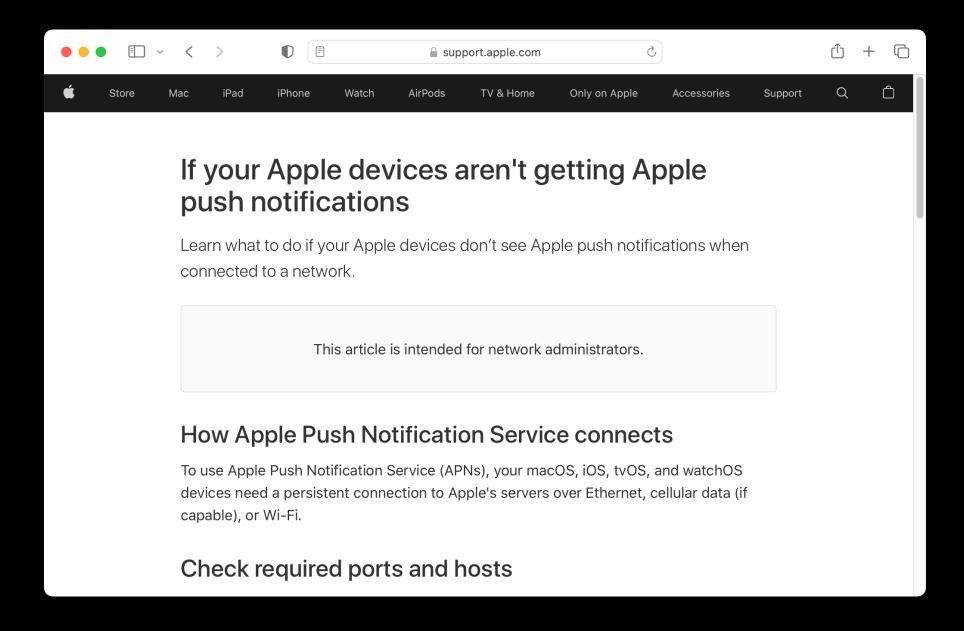




## APNS







#### https://support.apple.com/HT203609

#### Check required ports and hosts

If you use a firewall or private Access Point Name for cellular data, your Apple devices must be able to connect to specific ports on specific hosts:

- TCP port 5223 to communicate with APNs.
- TCP port 443 or 2197 to send notifications to APNs.

TCP port 443 is used during device activation, and afterwards for fallback if devices can't reach APNs on port 5223. The connection on port 443 uses a proxy as long as the proxy allows the communication to pass through without decrypting.

The APNs servers use load balancing, so your devices don't always connect to the same public IP address for notifications. It's best to let your device access these ports on the entire 17.0.0.0/8 address block, which is assigned to Apple.

- APNS never needs an inbound network connection on your network.
- Only <u>outbound</u> connections from your network to Apple's network (17.0.0.0 / 8) are needed for APNS.
- APNS never makes unsolicited connections.
- APNS uses TLS 1.2
- APNS authenticates all transactions with device tokens and payload tokens, and validates all SSL certificates.



If you can't allow access to the entire 17.0.0.0/8 address block, open access via the same ports to these network ranges on IPv4 or IPv6:

#### IPv4

- 17.249.0.0/16
- 17.252.0.0/16
- 17.57.144.0/22
- 17.188.128.0/18
- 17.188.20.0/23

#### IPv6

- 2620:149:a44::/48
- 2403:300:a42::/48
- 2403:300:a51::/48
- 2a01:b740:a42::/48

• •		'	Push Diagnostics				
Status	∨ Host	Port	Platform	IP Address	Reverse DNS	Category	
Pass	itunes.apple.com	443	iOS, tvOS, and macOS	23.55.204.23	a23-55-2	App Store	
Pass	appldnld.apple.com	80	iOS only	17.253.21.202	usqas2-vi	Software updates	
Pass	tbsc.apple.com	443	macOS only	17.171.47.75		Device setup	
Pass	ocsp.apple.com	80	iOS, tvOS, and macOS	17.253.21.205	usqas2-vi	Certificate validation	
Pass	ocsp.entrust.net	80	iOS, tvOS, and macOS	23.13.165.231	a23-13-1	Certificate validation	
Pass	skl.apple.com	443	macOS only	17.171.47.7	skl-mdn	Software updates	
Pass	captive.apple.com	80	iOS, tvOS, and macOS	17.253.21.206	usqas2-vi	Device setup	
Pass	static.ips.apple.com	80	iOS, tvOS, and macOS	23.1.193.76	a23-1-19	Device setup	
Pass	gg.apple.com	80	macOS only	17.171.47.69		Software updates	
Pass	vpp.itunes.apple.com	443	iOS, tvOS, and macOS	17.125.249.4		Device setup	
Pass	osrecovery.apple.com	443	macOS only	17.42.252.38		Software updates	
Pass	5-courier.sandbox.pus	443	iOS, tvOS, and macOS	17.188.178.92		APNS	
Pass	updates-http.cdn-appl	80	iOS, tvOS, and macOS	17.253.21.206	usqas2-vi	Software updates	
Pass	5-courier.push.apple.c	5223	APNS	17.57.144.55	-	APNS	-
Pass	crl.entrust.net	80	iOS, tvOS, and macOS	23.62.230.72	a23-62-2	Certificate validation	
Pass	5-courier.push.apple.c	443	APNS	17.57.144.55		APNS	-

#### https://twocanoes.com/products/mac/push-diagnostics/

## A Push Odyssey: Journey to the Center of APNS:

https://www.youtube.com/watch?v=Z-Lg9uBbmfk

#### What's an MDM server?

- 1. HTTPS server
- 2. Needs to be able to respond with both of the following:

- HTTP 200 OK
- A plist in XML format which contains a command.

### Perpetual plist passing

```
<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<pli><pli><pli><pli>version="1.0">
  <dict>
    <key>Command</key>
    <dict>
      <key>Options</key>
      <dict></dict>
      <key>Queries</key>
      <array>
        <string>foo</string>
        <string>bar</string>
      </array>
      <key>RequestType</key>
      <string>DeviceInformation</string>
    </dict>
    <key>CommandUUID</key>
    <string>7564fecc-f1b5-4d2d-af17-986fdd68a252</string>
  </dict>
</plist>
```

### Perpetual plist passing

#### **MDM Server Certificates**

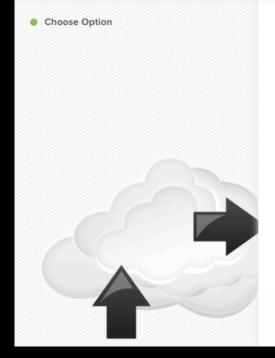
- APNS Vendor Certificate
- APNS Push Certificate



#### **MDM Server Certificates**

- APNS Vendor Certificate
  - Used to sign APNS push certificate's certificate requests (CSRs)

#### **Push Certificates**

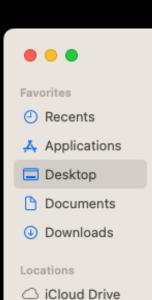


#### Choose an Option

- Download signed CSR from Jamf Nation
- Download CSR and sign later using Jamf Nation
- Upload push certificate (.p12)
- Get proxy server token from Jamf Authorization Server

Cancel

Next





Desktop

JAMFSignedCSR.plist

₩ \$

» Q

PD94bWwgdmVyc2lvbj0iMS4wIiBlbmNvZGluZz0iVVRGLTgiPz4KPCFET0NUWVBFIHBsaXN0IFBVQkxJQyAiLS8vQXBwbGUvL0RURCBQTElTVCAxLjAvL0V0IiAiaH R0cDovL3d3dy5hcHBsZS5jb20vRFREcy9Qcm9wZXJ0eUxpc3QtMS4wLmR0ZCI+CjxwbGlzdCB2ZXJzaW9uPSIxIj4KICA8ZGljdD4KICAgIDxrZXk+ UHVzaENlcnRTaWduYXR1cmU8L2tleT4KICAgIDxzdHJpbmc+

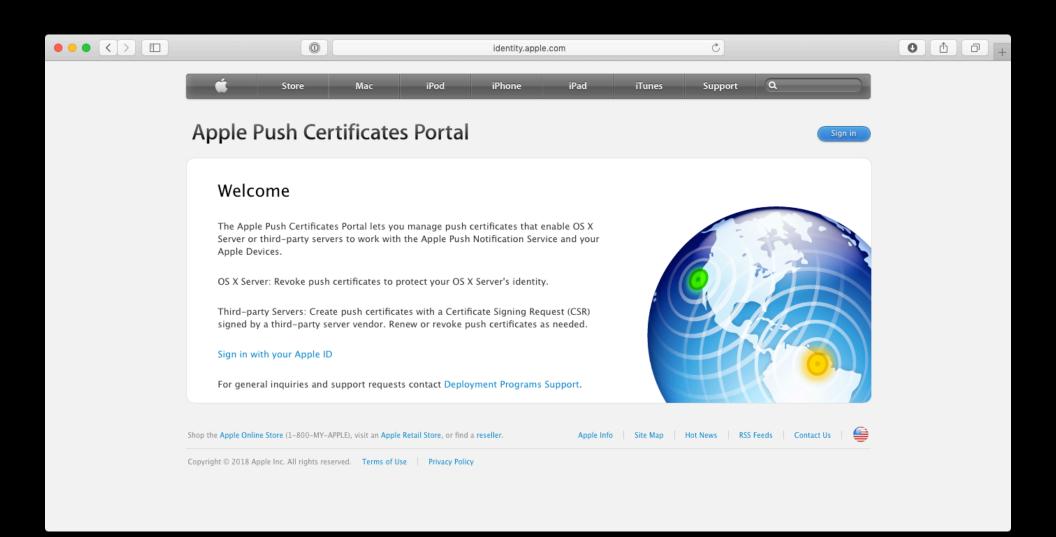
aTkvLzZTWlpXVEl2UnZiVDVQMLA4Wm1zOURvMkF3QWVLdzNTei9vaXJ4NEd6cVZMeVhIWUlybXFuOWYrckRaT2x6ckNsZE5ZdUF0TDN1RlRwOEJScUxxMzNOZXpYTH
JsNGR3TnhWSEJtbXRzKy9PblBHdmzjZFBrSGQ0RWZLTlJtWTlCT2c5UitKK0lSQmo3bEhEeERGS1RvWWhsQTZYK0k1eW5MdEpIYUR3RHQyY2JRVWE2aERmM3BFUmo5
RE13ZUVmaytjazBodDczNmd4SRUMwY1RJdTBRc0Z5NzlbUTh4RlpLQXh4NmxwWm9UbWVwYncyTGVjZjF6QU9JTGY0dT1MRmd6UElvMS9WVUFka3JpTXlyRXFMd2cyWX
U2RU0rcmF3VVpXbUIrcjdwUUVCNDY0Q1pQckh4aC95cXNneHBvcVFxNzhnNEQ3aU50Wm1jMVZXZDZBPT08L3N0cmluZz4KICAgIDxrZXk+
UHVzaENlcnRSZXF1ZXN001NSPC9rZXk+

CiAgICA8c3RyaW5nPk1JSUNXakNDQVVJQ0FRQXdGekVWTUJNR0ExVUVBd3dMUTT5dGNHRnV1U0JPWVcxbE1JSUJJakF0QmdrcwhrauC5dzBCQVFFRkFBT0NBUThBTU
LJQkNn50MBUUVBakMvbG1IMldsM04zWDBZTVRYdTg1QmsxWnVUN1ZuVGdDRLpYc1dZNEpPWXZYZFwQ0VKTUpveFhwbkxNZnRFUmx65mowT2NOMWg3VzkxeHpIWEZU
MDVxTnpCMXBXNKF5dkZHUXRCSFAZUKZYQj lnUVRjbUkva2g9bWYyUHJwTXZWcj voeURYdWdPUkhj0WxxZGkyTbWsCptVi85cHY30cBdcHzKMVUVZ1grVERRRUN0ddHdhdF
J5bFJybmJLbXhZem5QVis5QTdRSkRoa1dZMGd1YzZ0anNqTzNxRUNyc3ZtZHRyc045bDUwdnAzVVFqMnZYbGozVGtQZVJsN1ptYXB30VFHSXd00XBuS2x2V3RsYnNn
Y0pnSGZCWnFtWmZGME90T0ZQWm00amkxbTdRWlU4NkZ55jc0cUcrYy8wYE9WMnF1UEFUMG95a0loeExEWGUyU1NGR0FRSURBUUFCTUEwR0NTCUdTSWIZRFFFQkJRVU
FBNElCQVFCUEgzRHZsMXNmdWprMnB2MjNTNnFock9Vwij9kRXptWTRtd3RRR045NlbjdMnybGZhbWRXVVdwRDhBZ0owa21BNmxUTmJaWmx1MlU4VFpEUFZxc0MrTTJo
OHoySzllVTFaNFkyc1BnbXhQMVFLdmtqSDJWUUtkbTNtTjJtQ0JNZUdGYUM4T3VPR2dEclkyVFN1VHpQbGdYVA5R3hXbGEwcy9ub2R1VGVXRHV1alLUYnc0VE0xOV
REaTJuQlVOdmQ05zBIWHJqMWpzMkxxSWlPMndlK2kwUEFwbUFaNmpHVjg4NHNkbFVxU3NROVhnWVVZMXgxalc5MHZmTjgzNmlldkpHMjBKM3lLNWJqTkxERmJNYVh2
eWkxWnRuek9MRThwa2lioDRZ0DhtNzQSMkJUtKhXbzZ5a1BkQ05ZQ29rT1B0ajF0bkQzUWdBY1oreksxLzdTRHA8L3N0cmluzz4KICAgIDxrZXk+
UHV2aENDZXJ08WZDY2F0ZUNOYWluPc9rZXk+

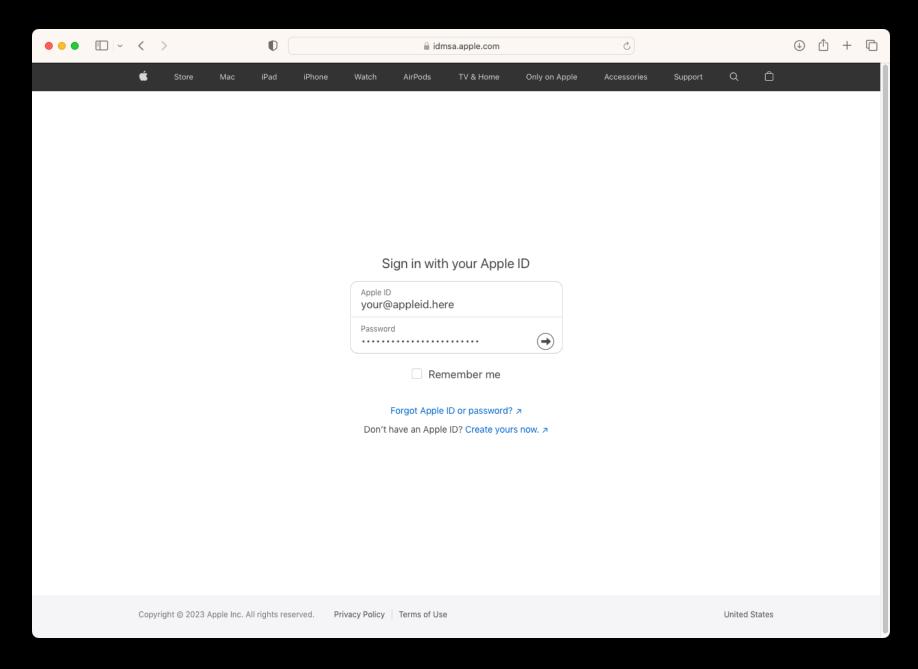
CiagICA8c3RyaW5nPi0tLS0tQkVHSU4gQ0VSVElGSUNBVEUtLS0tLQpNSUlGZFRDQ0JGMmdBd0lCQWdJSUYzNDFWdStITEhRd0RRWUpLb1pJaHZjTkFRRUZCUUF3Z1 pZeEN6OUpCZ05WCkJBWVRBbFZUTVJNd0VRWURWUVFLREFwOmNIOnNaU0JKYm1NdU1Td3dLZ1\EV\FRTERDTkJiSEJzW\NCWGIzSnMKWkhkcFpHVWdSR1Yvw\d4dmNH VnlJRkpsYkdGMGFXOXVjekZFTUVJR0ExVUVBd3c3UVhCd2JHVWdWMjl5YkdSMwphV1JsSUVSbGRtVnNiM0JsY2lCU1pXeGhkR2x2Ym5NZ1EyVnlkR2xtYVdOaGRHbH ZiaUJCZFhSb2IzSnBkSGt3CkhoY05NVGd3TlRBNE1UTTBNREl4V2hjTk1Ua3d0VEE0TVRNME1ESXhXakNCaERFYU1CZ0dDZ21TSm9tVDhpeGsKQVFFTUNrTlV0emxD TjBkVk1sWXhKekFsQmdOVkJBTU1IazFFVFNCV1pXNWtiM0k2SUVwQ\RVwWdVMjltZEhkaApjbVVzSUV4TVF6RVRNQkVHQTFVRUN3d0tRMVEzT1VJM1IxVX\WakViTU JrRØExVUVDZ3dTU2tGTlJpOlRiMlowCmOvRnlaU3dnVEV4RE1Rc3dDUVlEVlFRRØV3SlZVekNDOVNJdØRRWUpLb1pJaHZiTkFRRUJCUUFEZ2dFUEFE00MKOVFvO2dn RUJBS29QRngyRHRYQldQUlRoQUtRM1ZnMzJTZ0RnOHJqbnBEOGdTd0IyN3l4czBib0p5azIvem9QdQpLYm5H0XBXK2VpRHB0WTZNZ04wUFdSMUlET2ZzZWZNbGNEVz VNUGxYbFZ6WkZsQUp6VmYvVStmeCtTb2sxMDJ2CndBM1FUT2lJQUhaVlq0eHBiVi9HN2NCbG5hK2l0clVIT1q00FFIanBkRWs4UDkxTHRBOXNrc1hoQWhESDNoU24K d3RUWUNoUWhIaXF6NURKTEk3Y0NaYisyUit3NmdQYmxTbFVTYmx0dDY5L3NVcGxtSUF4WGZEM2lV0E55RDl4WApHb2RmelVvckRKMm83bllnZUMycGMzTGFuT20x0E hXMlhTQnRNSjBTRnhaUnhiRlY2c0ZJQlRQNVFTV0hZUDJpClcrQjhMd2JnWm9aSWVVcVBPS3ZuZW5UQnlHdmFrSlVDQXdFQUFhT0NBZFV3Z2dIUk1Bd0dBMVVkRXdF Qi93UUMKTUFBd0h3WURWUjBqQkJnd0ZvQVVpQ2NYQ2FtMkdHQ0w3T3U2OWtkWnhWSlVvN2N3Z2dFUEJnTlZIU0FFZ2dFRwpNSUlCQWpDQi93WUpLb1pJaHZkalpBVU JNSUh4TUlIREJnZ3JCZ0VGQlFjQ0FqQ0J0Z3lCczFKbGJHbGhibU5sCklH0XVJSFJvYVhNZ1kyVnlkR2xtYVd0aGRHVWdZbmtnWVc1NUlIQmhjblI1SUdGemMzVnRa WE1nWVdOalpYQjAKWVc1alpTQnZaaUIwYUdVZ2RHaGxiaUJoY0hCc2FXTmhZbXhsSUhOMFlXNWtZWEprSUhSbGNtMXpJR0Z1WkNCagpiMjVrYVhScGIyNXpJRzltSU hWelpTd2dZMlZ5ZEdsbWFXTmhkR1VnY0c5c2FXTjVJR0Z1WkNCalpYSjBhV1pwClkyRjBhVzl1SUhCeVlXTjBhV05sSUh0MFlYUmxiV1Z1ZEhNdU1Da0dDQ3NH0VFV RkJ3SUJGaDFvZEhSd09pOHYKZDNkM0xtRndjR3hsTG10dmJTOWhjSEJzWldOaEx6Qk5CZ05WSFI4RVJqQkVNRUtnUUtBK2hqeG9kSFJ3T2k4dgpaR1YyWld4dmNHVn lMbUZ3Y0d4bExtTnZiUzlqWlhKMGFXWnBZMkYwYVc5dVlYVjBhRzl5YVhSNUwzZDNaSEpqCllTNWpjbXd3SFFZRFZSME9C0llFRktw0W8wTG81Yi9hWEVFMVh1SS9a T1ZoOU\Kdk1BNEdBMVVkRHdFQi93UUUKQXdJSGdEQVBCZ2txaGtpRzkyTmtCQXdFQWdVQU1BMEdDU3FHU0\iM0RRRUJCUVVBQTRJQkFRQ\\0S3YvdzMwNApQN0VuSD FweXFmQnZ5VmFPWkNnU0VIVlNDbTMyb0thRjZWSy9PaVFEaW1wd1NndXRzRG5ya0Ew0EJXV3RUMktJCkd4eFRQaFZGUkJ1VkFmaHgyN0tMUEtvQnREN1pyMnVZYjli ZE9saUpDTGxnVDVnMS9ZMkRHUFQ1SDY5azk2MWwKcllwRmQ0Q2xGbkhwMk91ZG1Xbi9mTHhaNG5WWi9ZeU1YcnlRZlNWdEJ0dzJ3bHlBRlVjVHl0VW5sM1hsMkM4cg pvVStka244VFFYN3VXR3VWTldSU05YaGpMd0J0VjFnRU10Tjd6NkU30HUr0WVLTnVLQnpGWi85V2FBYWFrdVFPCmVCcXVqekdteDhSWGprZW84TTdwSi8rczFPRlcw ZFpwQUNqOXNrcTJ3dWRJY0FxbmQrYzA0dUhaL0hhaXp0K0UKMDRtSW56YSt6emYrCi0tLS0tRU5EIENFUlRJRklDQVRFLS0tLS0KLS0tLS1CRUdJTiBDRVJUSUZJQ0 FURSØtLSØtCk1JSUVJakND0XdxZØF3SUJBZØlJOW02OHhEbHRv0kF3RFFZSktvWklodmNO0VFFRkJR0XdZakVMTUFrRØExVUUKOmhN01ZWTXhFekFSOmd0VkJBb1RD a0Z3Y0d4bElFbHVZeTR4SmpBa0JnTlZCQXNUSFVGd2NHeGxJRU5sY25ScApabWxqWVhScGIyNGdRWFYwYUc5eWFYUjVNUll3RkFZRFZRUURFdzFCY0hCc1pTQlNiMj kwSUVOQk1CNFhEVEV6Ck1ESXdOekl4TkRnME4xb1hEVEl6TURJd056SXhORGcwTjFvd2daWXhDekFKQmd0VkJBWVRBbFZUTVJNd0VRWUQKVlFRS0RBcEJjSEJzWlNĆ SmJtTXVNU3d3S2dZRFZRUUxEQ05CY0hCc1pTQlhiM0pzWkhkcFpHVWdSR1YyWld4dgpjR1Z5SUZKbGJHRjBhVzl1Y3pGRU1FSUdBMVVFQXd3N1FYQndiR1VnVjI5eW JHUjNhV1JsSUVSbGRtVnNiM0JsCmNpQlNaV3hoZedsdmJuTWdRMlZ5ZEdsbWFXTmhkR2x2YmlCQmRYUm9iM0pwZEhrd2dnRWlNQTBHQ1NxR1NJYjMKRFFFQkFRVUFB NE\CRHdBd2dnRUtBb0\CQVFES09GU215MWFxeUNRNVNPbU03dXhmdUq4bWtidzBVM3JPZkdPQQpZWGRrWHFVSEk3WTUvbEF0R\ZaWWNDMSt4RzdCU29VK0wvRGVoQn FoVjhtdmV4ai9hdm9WRWtrVkNCbXNxdHNxCk11MldZMmhTRlQyTWl1eS9heGlWNEFPc0FYMlhCV2ZPRG9XVk4ycnRDYmF1WjgxUlpKL0dYTkc4VjI1bk5ZQjIKTnFT SGdXNDRqOWdyRlU1N0pkaGF2MDZEd1kzU2s5VWFjYlZnbkowelRsWDVFbGdNaHJnV0RjSGxkMFd0VUVpNgpLeTNrbElYaDZNU2R4bWlsc0tQ0FozNXd1Z0paUzNkQ2 tUbTU5YzNoVE8vQU8waU1wdVVoWGYxcWFydW5GalZnCjB1YXQ4MFlweWVqRGkrbDV3R3BoWnhXeThQM2xhTHhpWDI3UG1kM3ZHMlAra21XckFnTUJBQUdqZ2FZd2dh TXcKSFFZRFZSME9CQllFRklnbkZ3bXB0aGhnaSt6cnV2WkhXY1ZTVktPM01B0EdBMVVkRXdFQi93UUZNQU1CQWY4dwpId1lEVlIwakJCZ3dGb0FVSzlCcFI1UjJDZj cwYTQwdVFLYjNSMDEvQ0Y0d0xnWURWUjBmQkNjd0pUQWpvQ0dnCkg0WWRhSFIwY0RvdkwyTnliQzVoY0hCc1pTNWpiMjB2Y205dmRDNWpjbXd3RGdZRFZSMFBBUUgv QkFRREFnR0cKTUJBR0NpcUdTSWIzWTJRR0FnRUVBZ1VBTUEwR0NTcUdTSWIzRFFFQkJRVUFBNE\CQVFCUHor0Vp2aXoxc213dgpqKzRUaHpMb0JUV29ib3Q5eVdrTX Vka1h2SGNzMUdmaS9acHRPbGxjMzRNQnZiS3VLbUZ5c2EvTncwVXdqNk9ECkRjNGRSN1R4azRxamRKdWt3NWh5aHpzK3IwVUxrbFM1TXJ1UUdGTnJDazRRdHRrZFVH d2hnQXFKVGxlTWExczqKUGFiOTN2Y05JeDBMU2lhSFA3cVJra3lrR1JJWmJWZjFlbGlIZTJpSzVJYU1TdXZpU1JTcXBkMVZBS211dTBzdwpydUdnc2J3cGdPWUpkK1 crTktJQnluL2M0Z3JtTzdpNzdMcGlsZk1GWTBHQ3pRODdIVXlWcE51citjbVY2VS9rClRlY21tWUhwdlBtMEtkSUJlbWJoTG96MklZckYrSGpoZ2E2LzA1Q2RxYTN6 ci8wNEdwWm5NQnhScFZ6c2NZcUMKdEd3UERCVWYKLS0tLS1FTkQgQ0VSVElGSUNBVEUtLS0tLQotLS0tLUJFR0lOIENFUlRJRklDQVRFLS0tLS0KTUlJRXV6Q0NBNk 9nQXdJQkFnSUJBakF0QmdrcWhraUc5dzBCQVFVRkFEQmlNUXN3Q1FZRFZRUUdFd0pWVXpFVApNQkVHQTFVRUNoTUtRWEJ3YkdVZ1NXNWpMakVtTUNRR0ExVUVDeE1k UVhCd2JHVWdRMlZ5ZEdsbWFXTmhkR2x2CmJpQkJkWFJvYjNKcGRIa3hGakFVQmdOVkJBTVREVUZ3Y0d4bElGSnZiM1FnUTBFd0hoY05NRFl3TkRJMU1gRTAKTURNMl doY05NelV3TWpBNU1qRTBNRE0yV2pCaU1Rc3dDUVlEVlFRR0V3SlZVekVUTUJFR0ExVUVDaE1LUVhCdwpiR1VnU1c1akxqRW1NQ1FHQTFVRUN4TWRRWEJ3YkdVZ1Ey VnlkR2xtYVdOaGRHbHZiaUJCZFhSb2IzSnBkSGt4CkZgQVVCZ05W0kFNVERVRndiR3hsSUZKdmIzUWdRMEV3Z2dFaU1BMEdDU3FHU0liM0RRRUJBUVVBOTRJ0kR3QX cKZ2dFS0FvSUJBUURra2FrSkq1SGJIa2RRNndYdFhubUVMZXMyb2xkTVZleUxHWW5lK1V0czlRZXJJakFDNkJnKworRkFKMDM5QnFKajUwY3BtbkNSckVkQ2p1K1Fi S3NNZmxaNTZES1JIaTF2VUZqY3p50FF0VGM0VWFkSEpHWEwxClhRN1ZmMSti0GlVRHVsV1BUViB00FdRMUl4VkxGVmtkczVUMzlweW/6MUM2d1ZoUVo00El0000zeT Z3c0lH0XcKdGo4Qk1JeTNR0DhQblQzekswa29Hc2orenJXNUR0bGVITmJMUGJVNnJmUVBEZ0NTQzdFaEZpNTAxVHd0MjJJVwpxNk54a2tkVFZjR3ZMMEd6K1B2amNN M21vMHhGZmg5TWExQ1dRwW5FZEdJTEVJTkJoek9LZ2JFd1dPeGFCREtNCmFMT1BIZDVsYy85blhtVzhTZGgybnpNVVphRjNsTWt0QWdNQkFBR2pnZ0Y2TUlJQmRqQU 9CZ05WSFE4QkFm0EUKQkFNQ0FRWXdEd1lEVlIwVEFRSC9CQVV3QXdFQi96QWRCZ05WSFE0RUZnUVVLOUJwÜjVSMkNmNzBhNDB1UUtiMwpSMDEvQ0Y0d0h3WURWUjBq OkJnd0ZvOVVLOUJwUiVSMkNmNzBhNDB1UUtiM1IwMS9DRiR3Z2dFUkJnTlZIU0FFCmdnRUlNSUlCOkRD00FROUdDU3FHU0liM1kvUUZBVENCOGpBcUJnZ3JCZ0VGOl FjQ0FSWWVhSFIwY0hNnkx50TMKZDNjdVlYQndiR1V1WTI5dEwyRndjR3hsWTJFdk1JSERCZ2dyQmdFRkJRY0NBakNCdGhxQnMxSmxiR2xoYm10bApJRzl1SUhSb2FY TWdZMlZ5ZEdsbWFXTmhkR1VnWW5rZ1lXNTVJSEJoY25SNUlHRnpjM1Z0WlhNZ1lXTmpaWEIwCllXNWpaU0J2WmlCMGFHVWdkR2hsYmlCaGNIQnNhV05oWW14bElITj BZVzVrWVhKa0lIUmxjbTF6SUdGdVpDQmoKYjI1a2FYUnBiMjV6SUc5bUlIVnpaU3dnWTJWeWRHbG1hV05oZEdVZ2NHOXNhV041SUdGdVpDQmpaWEowYVdacApZMkYw YVc5dulIQnlZV04wYVd0bElITjBZWFJsYldWdWRITXVNQTBHQ1NxR1NJYjNEUUVCQlFVQUE0SUJBUUJjCk5wbE1MWGkzN1l5YjNQTjNtL0oyMG5jd1Q4RWZoWU9GRz VrOVJ6ZnlxWnRBaml6VXNaQVMyTDcwYzV2dTBtUVAKeTNsUE50aWlQdmw0LzJ2SUIreDlPWU9MVXlEVE9NU3h2NXBQQ212L0sveFpwd1VKZkJkQVZoRWVkTk8zaXlN NwpSNlBWYnlUaTY5RzNjTjhQUmVFbnl2RnRlTzNudFJjWHF0eCtJalhLSmRYWkQ5WnIxS0lrSXhIM29heVBjNEZnCnhodGJDUytTc3ZoRVNQQmdPSjRW0VQwbVp5Q0 tNMnIzRFlMUDN1dWpML2xUYWx0a3dHTXpkL2M2Qnl4VzY5b1AKSVE3YXVuTVpUN1haTm4vQmgxWFpwNW01TWtMNzJ0VnhubjZoVXJjYnZaTkNKQklxeHc4ZHRrMmNY bVBJUzRBWApVS3FLMWRyay90QUpCemV3ZFhVaAotLS0tLUVORCBDRVJUSUZJQ0FURS0tLS0tCjwvc3RyaW5nPgogIDwvZGljdD4KPC9wbGlzdD4K

#### **MDM Server Certificates**

- APNS Push Certificate
  - Used by MDM server to communicate with APNS



#### https://identity.apple.com



## https://identity.apple.com

## APNS Apple ID Do's and Don'ts

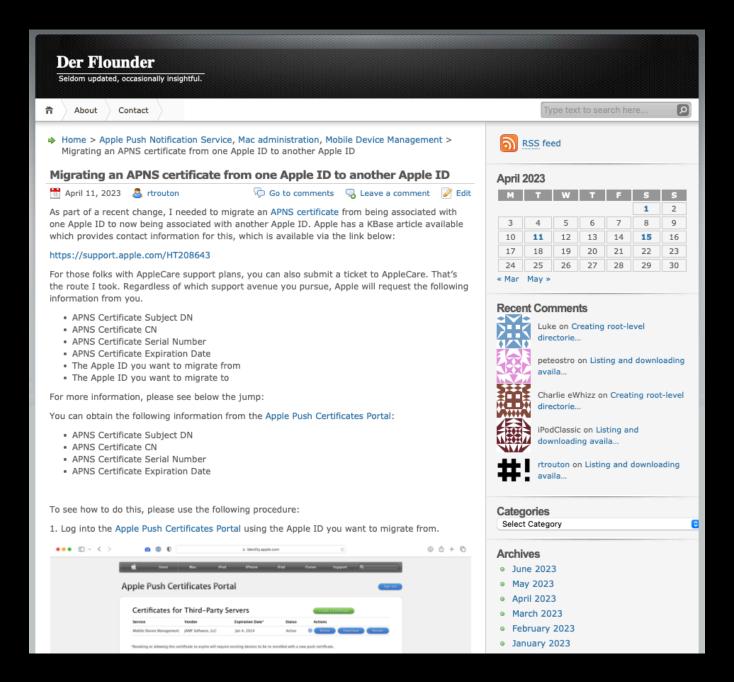
#### Do:

- Have an Apple ID dedicated just to creating your APNS certificate.
- Have multiple Apple IDs for your APNS certificates if you have more than one MDM server.
- Have the Apple ID(s) documented.

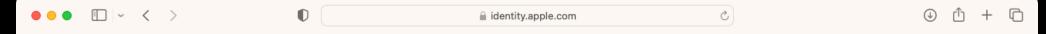
### APNS Apple ID Do's and Don'ts

#### Don't:

- Use a personal Apple ID.
- Use an Apple ID tied to your specific work email address.
- Lose the password to your Apple ID(s).



#### https://tinyurl.com/fixapns





Sign out

#### Certificates for Third-Party Servers

Service	Vendor Twocanoes Software, Inc	Expiration Date*	Status	Actions
	Twocannes Software Inc			
Mobile Device Management	rwocanoes sortware, me	Aug 22, 2022	Expired	() Renew Download Revoke
Mobile Device Management	JAMF Software, LLC	Dec 13, 2023	Active	() Renew Download Revoke
Mobile Device Management	JAMF Software, LLC	Jan 4, 2024	Active	() Renew Download Revoke
Mobile Device Management	JAMF Software, LLC	Jan 12, 2013	Revoked	(i) Renew
Mobile Device Management	JAMF Software, LLC	May 26, 2013	Revoked	Renew
Mobile Device Management	JAMF Software, LLC	Dec 9, 2014	Revoked	(i) Renew
Mobile Device Management	JAMF Software, LLC	Sep 16, 2015	Revoked	(i) Renew
Mobile Device Management	JAMF Software, LLC	Aug 30, 2016	Revoked	(i) Renew

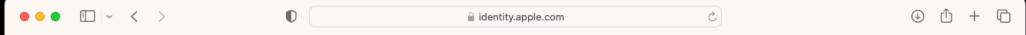
\*Revoking or allowing this certificate to expire will require existing devices to be re-enrolled with a new push certificate.

#### About Apple Push Certificates Portal

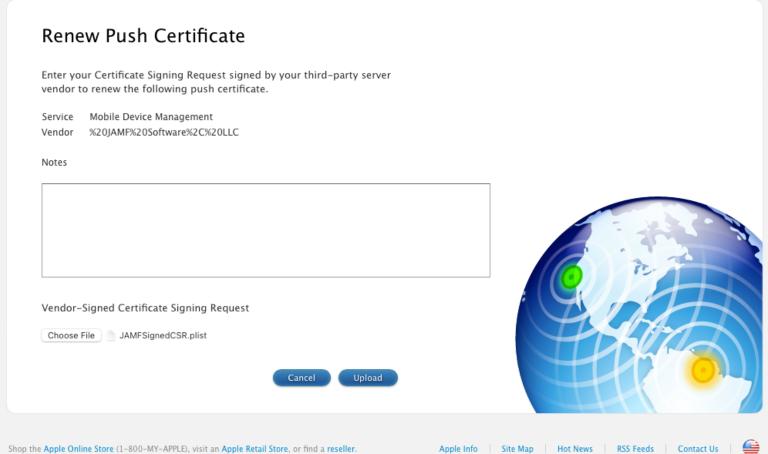
Create and manage push certificates that enable your third-party server to work with the Apple Push Notification Service and your Apple devices.

Learn more about Mobile Device Management

To protect your server's identity, Apple Push Certificates Portal allows you to revoke push

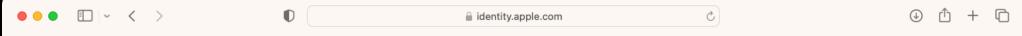






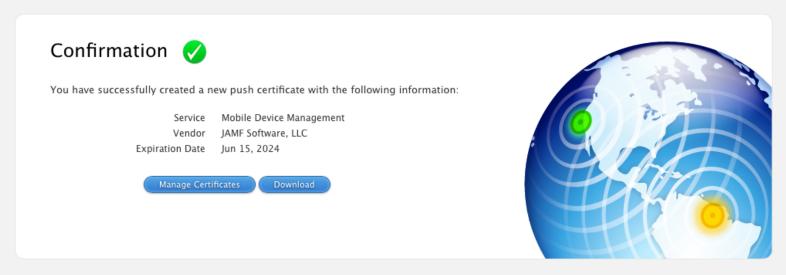
Shop the Apple Online Store (1-800-MY-APPLE), visit an Apple Retail Store, or find a reseller.











Shop the Apple Online Store (1-800-MY-APPLE), visit an Apple Retail Store, or find a reseller.

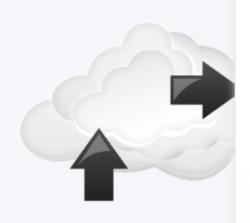
Apple Info | Site Map | Hot News | RSS Feeds | Contact Us



#### Settings: Global

#### ← Push certificates

- Choose Option
- Download CSR
- Sign CSR
- Create Certificate
- Upload Certificate
- Verify
- Complete



#### Verify Certificate



#### WARNING

Existing devices that are enrolled with Jamf Pro will no longer respond to push notifications.



Your new push notification certificate has a new "topic".

Existing Topic: com.apple.mgmt.External.fe5889be-8ae2-4a62-92fd-e94df8877c7e

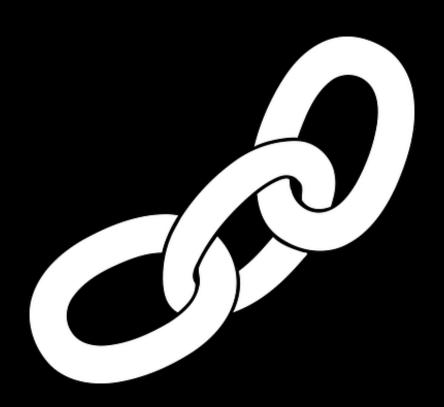
New Topic: com.apple.mgmt.External.b014b722-0715-49ff-a347-f40ba327ee20

Click Next to overwrite your existing certificate.

Cancel

Previous

Next



## **APNS** push certificate



#### APSP:fe5889be-8ae2-4a62-92fde94df8877c7e

#### Subject Name

User ID com.apple.mgmt.External.fe5889be-8ae2-4a62-92fd-e94df8877c7e
Common Name APSP:fe5889be-8ae2-4a62-92fd-e94df8877c7e
Country or Region US

#### Issuer Name

Common Name Apple Application Integration 2 Certification Authority
Organizational Unit Apple Certification Authority
Organization Apple Inc.
Country or Region US

Serial Number 6150069533494760542

Version

Signature Algorithm SHA-256 with RSA Encryption ( 1.2.840.113549.1.1.11 )

Parameters None

Not Valid Before Friday, June 16, 2023 at 12:14:41 PM Eastern Daylight Time
Not Valid After Saturday, June 15, 2024 at 12:14:40 PM Eastern Daylight Time

#### Public Key Info

Algorithm RSA Encryption (1.2.840.113549.1.1.1)

Parameters None

Public Key 256 bytes: C5 A6 4C C3 D2 8D 9A C2 ...

Exponent 65537

Key Size 2,048 bits

Key Usage Encrypt, Verify, Derive

Signature 256 bytes: 69 D5 39 7D FD 1A 18 6A ...

Extension Key Usage (2.5.29.15)

Critical NO

Usage Digital Signature

Extension Basic Constraints (2.5.29.19)

Critical NO

Certificate Authority NO

### APNS push certificate topic



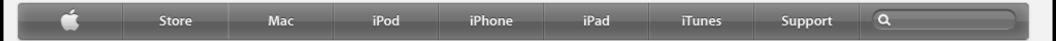
APSP:fe5889be-8ae2-4a62-92fd-e94df8877c7e

Subject Name

User ID com.apple.mgmt.External.fe5889be-8ae2-4a62-92fd-e94df8877c7e

Common Name APSP:fe5889be-8ae2-4a62-92fd-e94df8877c7e

Country or Region US



#### Certificates for Third-Pa

Service	Vendor
Mobile Device Management	Twocanoes Softw
Mobile Device Management	JAMF Software, LI

Serial Number: 759ea1d2c5dafe34

C=US, CN=APSP:fe5889be-8ae2-4a62-92fd-e94df8877c7e, Subject DN:

UID=com.apple.mgmt.External.fe5889be-8ae2-4a62-92fd-e94df8877c7e

Notes:

Mobile Device Management	Twocanoes Softw			
Mobile Device Management	JAMF Software, LI		Cancel	Update Note
Mobile Device Management	JAMF Software, LLC	Jan 4, 2024	Active	i Renew Download Revoke
Mobile Device Management	JAMF Software, LLC	Jan 12, 2013	Revoked	i Renew
Mobile Device Management	JAMF Software, LLC	May 26, 2013	Revoked	i Renew
Mobile Device Management	JAMF Software, LLC	Dec 9, 2014	Revoked	i Renew
Mobile Device Management	JAMF Software, LLC	Sep 16, 2015	Revoked	i Renew
Mobile Device Management	JAMF Software, LLC	Aug 30, 2016	Revoked	(i) Renew



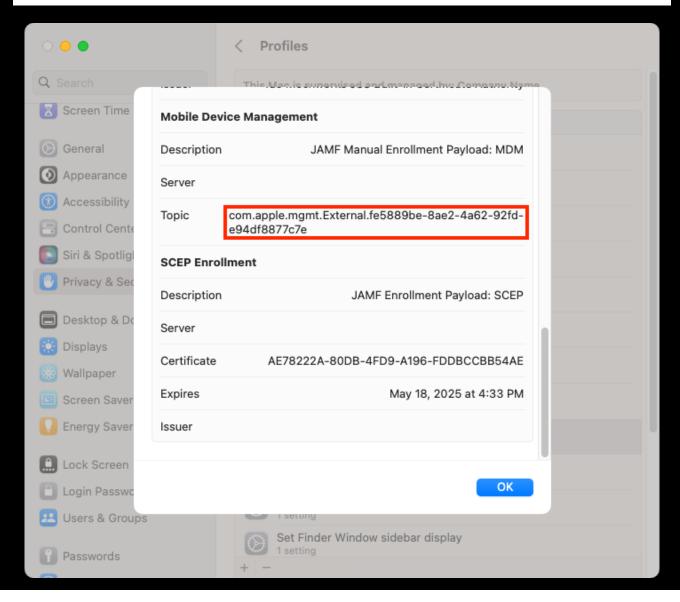
#### APSP:fe5889be-8ae2-4a62-92fd-e94df8877c7e

Subject Name

User ID com.apple.mgmt.External.fe5889be-8ae2-4a62-92fd-e94df8877c7e

Common Name APSP:fe5889be-8ae2-4a62-92fd-e94df8877c7e

Country or Region US



#### Settings: Global

#### ← Push certificates

- Choose Option
- Download CSR
- Sign CSR
- Create Certificate
- Upload Certificate
- Verify
- Complete

#### Verify Certificate



#### WARNING

Existing devices that are enrolled with Jamf Pro will no longer respond to push notifications.



Your new push notification certificate has a new "topic".

Existing Topic: com.apple.mgmt.External.fe5889be-8ae2-4a62-92fd-e94df8877c7e

New Topic: com.apple.mgmt.External.b014b722-0715-49ff-a347-f40ba327ee20

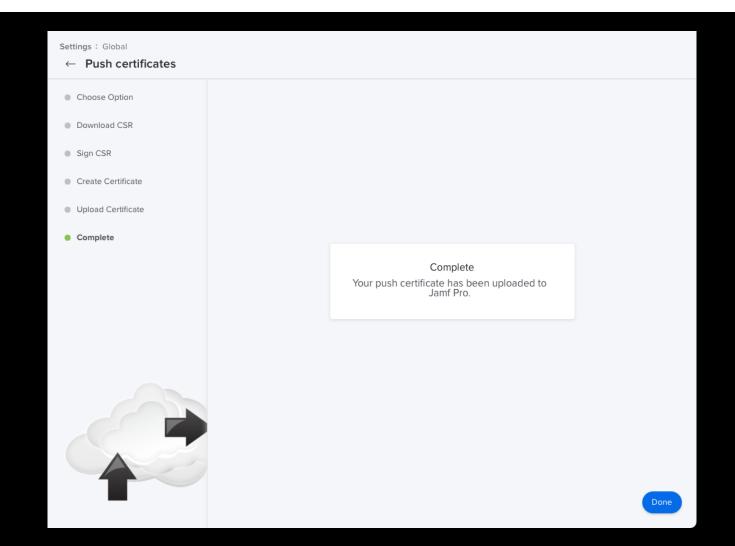
Click Next to overwrite your existing certificate.

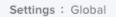
Cancel

Previous

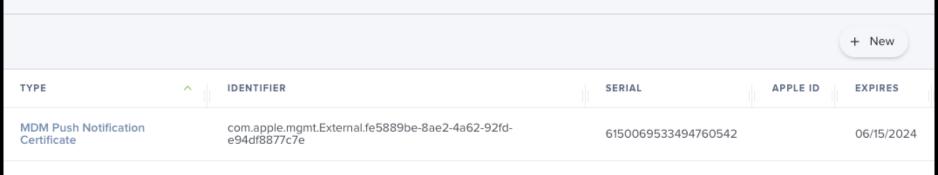
Next

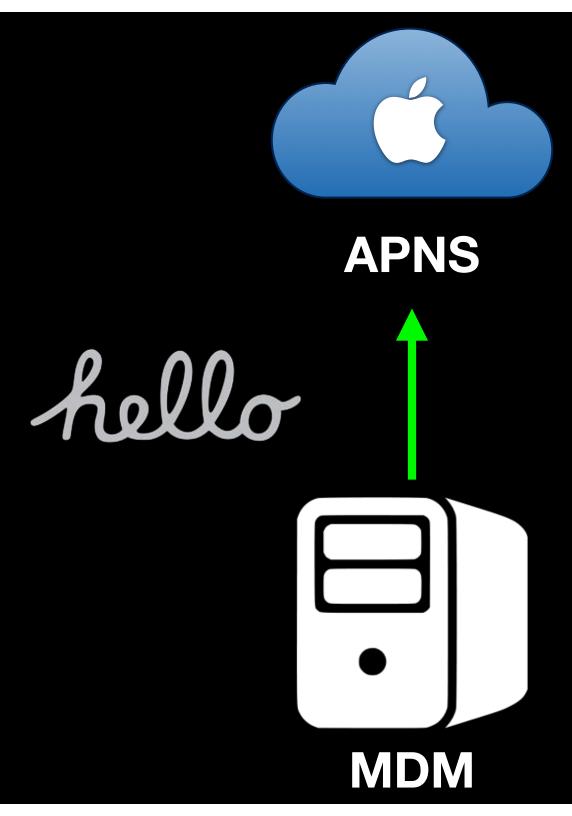




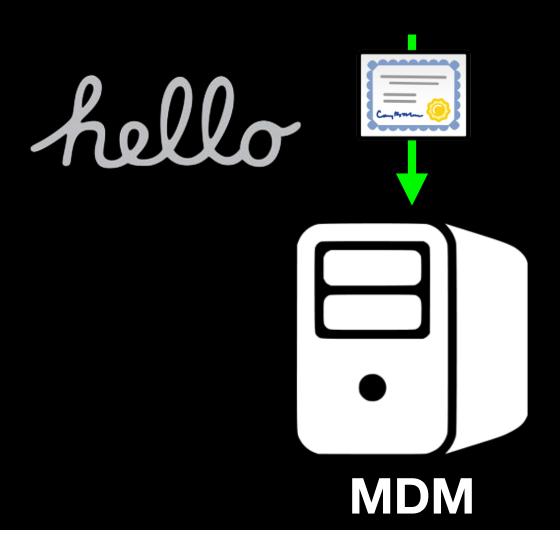


#### ← Push certificates



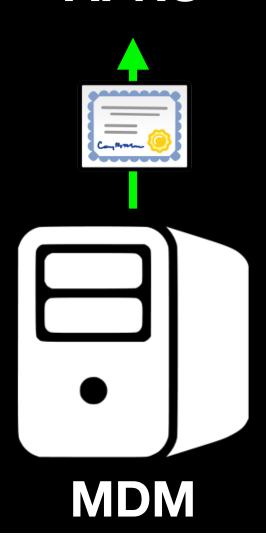




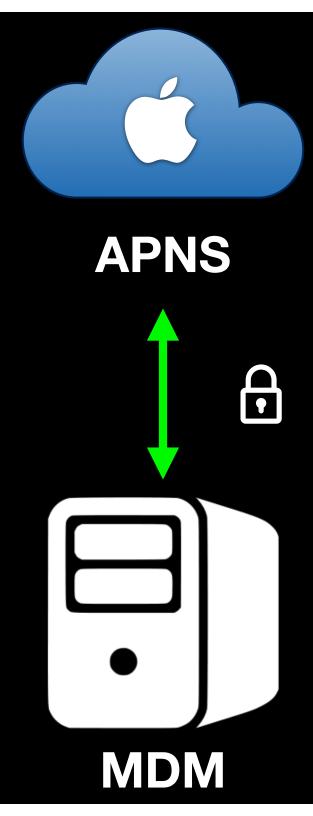








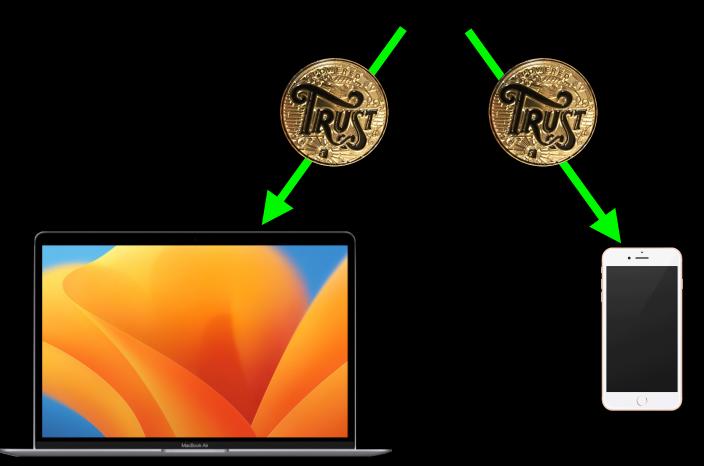


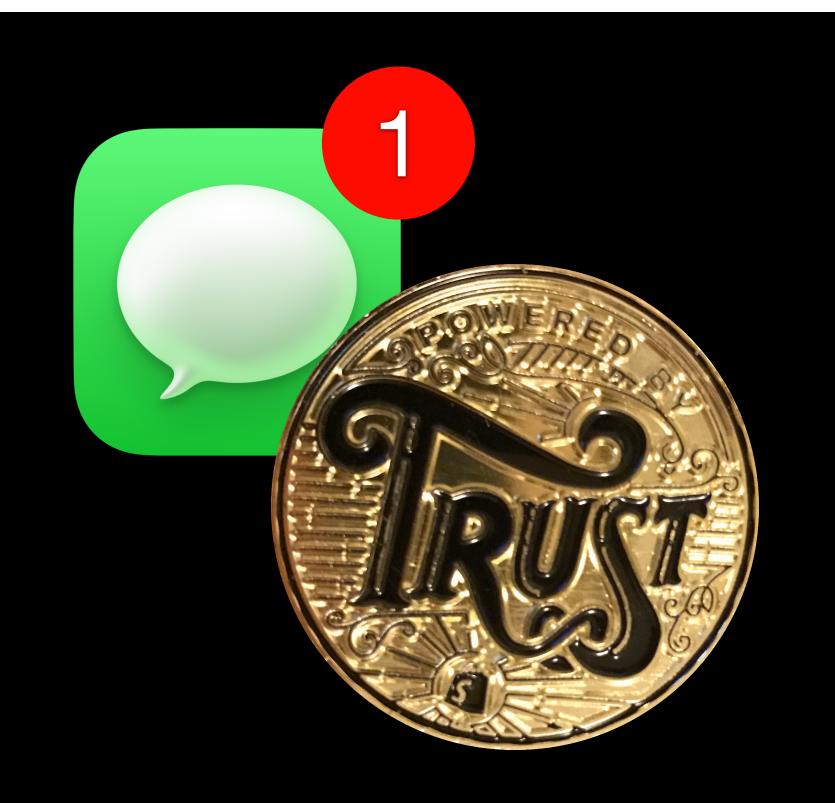


# **APNS** device token

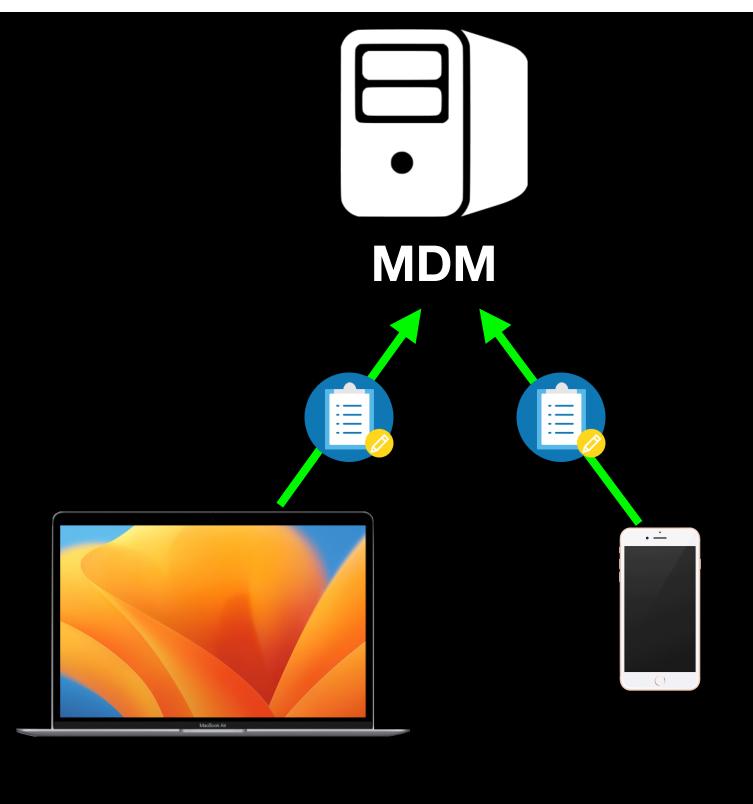


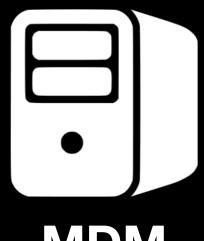












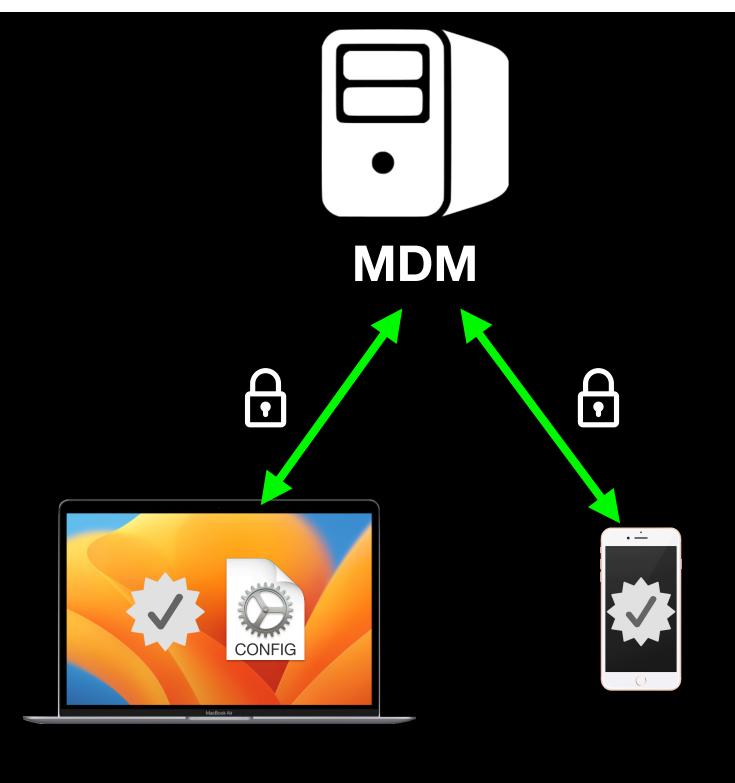


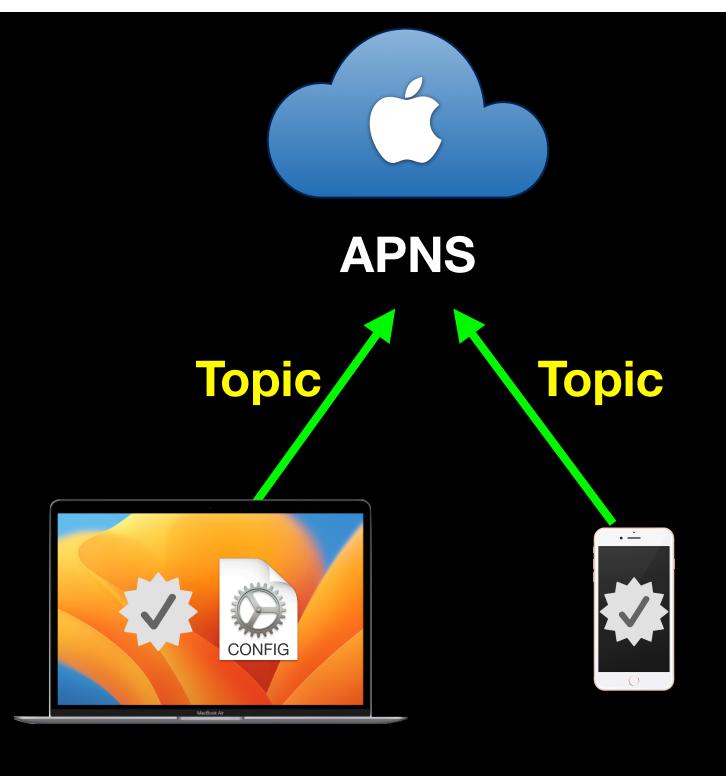
























# MDM



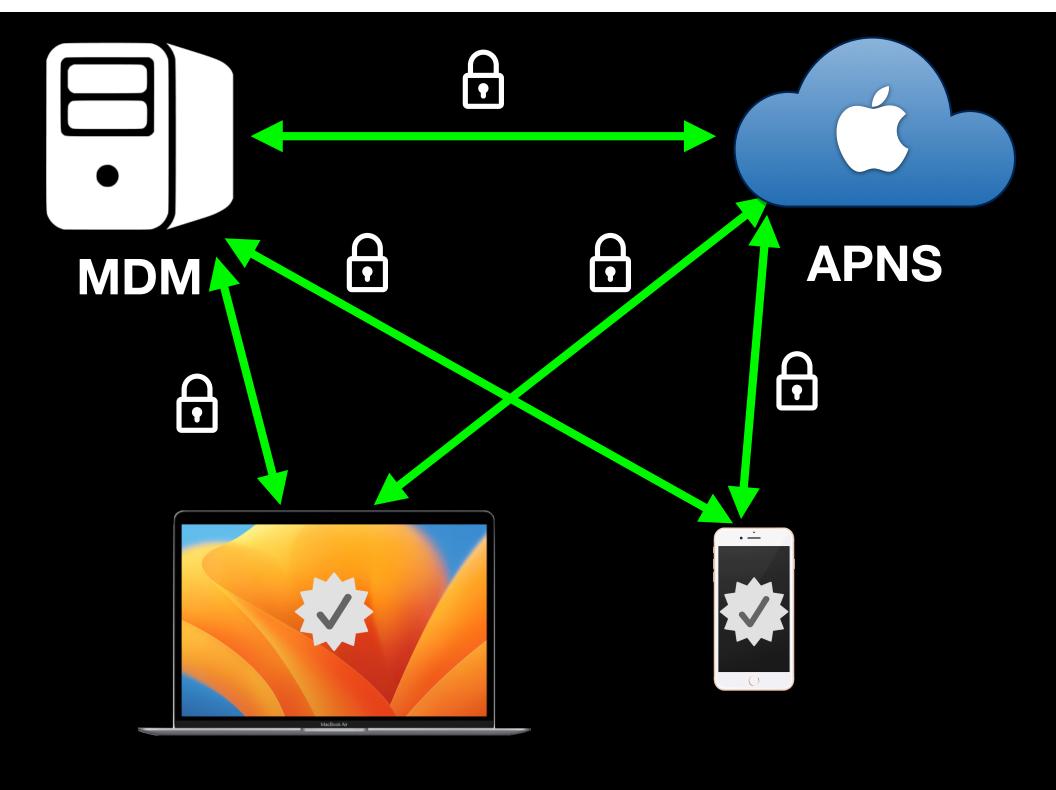


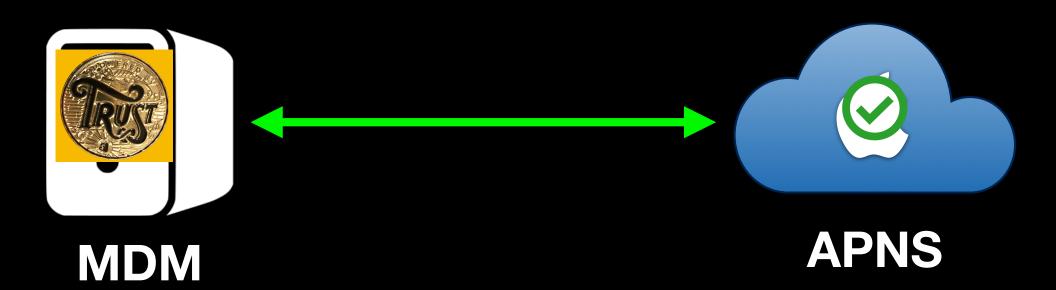




# PushMagic

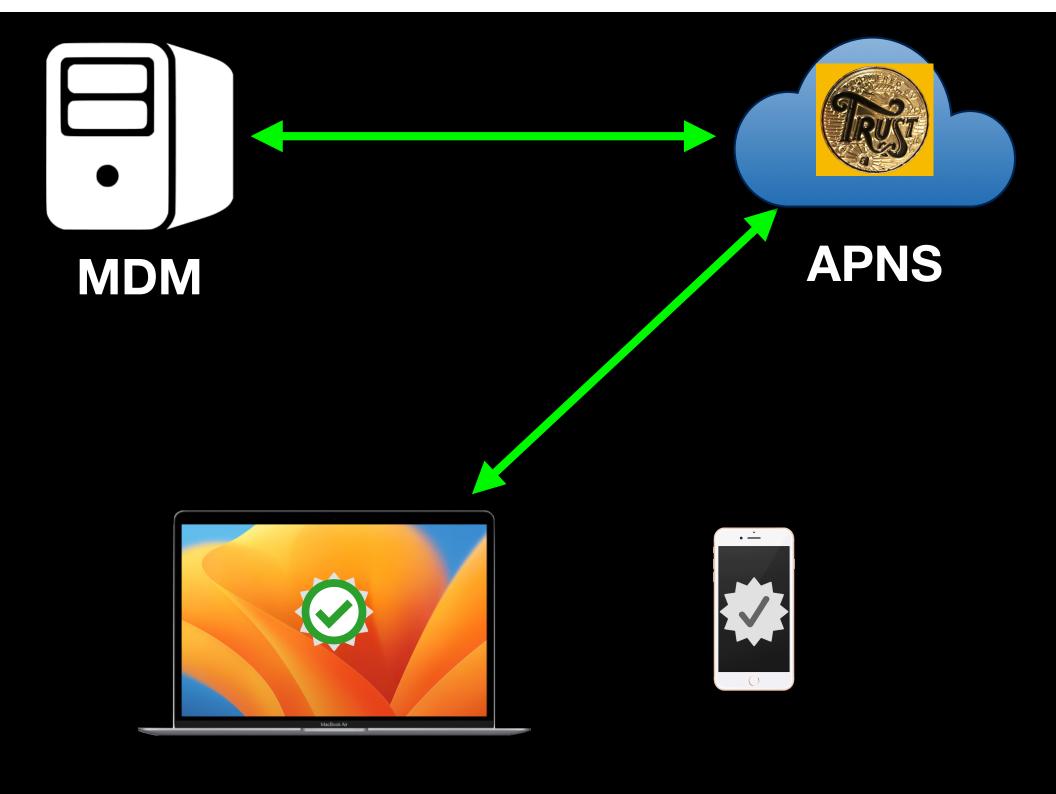


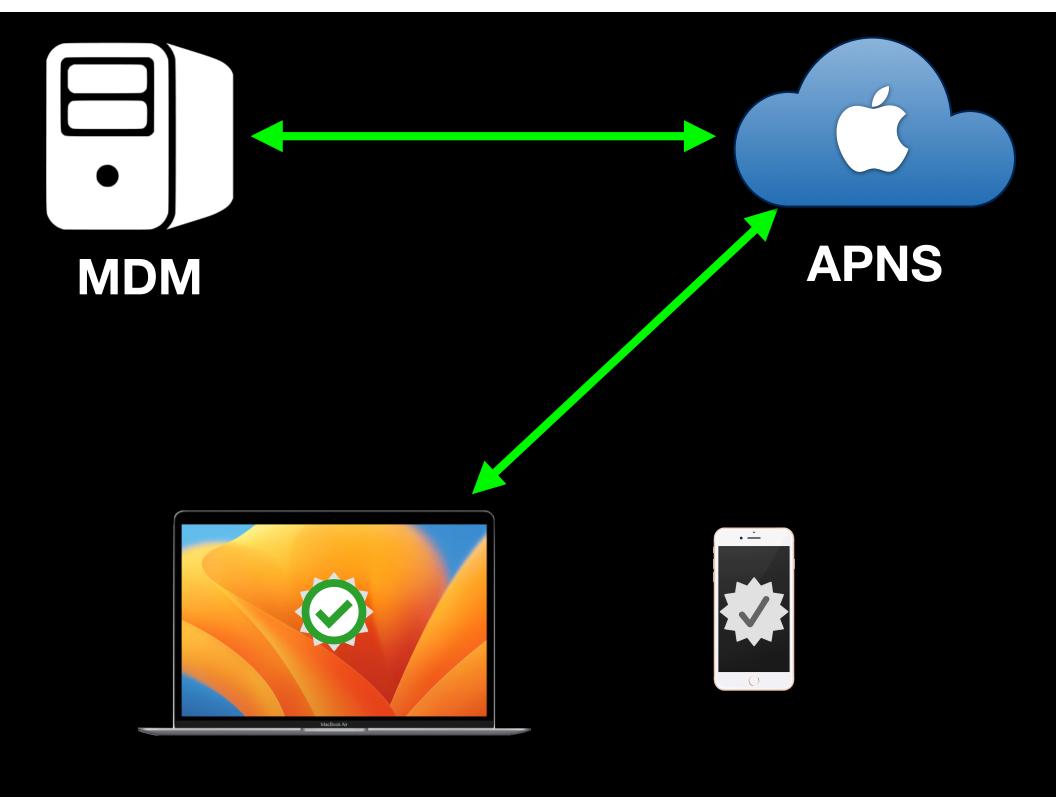


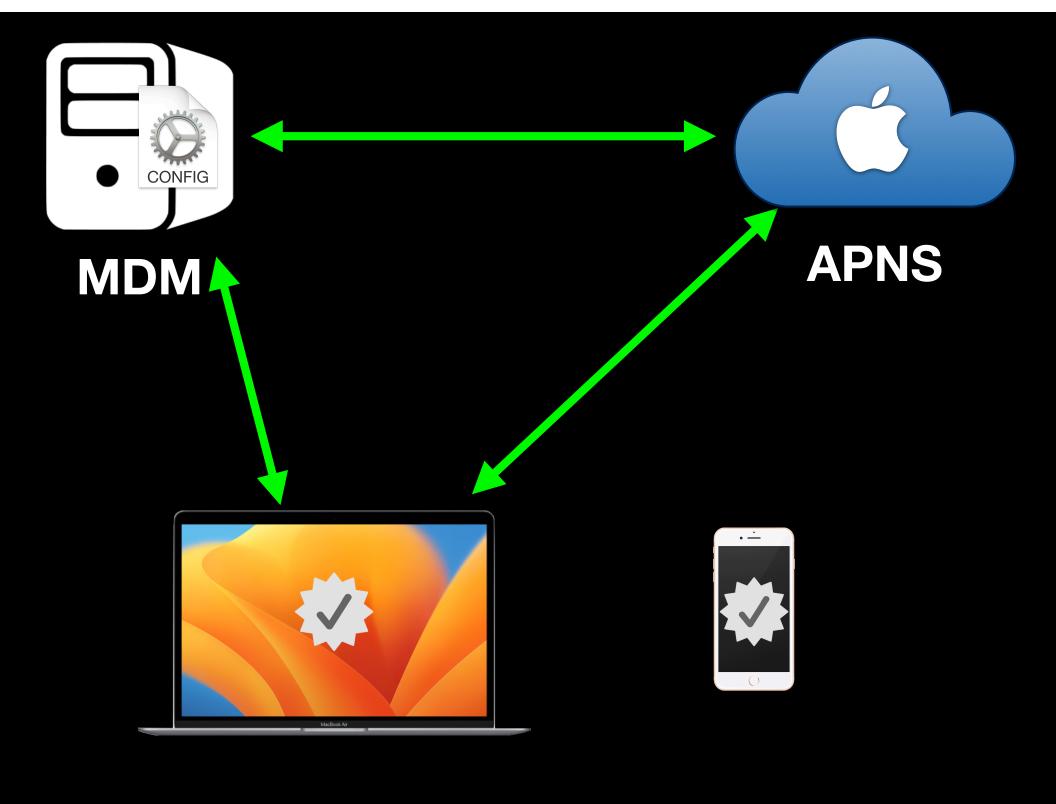














# "Hey you! Check in with your MDM server!"



# Topic











## What is DDM?

#### What it is:

New data management paradigm:

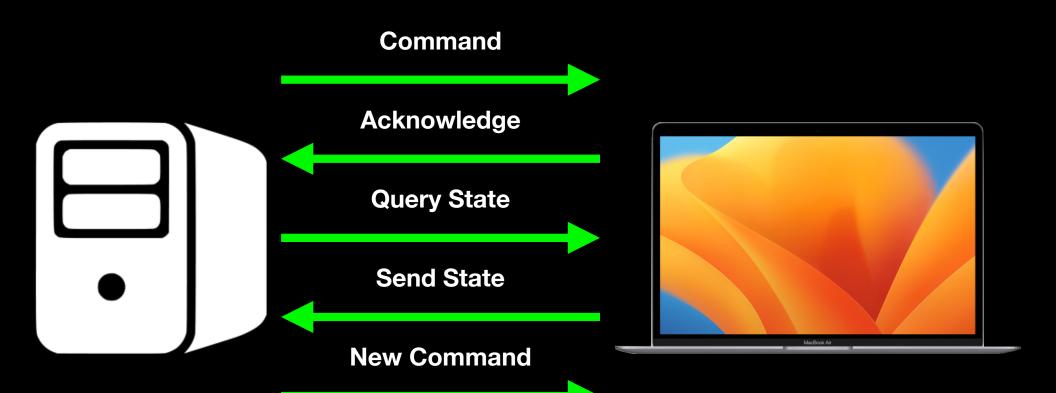
•Avoids common performance and scaling issues seen with MDM

#### What it is not:

New management protocol: DDM has been added to the existing MDM protocol to make DDM adoption easier.

## Why use DDM?

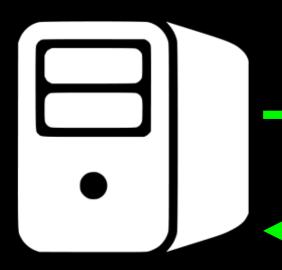
## MDM



#### MDM

- •Each management workflow takes time and multiple round trips between the MDM server and the managed device
- Performance challenges grow larger as the number of devices being managed increases across the organization

#### DDM



Here's the plan. You got this?

Thanks, I got this.
Check in with you later.



## DDM Data Model

- Declarations
- Status Channel
- Extensibility

```
"Type":"com.apple.configuration.passcode.settings",
"Identifier":"4AE28C9F-7082-4521-B435-2550E8B4D57A",
"Server Token":"EAB5142C-7E86-4C8E-B576-B7F94D0F6CEA",
"Payload": {stuff goes here}
```

```
"Type":"com.apple.configuration.passcode.settings",
"Identifier":"4AE28C9F-7082-4521-B435-2550E8B4D57A",
"Server Token":"EAB5142C-7E86-4C8E-B576-B7F94D0F6CEA",
"Payload": {stuff goes here}
```

Type: Identifies the type of policy

```
"Type":"com.apple.configuration.passcode.settings",
"Identifier":"4AE28C9F-7082-4521-B435-2550E8B4D57A",
"Server Token":"EAB5142C-7E86-4C8E-B576-B7F94D0F6CEA",
"Payload": {stuff goes here}
```

# Identifier: Unique identifier for declaration

```
"Type":"com.apple.configuration.passcode.settings",
"Identifier":"4AE28C9F-7082-4521-B435-2550E8B4D57A",
"Server Token":"EAB5142C-7E86-4C8E-B576-B7F94D0F6CEA",
"Payload": {stuff goes here}
```

ServerToken: Unique version identifier, based on the Identifier value

```
"Type":"com.apple.configuration.passcode.settings",
"Identifier":"4AE28C9F-7082-4521-B435-2550E8B4D57A",
"Server Token":"EAB5142C-7E86-4C8E-B576-B7F94D0F6CEA",
"Payload": {stuff goes here}
```

#### Payload: Settings for the policy

- Type: Identifies the type of policy
- Identifier: Unique identifier for declaration
- ServerToken: Unique version identifier, based on the Identifier value.
- Payload: The settings for the policy.

- Configurations
- Assets
- Activations
- Management

```
{
  "Type": "com.apple.configuration.passcode.settings",
  "Identifier": "4AE28C9F-7082-4521-B435-2550E8B4D57A",
  "Server Token": "EAB5142C-7E86-4C8E-B576-B7F94D0F6CEA",
  "Payload": {
    "RequirePasscode": "true",
    "RequireComplexPasscode": "true",
    "MinimumLength": 6,
    "MaximumFailedAttempts": 10,
    "MaximumGracePeriodInMinutes": 10,
    "MaximumInactivityInMinutes": 10,
    "PasscodeReuseLimit": 0
  }
}
```

# Configuration: represents policies being applied to the device.



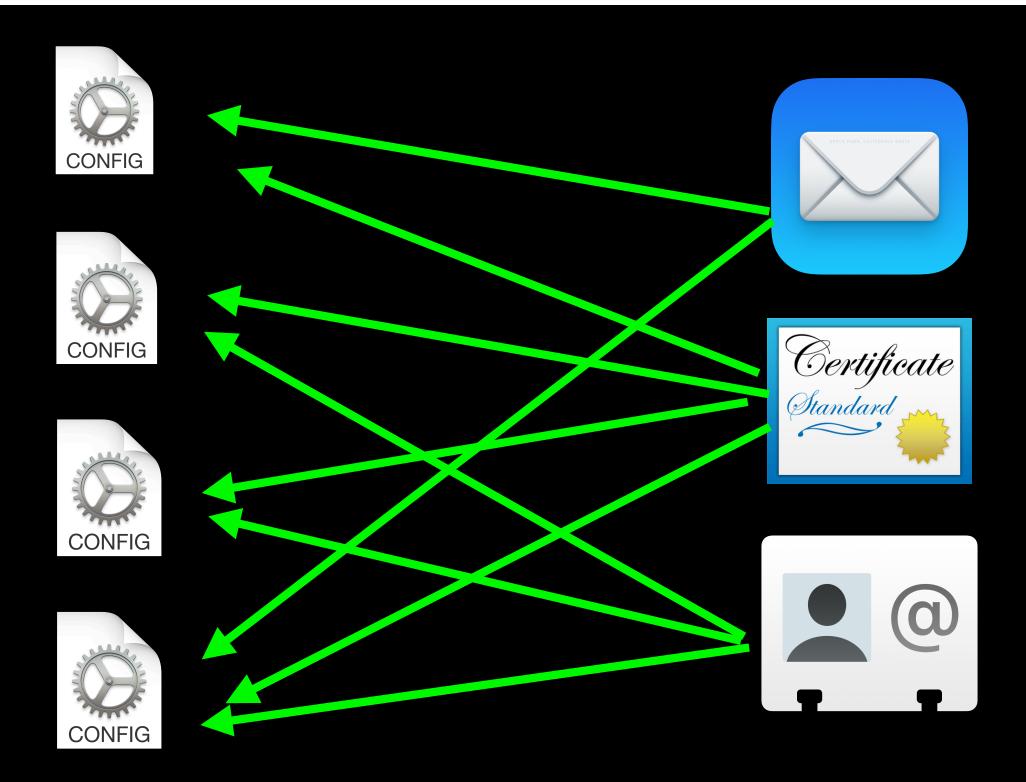




Assets: data needed by a configuration.

```
{
  "Type": "com.apple.asset.useridentity",
  "Identifier": "0DEE79A7-3244-42A0-A4CB-46333AC0F63A",
  "Server Token": "469D704C-A817-4B71-A1B5-B221FDB43E97",
  "Payload": {
    "FullName": "First Last",
    "EmailAddress": "user@example.com"
  }
}
```

# Assets: data needed by a configuration.

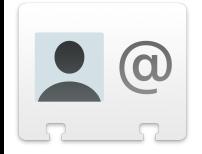


























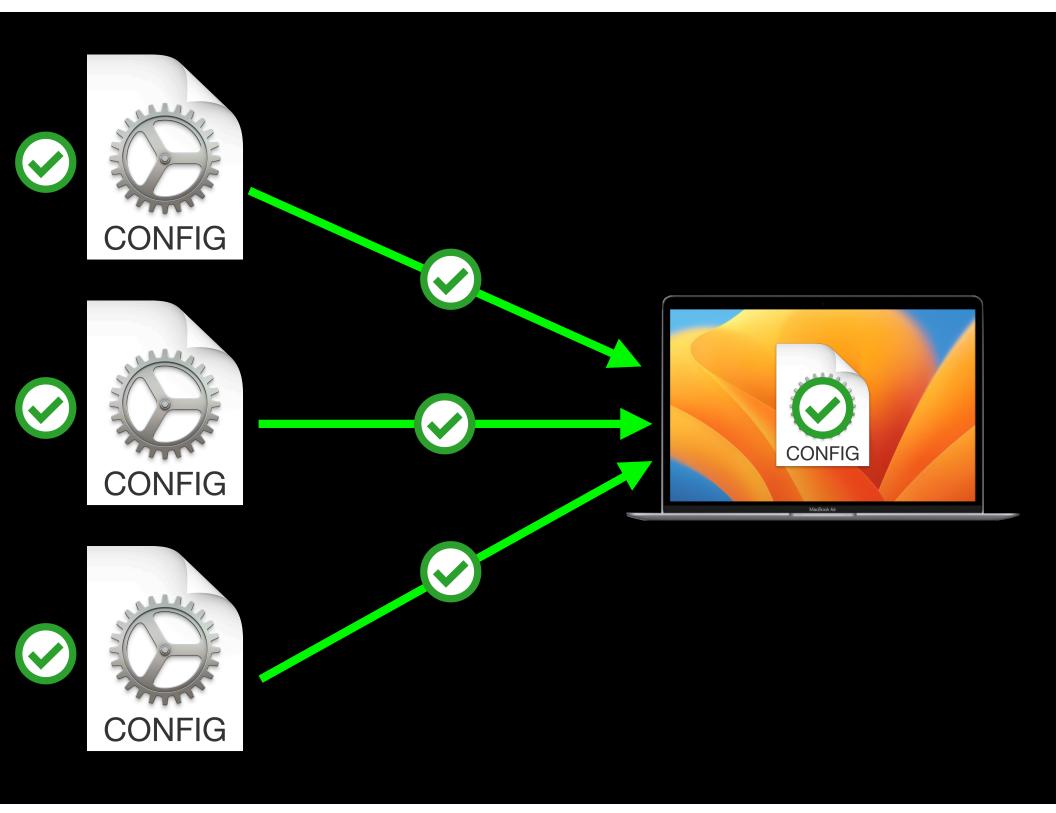






```
{
  "Type": "com.apple.activation.simple",
  "Identifier": "2AD45A8B-B656-4E51-8406-D97549CDE134",
  "Server Token": "7BCE079A-73D6-4A3E-8F5B-9B6021F43140",
  "Payload": {
      "StandardConfigurations": [
            "F3FB5A3F-9835-4A9B-9ED0-D2C813E6668E",
            "EBC2380F-4F8A-4E75-B9AC-F6300AFBD7FE"
            ]
        }
    }
}
```

#### Activation: group of configurations







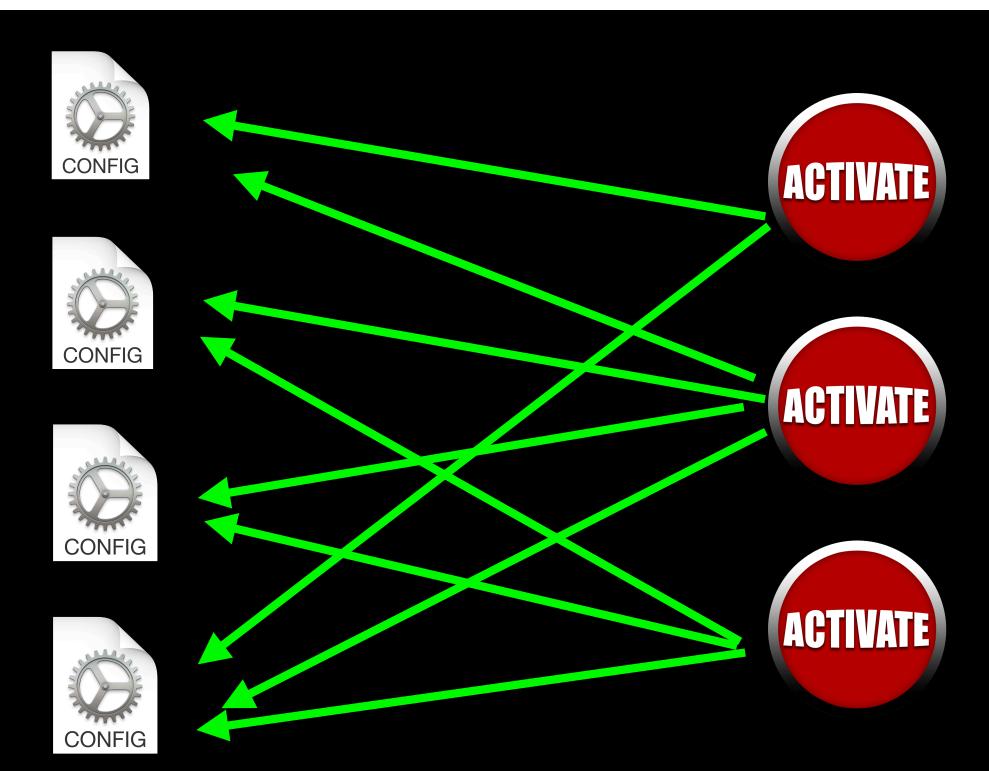












## **Activation Predicates**

- Determines activation behavior
  - Boolean logic
  - •Device will only process activation if predicate evaluates to TRUE

## Activation Predicates

Management: properties of the overall management state on the device.

# Management Declarations

- Represent properties of the overall management state
- Organization information
- MDM server capabilities
- Conveys static information to the device.

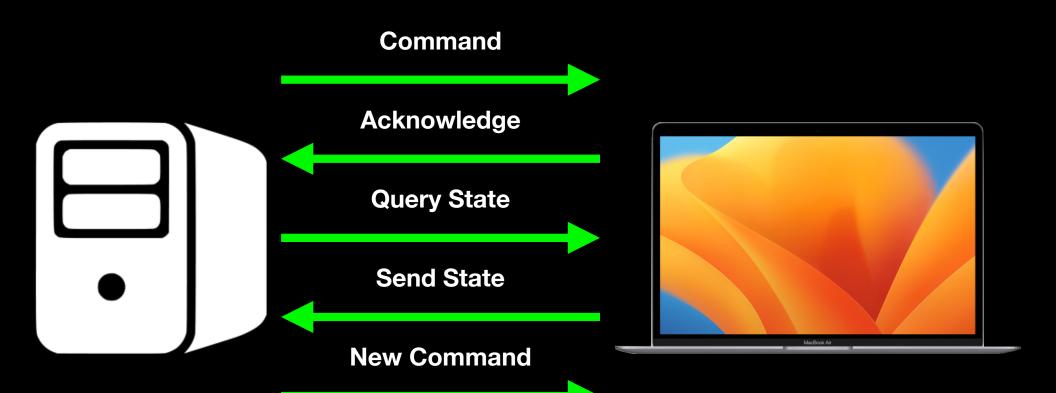
- Configuration: represents policies being applied to the device.
- Assets: data needed by a configuration.
- Activation: group of configurations
- Management: properties of the overall management state on the device.

#### Status Channel



**Status Channel** 

## MDM



#### Status Items

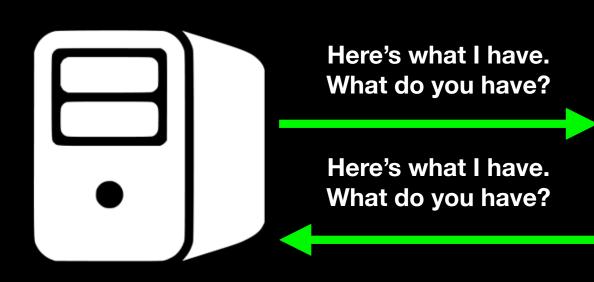
- device.operating-system.family
- device.operating-system.version
- device.model.family
- device.model.identifier

#### Status Items

### Status Items

```
"StatusItems": {
  "device": {
    "operating-system": {
      "version": "16.0"
"Errors":
```

## Extensibility





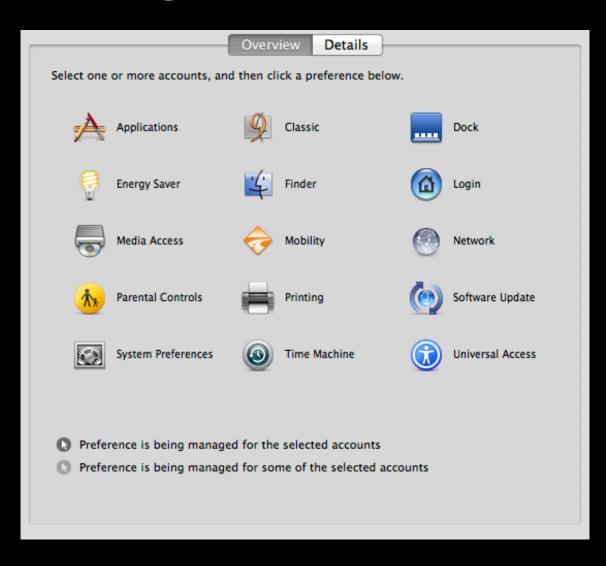
## Extensibility

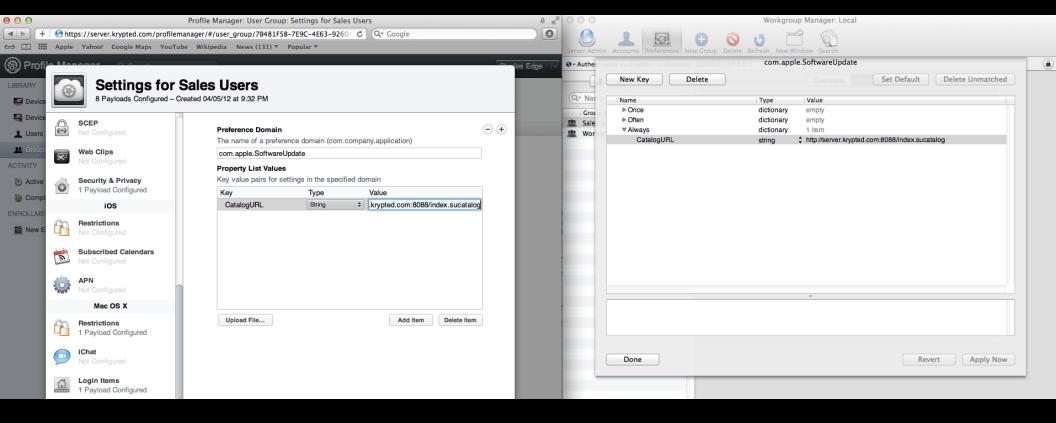
- Both endpoint and MDM server advertise what they support
  - Supported features
  - Supported payloads
  - MDM server indicates support in management declaration.
  - Client indicates support as specific status item.

- DDM is integrated into the MDM protocol for enrollment, transport and authentication.
  - Declarations and MDM commands / profiles coexist
  - Unenrolling from MDM management also removes all DDM.

- DDM is not disruptive to MDM.
  - Declarations and MDM commands / profiles coexist.
  - DDM can send and install MDM profiles as configurations.

```
"Type": "com.apple.configuration.legacy",
"Identifier": "4B0E572A-7188-4249-87B3-C58F2340ECF8",
"Server Token": "815357CC-6571-4992-A8E4-AFDB9DB0CD89",
"Payload": {
    "ProfileURL": "https://mdm.server.goes.here/profiles/importantsetting.mobileconfig"
}
```





```
"Type": "com.apple.configuration.legacy",
"Identifier": "4B0E572A-7188-4249-87B3-C58F2340ECF8",
"Server Token": "815357CC-6571-4992-A8E4-AFDB9DB0CD89",
"Payload": {
    "ProfileURL": "https://mdm.server.goes.here/profiles/importantsetting.mobileconfig"
}
```

### UNDERSTAND



makeameme.org



#### New DDM-managed software updates

- Can enforce software updates for a specified OS version and build at specified time.
- Available for the following platforms:
  - macOS
  - iOS
  - iPadOS

#### New DDM-managed software updates

- DDM software update configurations can coexist with MDM software update commands
  - Software updates enforced by DDM will take precedence over MDM commands or profiles



#### **DDM-managed app deployment**

- DDM configuration can specify an app be available on a device at a desired time.
  - App can be sent to the device ahead of time, then made available when needed.
  - Administrators can switch between sets of apps as needed.

#### DDM-managed app deployment

- App can be shown to user without the app being installed, so that the user can choose when to install it.
  - Since user is choosing to install, no consent prompt appears.
- Asynchronous reporting keeps the admin up to date on changes to managed apps on the endpoints.

#### **DDM-managed security compliance**

- sshd
- sudo
- PAM
- CUPS
- Apache httpd
- bash
- zsh

#### **DDM-managed security compliance**

- FileVault status monitoring
  - Status item: diskmanagement.filevault.enabled
    - Returns a boolean value to indicate whether FileVault is enabled or not



# puppet







imgflip.com



#### Useful Links

Apple Mobile Device Management: <a href="https://">https://</a>
<a href="https://">developer.apple.com/documentation/devicemanagement</a>

Apple Device Management documentation: <a href="https://">https://</a>
<a href="https://">developer.apple.com/documentation/devicemanagement</a>

A Push Odyssey - Journey to the Center of APNS: https://www.youtube.com/watch?v=Z-Lg9uBbmfk

Getting MicroMDM working and working with MicroMDM: <a href="https://youtube.com/watch?v=WGKT-PyHz61">https://youtube.com/watch?v=WGKT-PyHz61</a>

Demystifying MDM: open source endeavours to manage Macs: <a href="https://youtube.com/watch?v=6DBGIDcBKFw">https://youtube.com/watch?v=6DBGIDcBKFw</a>

#### **Useful Links**

WWDC 2023 What's New in managing Apple devices: <a href="https://developer.apple.com/wwdc23/10040">https://developer.apple.com/wwdc23/10040</a>

WWDC 2023 Explore advances in declarative device management: <a href="https://developer.apple.com/wwdc23/10041">https://developer.apple.com/wwdc23/10041</a>

WWDC 2022 Adopt declarative device management: <a href="https://developer.apple.com/wwdc22/10046">https://developer.apple.com/wwdc22/10046</a>

WWDC 2021 Meet Declarative Device Management: <a href="https://developer.apple.com/wwdc21/10131">https://developer.apple.com/wwdc21/10131</a>

# Downloads

PDF available from the following link:

https://tinyurl.com/PSUMac2023PDF

Keynote slides available from the following link:

https://tinyurl.com/PSUMac2023Keynote