ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΛΟΠΟΝΝΗΣΟΥ

ΜΟΝΑΔΑ ΨΗΦΙΑΚΗΣ ΔΙΑΚΥΒΕΡΝΗΣΗΣ

Οδηγός
Ασφαλούς Απομακρυσμένης Πρόσβασης
σε Υποδομές Πανεπιστημίου
μέσω Pangolin και Authentik

Pangolin Client (WireGuard) · Authentik Identity Provider · Multi-Factor Authentication (OTP)

Έκδοση 1.0

Ιούλιος 2026

Πίνακας Περιεχομένων

1. Εισαγωγή

1.1 Σκοπός του Οδηγού

Ο παρών οδηγός απευθύνεται σε μέλη του προσωπικού, ερευνητές, μεταπτυχιακούς και διδακτορικούς φοιτητές του Πανεπιστημίου Πελοποννήσου που χρειάζεται να αποκτήσουν ασφαλή, απομακρυσμένη πρόσβαση σε εσωτερικούς διακομιστές (servers) και εικονικές μηχανές (VM) του Ιδρύματος μέσω SSH ή Remote Desktop (RDP). Περιγράφει αναλυτικά, βήμα προς βήμα, κάθε στάδιο της διαδικασίας: από την υποβολή αιτήματος εξουσιοδότησης πρόσβασης, μέχρι την εγκατάσταση του λογισμικού σύνδεσης, την ενεργοποίηση του λογαριασμού, τη ρύθμιση πιστοποίησης δύο παραγόντων (2FA/OTP) και την καθημερινή χρήση της υπηρεσίας.

Ο οδηγός δεν προϋποθέτει καμία προηγούμενη εξοικείωση με το Pangolin ή το Authentik. Κάθε όρος και κάθε οθόνη που θα συναντήσει ο χρήστης εξηγείται αναλυτικά.

1.2 Τι είναι το Pangolin

Το Pangolin είναι η πλατφόρμα ασφαλούς απομακρυσμένης πρόσβασης (secure remote access platform) που χρησιμοποιεί το Πανεπιστήμιο για τη διαχείριση της πρόσβασης σε εσωτερικούς πόρους (servers, εικονικές μηχανές, εσωτερικές υπηρεσίες δικτύου). Αντί να εκθέτει τους διακομιστές απευθείας στο Internet —κάτι που θα τους καθιστούσε ευάλωτους σε επιθέσεις— το Pangolin δημιουργεί έναν κρυπτογραφημένο, ιδιωτικό «tunnel» (σήραγγα δικτύου) μεταξύ της συσκευής του εξουσιοδοτημένου χρήστη και του εσωτερικού δικτύου του Ιδρύματος, βασισμένο στο πρωτόκολλο WireGuard.

Η πρόσβαση μέσω Pangolin πραγματοποιείται μέσω ενός μικρού προγράμματος (Pangolin Client) που εγκαθίσταται στον υπολογιστή του χρήστη. Το πρόγραμμα αυτό δημιουργεί την κρυπτογραφημένη σύνδεση προς το δίκτυο του Πανεπιστημίου, ώστε ο χρήστης να μπορεί στη συνέχεια να χρησιμοποιήσει τα δικά του εργαλεία (π.χ. SSH client, Remote Desktop Connection) για να συνδεθεί στον συγκεκριμένο πόρο για τον οποίο έχει λάβει εξουσιοδότηση πρόσβασης.

1.3 Τι είναι το Authentik

Το Authentik είναι ο πάροχος ταυτότητας (Identity Provider — IdP) του Ιδρύματος. Είναι το σύστημα που επαληθεύει «ποιος είστε» πριν επιτραπεί οποιαδήποτε σύνδεση: ελέγχει το όνομα χρήστη και τον κωδικό πρόσβασης (ιδρυματικός λογαριασμός SSO) και, στη συνέχεια, τον δεύτερο παράγοντα πιστοποίησης (OTP). Το Pangolin είναι ήδη συνδεδεμένο με το Authentik, οπότε κατά την ενεργοποίηση του λογαριασμού σας στο Pangolin θα μεταφερθείτε αυτόματα στη σελίδα σύνδεσης του Authentik για να ολοκληρώσετε την ταυτοποίησή σας.

1.4 Τι είναι το Zero Trust

Το μοντέλο ασφαλείας Zero Trust («μηδενική εμπιστοσύνη») βασίζεται στην αρχή ότι καμία σύνδεση — είτε προέρχεται από το εσωτερικό δίκτυο είτε από το Internet— δεν θεωρείται εξ ορισμού αξιόπιστη.

Κάθε αίτημα πρόσβασης πρέπει να ταυτοποιείται και να εξουσιοδοτείται ρητά, για συγκεκριμένο χρήστη και συγκεκριμένο πόρο, πριν επιτραπεί η σύνδεση. Η αρχιτεκτονική Pangolin/Authentik υλοποιεί αυτή την αρχή: ο διακομιστής δεν είναι προσβάσιμος σε κανέναν εκ των προτέρων· η πρόσβαση ανοίγει μόνο μετά από επιτυχή πιστοποίηση ταυτότητας, έλεγχο εξουσιοδότησης ανά πόρο και δημιουργία κρυπτογραφημένου tunnel.

1.5 Τι είναι το Single Sign-On (SSO)

Το Single Sign-On επιτρέπει στον χρήστη να χρησιμοποιεί τα ίδια διαπιστευτήρια (τον ιδρυματικό λογαριασμό του) για να ταυτοποιείται σε πολλαπλές υπηρεσίες του Ιδρύματος, χωρίς να χρειάζεται να θυμάται ξεχωριστούς κωδικούς για κάθε σύστημα. Στο πλαίσιο του Pangolin, η ταυτοποίηση γίνεται μέσω του ίδιου ιδρυματικού λογαριασμού SSO που χρησιμοποιείται και σε άλλες υπηρεσίες του Πανεπιστημίου.

1.6 Τι είναι το OTP και το MFA

Το One-Time Password (OTP) είναι ένας κωδικός μίας χρήσης, με περιορισμένη χρονική ισχύ (συνήθως 30 δευτερόλεπτα), ο οποίος παράγεται από μια εφαρμογή Authenticator στο κινητό τηλέφωνο του χρήστη (Time-based One-Time Password — TOTP). Αποτελεί τον δεύτερο παράγοντα πιστοποίησης (second factor) στο πλαίσιο της πιστοποίησης πολλαπλών παραγόντων — Multi-Factor Authentication (MFA): ακόμη και αν κάποιος αποκτήσει τον κωδικό πρόσβασής σας, δεν μπορεί να συνδεθεί χωρίς πρόσβαση στη συσκευή σας που παράγει το OTP.

1.7 Γιατί χρησιμοποιούνται στο Πανεπιστήμιο

- Προστασία κρίσιμων ερευνητικών και διοικητικών υποδομών από μη εξουσιοδοτημένη πρόσβαση.
- Συμμόρφωση με πολιτικές ασφάλειας πληροφοριών και κανονιστικές απαιτήσεις (π.χ. προστασία προσωπικών δεδομένων).
- Εξάλειψη της ανάγκης άμεσης έκθεσης διακομιστών στο Internet (καμία ανοιχτή θύρα SSH/RDP προς τα έξω).
- Λεπτομερής, ελεγχόμενη και καταγεγραμμένη εξουσιοδότηση πρόσβασης ανά χρήστη και ανά πόρο.
- Δυνατότητα άμεσης ανάκλησης πρόσβασης σε περίπτωση αποχώρησης μέλους ή ύποπτης δραστηριότητας.

1.8 Πλεονεκτήματα Ασφαλείας

Χαρακτηριστικό	Όφελος Ασφαλείας
Κρυπτογραφημένο tunnel WireGuard	Η κίνηση δικτύου δεν είναι αναγνώσιμη από τρίτους κατά τη μεταφορά.

Χαρακτηριστικό	Όφελος Ασφαλείας
Καμία δημόσια έκθεση θυρών SSH/RDP	Οι servers δεν είναι σαρώσιμοι ή προσβάσιμοι απευθείας από το Internet.
Πιστοποίηση SSO μέσω Authentik	Κεντρική διαχείριση ταυτότητας, ενιαία πολιτική κωδικών.
MFA (OTP)	Προστασία ακόμη και σε περίπτωση διαρροής κωδικού πρόσβασης.
Εξουσιοδότηση πρόσβασης ανά πόρο	Ο χρήστης βλέπει/συνδέεται μόνο στους πόρους για τους οποίους έχει ρητή έγκριση.
Καταγεγραμμένη διαδικασία αιτήματος (ticketing)	Πλήρης ιχνηλασιμότητα: ποιος ζήτησε, ποιος ενέκρινε, πότε.

ΣΥΜΒΟΥΛΗ (TIP)

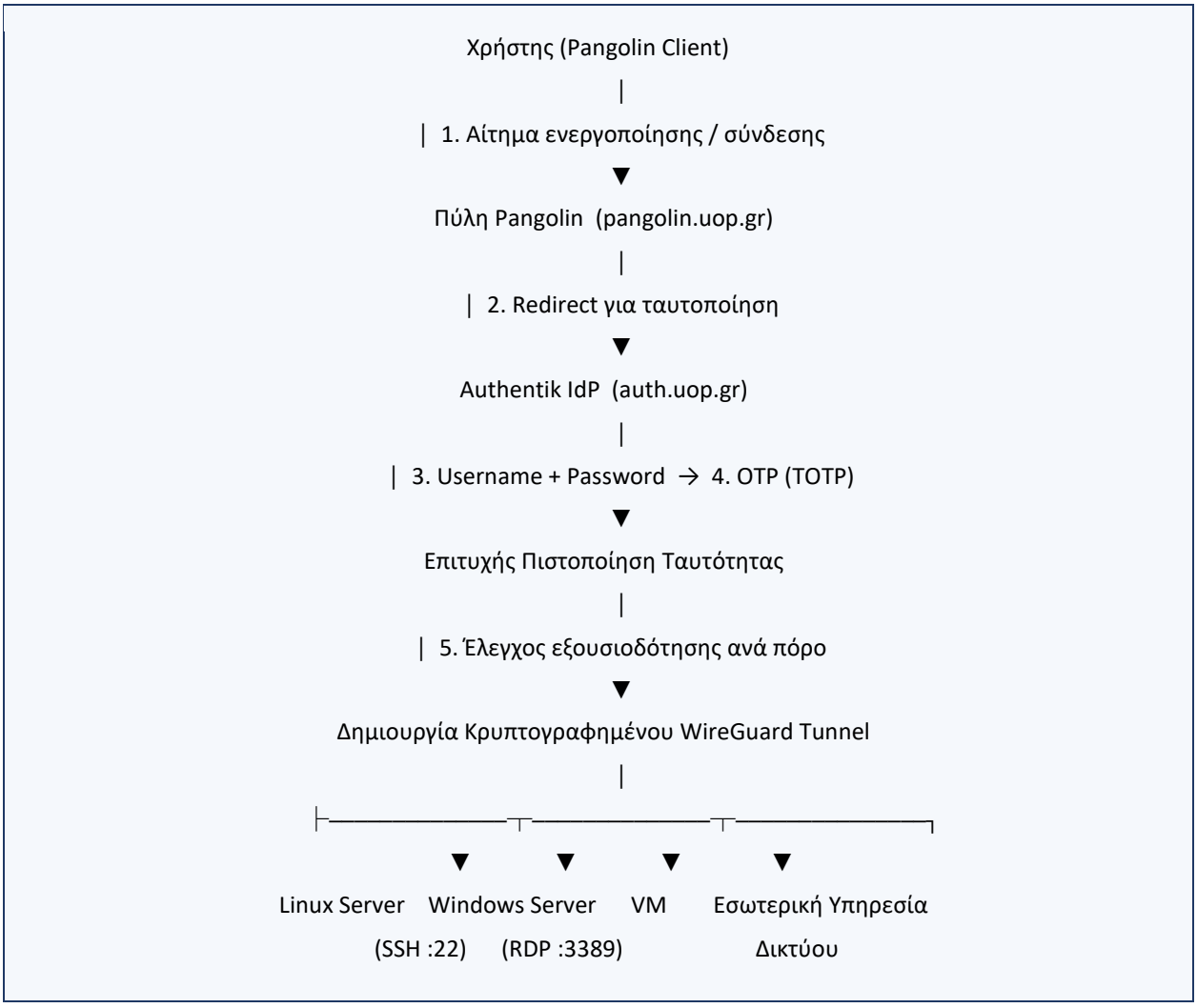
Αν είστε διαχειριστής πόρου (server) και θέλετε να παραχωρήσετε πρόσβαση σε συναδέλφους ή φοιτητές σας, δείτε την ενότητα 5 «Διαδικασία Αίτησης Εξουσιοδότησης Πρόσβασης».

2. Αρχιτεκτονική και Τρόπος Λειτουργίας

2.1 Επισκόπηση

Σε αντίθεση με λύσεις πρόσβασης τύπου «reverse proxy» όπου ο χρήστης ανοίγει μια συνεδρία SSH/RDP μέσα στον browser, η εγκατάσταση του Πανεπιστημίου χρησιμοποιεί το μοντέλο Pangolin Client: ένα πρόγραμμα που εγκαθίσταται στη συσκευή του χρήστη και δημιουργεί ιδιωτικό, κρυπτογραφημένο δίκτυο (overlay network) μέσω WireGuard ανάμεσα στη συσκευή και το εσωτερικό δίκτυο του Ιδρύματος. Μέσα σε αυτό το ιδιωτικό δίκτυο, ο χρήστης συνδέεται στον πόρο του χρησιμοποιώντας το δικό του, εξωτερικό λογισμικό (π.χ. PuTTY, OpenSSH, Microsoft Remote Desktop).

2.2 Διάγραμμα Ροής Αρχιτεκτονικής



Διάγραμμα 1 — Ροή πιστοποίησης και δημιουργίας ασφαλούς διαύλου πρόσβασης.

2.3 Ανάλυση Βημάτων

1. **Εκκίνηση Pangolin Client:** ο χρήστης εκκινεί το πρόγραμμα Pangolin Client στον υπολογιστή του και επιλέγει σύνδεση στην πύλη του Ιδρύματος.
2. **Ανακατεύθυνση σε Authentik:** το Pangolin ανακατευθύνει το αίτημα ταυτοποίησης στο Authentik, τον Identity Provider του Ιδρύματος.
3. **Εισαγωγή διαπιστευτηρίων:** ο χρήστης εισάγει το ιδρυματικό του username και password (πρώτος παράγοντας πιστοποίησης).
4. **Δεύτερος παράγοντας (OTP):** το Authentik ζητά κωδικό OTP από εφαρμογή Authenticator (ή, εναλλακτικά, μέσω e-mail). Μόνο μετά την επιτυχή επαλήθευση και των δύο παραγόντων θεωρείται η ταυτοποίηση πλήρης.
5. **Έλεγχος εξουσιοδότησης:** το σύστημα ελέγχει σε ποιους πόρους έχει εγκεκριμένη πρόσβαση ο συγκεκριμένος χρήστης, βάσει του αιτήματος που έχει εγκριθεί από τη Μονάδα Ψηφιακής Διακυβέρνησης (βλ. ενότητα 5).
6. **Δημιουργία tunnel:** ανοίγει κρυπτογραφημένο WireGuard tunnel ανάμεσα στη συσκευή του χρήστη και το εσωτερικό δίκτυο του Ιδρύματος.
7. **Πρόσβαση στον πόρο:** ο χρήστης χρησιμοποιεί το δικό του εργαλείο (SSH client ή RDP client) για να συνδεθεί απευθείας στη διεύθυνση IP του εγκεκριμένου πόρου, μέσα από το ασφαλές tunnel.

ΑΣΦΑΛΕΙΑ (SECURITY)

Το firewall κάθε πόρου είναι ρυθμισμένο ώστε να δέχεται συνδέσεις στις θύρες SSH (22) ή RDP (3389) αποκλειστικά από το εύρος διευθύνσεων του WireGuard tunnel του Pangolin. Οποιαδήποτε άλλη προσπάθεια σύνδεσης απορρίπτεται αυτόματα, ανεξάρτητα από το αν διαθέτει έγκυρα διαπιστευτήρια.

2.4 Βασικά Στοιχεία της Αρχιτεκτονικής

Στοιχείο	Ρόλος
Pangolin Client	Λογισμικό στη συσκευή του χρήστη που δημιουργεί το WireGuard tunnel προς το Ίδρυμα.
Πύλη Pangolin (pangolin.uop.gr)	Σημείο εισόδου· διαχειρίζεται την ενεργοποίηση λογαριασμού και τη δρομολόγηση προς το Authentik.
Authentik IdP (auth.uop.gr)	Επαληθεύει ταυτότητα χρήστη (username/password + OTP).
WireGuard Tunnel	Κρυπτογραφημένο ιδιωτικό δίκτυο (overlay network) μεταξύ χρήστη και εσωτερικού δικτύου.

Στοιχείο	Ρόλος
Πόρος (Resource/Server)	Ο εσωτερικός διακομιστής/VM στον οποίο τελικά συνδέεται ο χρήστης μέσω SSH ή RDP.
Firewall πόρου	Επιτρέπει συνδέσεις SSH/RDP μόνο από το εύρος IP του WireGuard tunnel.

3. Προαπαιτούμενα

3.1 Λογαριασμός και Εξουσιοδότηση

- Ενεργός ιδρυματικός λογαριασμός (SSO username/password).
- Εγκεκριμένο αίτημα εξουσιοδότησης πρόσβασης για τον συγκεκριμένο πόρο (βλ. ενότητα 5) — χωρίς αυτό δεν είναι δυνατή η πρόσβαση, ανεξάρτητα από το αν έχετε εγκαταστήσει τον Pangolin Client.

3.2 Συσκευή και Λογισμικό

Απαίτηση	**Λεπτομέρειες**
Λειτουργικό σύστημα	Windows 11, macOS 12+ ή σύγχρονη διανομή Linux.
Pangolin Client	Λήψη και εγκατάσταση από τον επίσημο σύνδεσμο (ενότητα 6).
Πρόσβαση στο Internet	Σταθερή σύνδεση Internet (ενσύρματη ή ασύρματη).
Authenticator App	Εφαρμογή κινητού για παραγωγή κωδικών TOTP (π.χ. Google Authenticator, Microsoft Authenticator, Aegis, FreeOTP, 2FAS, Bitwarden Authenticator).
Browser	Σύγχρονος browser (Chrome, Edge, Firefox, Safari) για την αρχική ταυτοποίηση μέσω Authentik.
Λογισμικό SSH client	Π.χ. OpenSSH (ενσωματωμένο σε Windows/macOS/Linux), PuTTY — απαιτείται για πρόσβαση σε Linux servers.
Λογισμικό RDP client	Π.χ. Microsoft Remote Desktop Connection (Windows), Microsoft Remote Desktop (macOS/iOS) — απαιτείται για πρόσβαση σε Windows servers.
Δικαιώματα εγκατάστασης	Δικαιώματα διαχειριστή (ή αντίστοιχα) στη συσκευή σας για την εγκατάσταση του Pangolin Client.

3.3 Δικτυακές Απαιτήσεις

- Το firewall της τοπικής σας συσκευής ή δικτύου (π.χ. οικιακό router, εταιρικό δίκτυο) δεν πρέπει να μπλοκάρει εξερχόμενη κίνηση WireGuard (UDP).
- Σε περίπτωση χρήσης δικτύου τρίτου οργανισμού με αυστηρούς περιορισμούς εξερχόμενης κίνησης, ενδέχεται να απαιτηθεί συνεννόηση με τον τοπικό διαχειριστή δικτύου.
- Δεν απαιτείται καμία ενέργεια στο DNS από την πλευρά του χρήστη· η ανάλυση ονομάτων pangolin.uop.gr και auth.uop.gr γίνεται κανονικά μέσω του δημόσιου DNS.

ΣΗΜΕΙΩΣΗ (NOTE)

Δεν χρειάζεται να έχετε χρησιμοποιήσει ξανά VPN λογισμικό. Ο Pangolin Client είναι αυτόνομος και δεν απαιτεί επιπλέον ρυθμίσεις δικτύου από τον χρήστη.

4. Επισκόπηση Διαδικασίας — Από το Αίτημα έως τη Σύνδεση

Η συνολική διαδικασία απόκτησης πρόσβασης περιλαμβάνει πέντε βασικά στάδια, τα οποία αναλύονται στα επόμενα κεφάλαια:

1. Υποβολή και έγκριση αιτήματος εξουσιοδότησης πρόσβασης (ενότητα 5).
2. Ρύθμιση του firewall στον πόρο, ώστε να δέχεται συνδέσεις μόνο μέσω Pangolin (ενότητα 6).
3. Εγκατάσταση του Pangolin Client στη συσκευή του χρήστη (ενότητα 7).
4. Πρώτη σύνδεση, ενεργοποίηση λογαριασμού και ρύθμιση 2FA/OTP (ενότητα 8).
5. Καθημερινή σύνδεση/αποσύνδεση και πρόσβαση στους πόρους μέσω SSH ή RDP (ενότητες 9-11).

ΣΗΜΑΝΤΙΚΟ (IMPORTANT)

Τα στάδια Α και Β αποτελούν προαπαιτούμενο και συνήθως πραγματοποιούνται μία φορά, πριν αποκτήσει πρόσβαση ο χρήστης σε έναν συγκεκριμένο πόρο. Η εγκατάσταση Client (στάδιο Γ) γίνεται μία φορά ανά συσκευή χρήστη, ανεξάρτητα από τον αριθμό πόρων στους οποίους θα αποκτήσει πρόσβαση.

5. Διαδικασία Αίτησης Εξουσιοδότησης Πρόσβασης σε Πόρους

5.1 Γενικές Αρχές

Η πρόσβαση σε κάθε πόρο μέσω Pangolin δεν είναι αυτόματη. Ο διαχειριστής-υπεύθυνος του πόρου πρέπει να υποβάλει αίτημα στη Μονάδα Ψηφιακής Διακυβέρνησης, η οποία εκχωρεί εξουσιοδότηση στον συγκεκριμένο πόρο και στους συγκεκριμένους χρήστες που έχουν ζητηθεί. Η εξουσιοδότηση παρέχεται πάντα ανά πόρο και ανά χρήστη — η έγκριση πρόσβασης σε έναν server δεν συνεπάγεται αυτόματα πρόσβαση σε άλλους πόρους.

5.2 Υποβολή Αιτήματος μέσω Συστήματος Ticketing

Υποβάλετε νέο ticket στη διεύθυνση:

ΣΗΜΕΙΩΣΗ (NOTE)

https://helpdesk.uop.gr/

με θέμα στη μορφή:

ΣΗΜΑΝΤΙΚΟ (IMPORTANT)

[PANGOLIN] Αίτημα πρόσβασης – <username> – <όνομα πόρου>

ΠΡΟΣΟΧΗ (WARNING)

Αιτήματα που υποβάλλονται προφορικά, τηλεφωνικά ή μέσω e-mail δεν γίνονται δεκτά. Απαιτείται πάντα γραπτή καταγραφή μέσω του συστήματος ticketing, για λόγους ελέγχου και ασφάλειας.

5.3 Στοιχεία που Πρέπει να Περιλαμβάνει το Αίτημα

Πεδίο	Περιγραφή	Παράδειγμα
Ονοματεπώνυμο	Πλήρες όνομα αιτούντος	Γιώργος Παπαδόπουλος
Ιδρυματικό username	Το username SSO	gpapadop
Τμήμα / Εργαστήριο	Οργανική μονάδα στην οποία ανήκει	Εργαστήριο Δικτύων
Πόρος / Server	Όνομα ή IP του πόρου	srv-lab01 / 192.168.x.x
Τύπος πρόσβασης	Τι χρειάζεται ακριβώς	SSH, RDP
Σκοπός χρήσης	Σύντομη αιτιολόγηση	Εκτέλεση πειραμάτων έρευνας

Πεδίο	Περιγραφή	Παράδειγμα
Διάρκεια	Μόνιμη ή προσωρινή (με ημερομηνία λήξης)	Έως 31/12/2026
Υπεύθυνος / Επιβλέπων	Ονοματεπώνυμο επιβλέποντος	Δρ. Μαρία Κωνσταντίνου
Χρήστες με δικαίωμα πρόσβασης*	Ονοματεπώνυμο / username SSO κάθε επιπλέον χρήστη	—

5.3.1 Πρόσβαση για Επιπλέον Χρήστες — Τεκμηρίωση Συναίνεσης

Όταν το αίτημα ζητά εξουσιοδοτημένη πρόσβαση στον πόρο και για χρήστες πέραν του αιτούντος, η απλή αναγραφή του ονόματός τους από τον κάτοχο του πόρου **δεν αρκεί**. Ο κάτοχος δεν μπορεί να εκπροσωπήσει ή να εγγυηθεί εκ μέρους τρίτου τη συναίνεσή του σε πρόσβαση που συνεπάγεται ευθύνη χρήσης και καταγραφή δραστηριότητας.

Η διαδικασία ακολουθεί τα εξής βήματα:

1. Ο κάτοχος/διαχειριστής του πόρου υποβάλλει ένα ενιαίο ticket, με όλα τα στοιχεία του πίνακα παραπάνω και πλήρη κατάλογο των επιπλέον χρηστών για τους οποίους ζητείται πρόσβαση.
2. Για **κάθε** επιπλέον χρήστη, πρέπει να επισυνάπτεται στο ίδιο ticket ρητή, τεκμηριωμένη συναίνεση, με έναν από τους παρακάτω αποδεκτούς τρόπους:
    - **Επισύναψη μηνύματος mail του ίδιου του χρήστη προς τον κάτοχο του πόρου**, το οποίο έχει αποσταλεί από το ιδρυματικό του e-mail/λογαριασμό, με σαφή διατύπωση αποδοχής (π.χ. «Αποδέχομαι αίτημα πρόσβασης στον πόρο <όνομα πόρου> για τον σκοπό που περιγράφεται στο παρόν ticket»). Η αποστολή από ιδρυματικό λογαριασμό λειτουργεί ως ταυτοποίηση του χρήστη.
    - **Επισύναψη υπογεγραμμένης φόρμας συναίνεσης** ψηφιακά υπογεγραμμένης
3. Το αίτημα θεωρείται πλήρες προς αξιολόγηση μόνο όταν έχει τεκμηριωθεί η συναίνεση όλων των αναφερόμενων επιπλέον χρηστών. Η Μονάδα Ψηφιακής Διακυβέρνησης δεν εγκρίνει πρόσβαση για χρήστη του οποίου η συναίνεση δεν είναι τεκμηριωμένη στο ticket, ακόμη και αν έχει κατονομαστεί από τον κάτοχο του πόρου.
4. Σε περίπτωση μερικής τεκμηρίωσης (π.χ. συναίνεση μόνο για κάποιους από τους αναφερόμενους χρήστες), η εξουσιοδότηση παρέχεται μόνο για τους χρήστες με πλήρως τεκμηριωμένη συναίνεση· για τους υπόλοιπους απαιτείται συμπληρωματική επιβεβαίωση πριν την έγκριση.

ΣΗΜΕΙΩΣΗ: Η ευθύνη συγκέντρωσης και επισύναψης των επιβεβαιώσεων συναίνεσης βαρύνει τον κάτοχο/διαχειριστή του πόρου που υποβάλλει το αίτημα. Η Μονάδα Ψηφιακής Διακυβέρνησης δεν αναλαμβάνει να επικοινωνήσει μεμονωμένα με κάθε επιπλέον χρήστη για επιβεβαίωση.

5.4 Εκχώρηση Πρόσβασης

Μετά την επεξεργασία του αιτήματος από τη Μονάδα Ψηφιακής Διακυβέρνησης, θα λάβετε απάντηση μέσω του συστήματος ticketing και στο ιδρυματικό σας e-mail, η οποία θα περιλαμβάνει επιβεβαίωση της έγκρισης καθώς και τα στοιχεία που θα χρειαστείτε ώστε να ρυθμίσετε τον πόρο για πρόσβαση μέσω Pangolin (βλ. ενότητα 6).

ΣΗΜΕΙΩΣΗ (NOTE)

Η Μονάδα Ψηφιακής Διακυβέρνησης διατηρεί το δικαίωμα να ανακαλέσει οποιαδήποτε εξουσιοδότηση χωρίς προειδοποίηση σε περίπτωση παραβίασης πολιτικής ασφαλείας ή κατάχρησης πρόσβασης.

5.5 Ανάκληση ή Τροποποίηση Πρόσβασης

Εάν χρειαστεί να ανακληθεί ή να τροποποιηθεί υπάρχουσα πρόσβαση (π.χ. λόγω αποχώρησης διδακτορικού ή μεταπτυχιακού φοιτητή, ολοκλήρωσης έργου, αλλαγής ρόλου), υποβάλλεται νέο ticket με θέμα:

ΣΗΜΑΝΤΙΚΟ (IMPORTANT)

[PANGOLIN] Ανάκληση πρόσβασης – <username> – <όνομα πόρου>

ΚΑΛΗ ΠΡΑΚΤΙΚΗ (BEST PRACTICE)

Υποχρέωση επιβλέποντος: σε περίπτωση αποχώρησης μέλους ομάδας που είχε πρόσβαση σε πόρους, ο επιβλέπων υποχρεούται να ενημερώσει άμεσα τη Μονάδα Ψηφιακής Διακυβέρνησης για την ανάκληση της πρόσβασης.

6. Ρυθμίσεις Πόρου — Firewall

Μετά την έγκριση του αιτήματος (ενότητα 5), ο διαχειριστής του πόρου λαμβάνει στοιχεία ρύθμισης μέσω ticketing/e-mail. Για να εξασφαλιστεί ότι κανείς δεν μπορεί να συνδεθεί απευθείας από το Internet στον πόρο, το firewall του πόρου πρέπει να ρυθμιστεί ώστε να δέχεται εισερχόμενες συνδέσεις στις σχετικές θύρες (π.χ. 22 για SSH, 3389 για RDP) αποκλειστικά από το εύρος διευθύνσεων IP του WireGuard tunnel του Pangolin. Κάθε άλλη προσπάθεια σύνδεσης πρέπει να απορρίπτεται.

6.1 Γενική Αρχή Ρύθμισης

1. Προσδιορίστε το εύρος IP διευθύνσεων του WireGuard tunnel, όπως αναγράφεται στα στοιχεία που σας απεστάλησαν.
2. Δημιουργήστε κανόνα firewall που επιτρέπει εισερχόμενη κίνηση στη θύρα της υπηρεσίας (SSH/RDP) μόνο από το συγκεκριμένο εύρος.
3. Προσθέστε ρητό κανόνα απόρριψης (deny/drop) για κάθε άλλη προέλευση στην ίδια θύρα.
4. Επαληθεύστε ότι δεν υπάρχουν προγενέστεροι κανόνες που επιτρέπουν ευρύτερη πρόσβαση (π.χ. “allow from any”) στις ίδιες θύρες.

6.2 Ενδεικτικές Οδηγίες ανά Λειτουργικό Σύστημα

Λειτουργικό Σύστημα	Εργαλείο Firewall	Ενέργεια
Linux (Ubuntu/Debian)	ufw	Περιορισμός κανόνα ufw allow στη θύρα 22 ώστε να ισχύει μόνο για το subnet του Pangolin tunnel· αφαίρεση τυχόν γενικού κανόνα allow 22/tcp.
Linux (RHEL/CentOS/Rocky)	firewalld	Δημιουργία rich rule που επιτρέπει την υπηρεσία ssh μόνο από το συγκεκριμένο source IP range του tunnel.
Windows Server	Windows Defender Firewall	Ρύθμιση κανόνα εισερχόμενων συνδέσεων για τη θύρα 3389 (RDP) ώστε το πεδίο «Remote IP address» να περιορίζεται στο εύρος του Pangolin tunnel.
macOS (server use)	pf / Application Firewall	Αντίστοιχος περιορισμός εισερχόμενης κίνησης στο εύρος του tunnel.

ΠΡΟΣΟΧΗ (WARNING)

1. Μέχρι να ολοκληρωθεί σωστά η ρύθμιση του firewall, ο πόρος είτε δεν θα είναι προσβάσιμος μέσω Pangolin είτε —αν παραμείνουν παλαιοί κανόνες— ενδέχεται να

Λειτουργικό Σύστημα	Εργαλείο Firewall	Ενέργεια

παραμένει εκτεθειμένος απευθείας στο Internet. Επικοινωνήστε με τη Μονάδα Ψηφιακής Διακυβέρνησης για επιβεβαίωση πριν θεωρήσετε τη ρύθμιση ολοκληρωμένη.

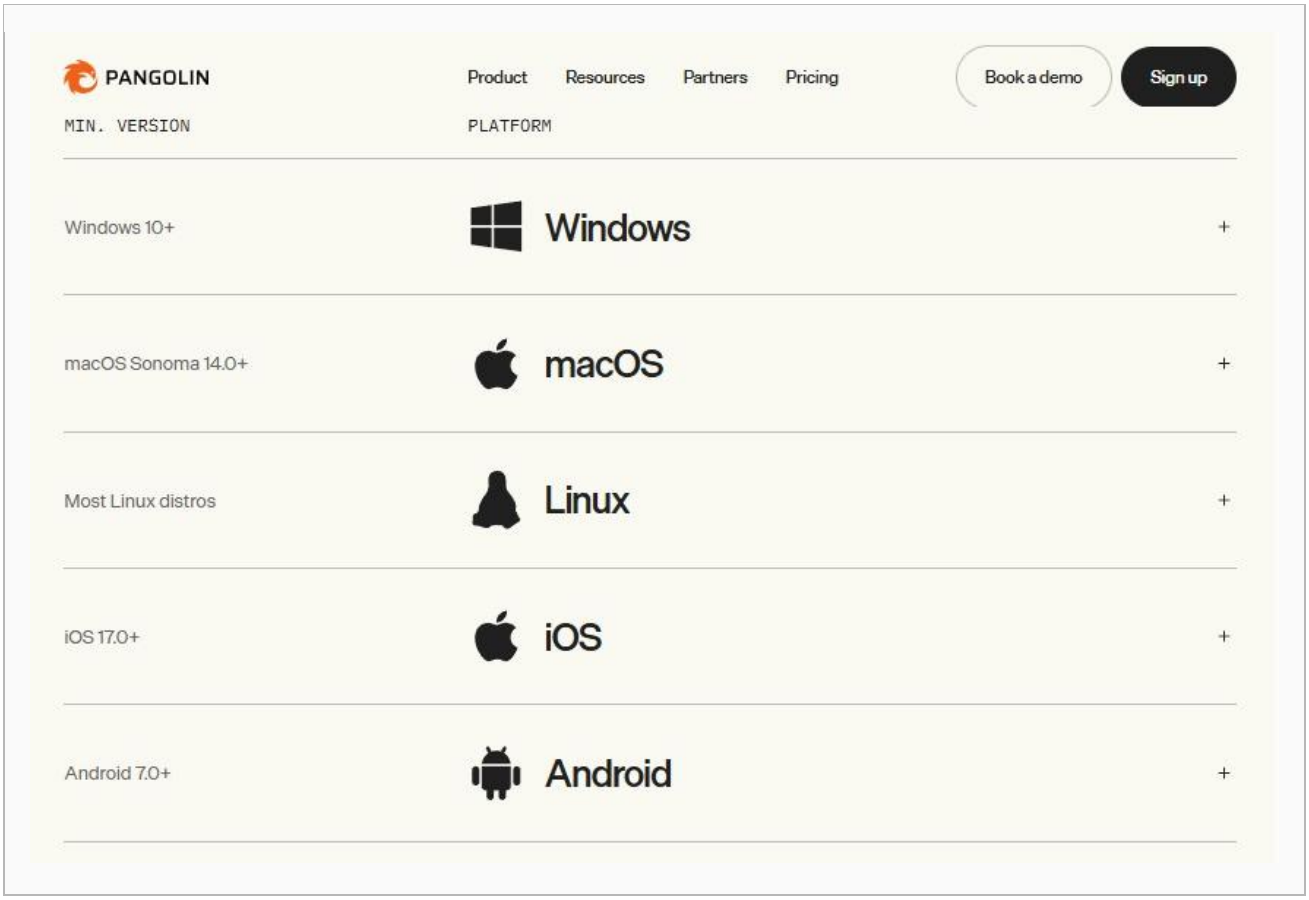
2. Για τη διασφάλιση της συμμόρφωσης με την πολιτική ασφαλούς πρόσβασης, θα διενεργούνται περιοδικοί έλεγχοι στους εξυπηρετητές, προκειμένου να επιβεβαιώνεται η ορθή εφαρμογή των προβλεπόμενων ρυθμίσεων.
3. Η διαπίστωση απόκλισης ή μη συμμόρφωσης με τις καθορισμένες απαιτήσεις θα θεωρείται παραβίαση της πολιτικής πρόσβασης στους εξυπηρετητές και θα αντιμετωπίζεται ανάλογα.

7. Εγκατάσταση του Pangolin Client

Η πρόσβαση σε εσωτερικούς πόρους απαιτεί την εγκατάσταση ενός μικρού προγράμματος σύνδεσης (client) στη συσκευή σας. Ακολουθήστε τα βήματα που αντιστοιχούν στο λειτουργικό σας σύστημα.

7.1 Λήψη του Προγράμματος Εγκατάστασης

1. Επισκεφθείτε τον σύνδεσμο λήψης: https://pangolin.net/downloads
2. Επιλέξτε την έκδοση που αντιστοιχεί στο λειτουργικό σας σύστημα (Windows / macOS / Linux).



7.2 Εγκατάσταση σε Windows

1. Εκτελέστε το αρχείο εγκατάστασης (.exe ή .msi).
2. Επιβεβαιώστε τυχόν μήνυμα ασφαλείας των Windows (SmartScreen), επιλέγοντας «Περισσότερες πληροφορίες» → «Εκτέλεση ούτως ή άλλως», αν εμφανιστεί.
3. Ολοκληρώστε τον οδηγό εγκατάστασης. Το πρόγραμμα εγκαθίσταται και εκτελείται ως υπηρεσία στο παρασκήνιο· δημιουργείται εικονίδιο στην επιφάνεια εργασίας και στη γραμμή εργασιών (system tray).

7.3 Εγκατάσταση σε macOS

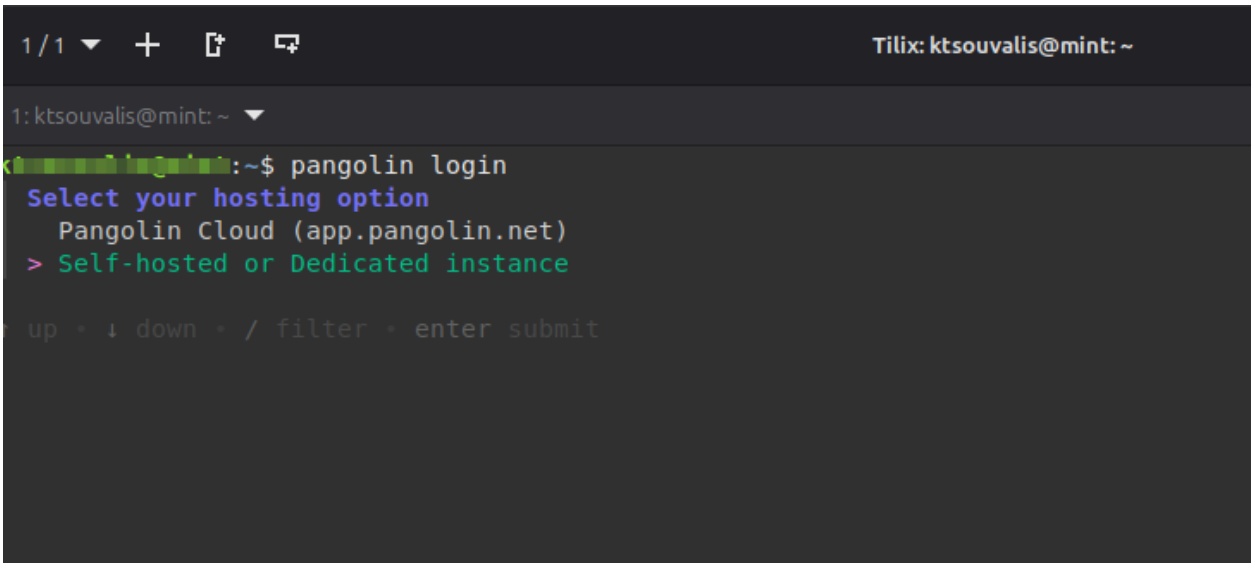
1. Ανοίξτε το αρχείο .dmg που κατεβάσατε.
2. Σύρετε το εικονίδιο της εφαρμογής στον φάκελο «Εφαρμογές» (Applications).
3. Κατά την πρώτη εκτέλεση, εγκρίνετε την άδεια πρόσβασης σε δίκτυο όταν σας ζητηθεί από το macOS.

7.4 Εγκατάσταση σε Linux

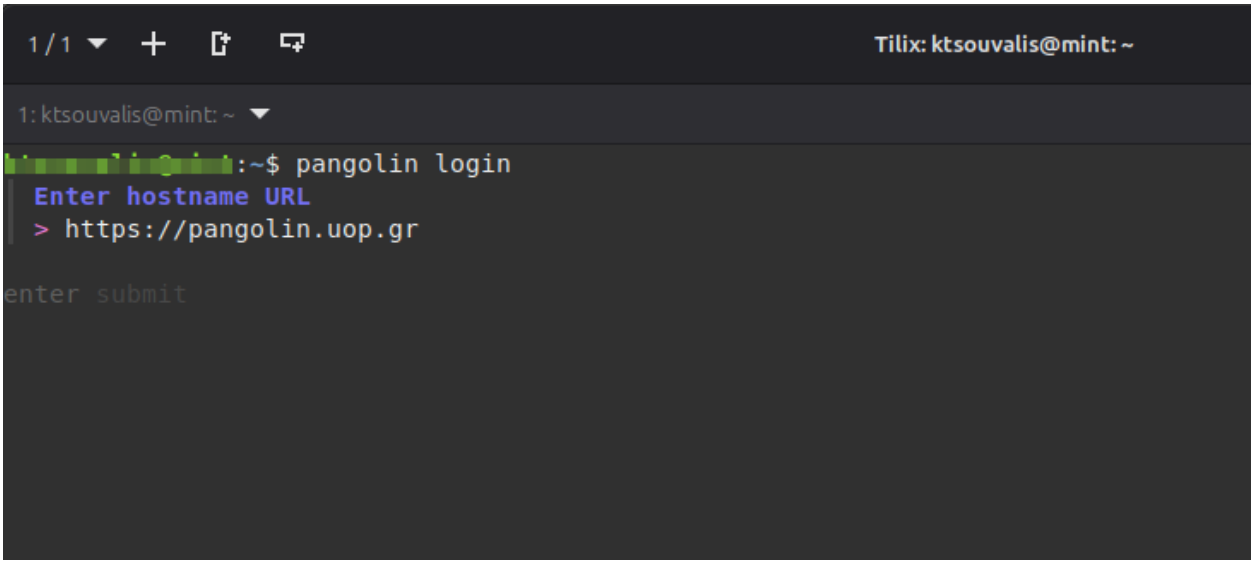
1. Εκτελέστε στο τερματικό την εντολή που κατεβάζει και εγκαθιστά το `pangolin cli`:

   ```
   curl -fsSL https://static.pangolin.net/get-cli.sh | bash
   ```

2. Για να ξεκινήσει η διαδικασία πιστοποίησης εκτελέστε:
   `pangolin login`
   και επιλέξτε `Self-hosted or Dedicated instance` και πατήστε `Enter`

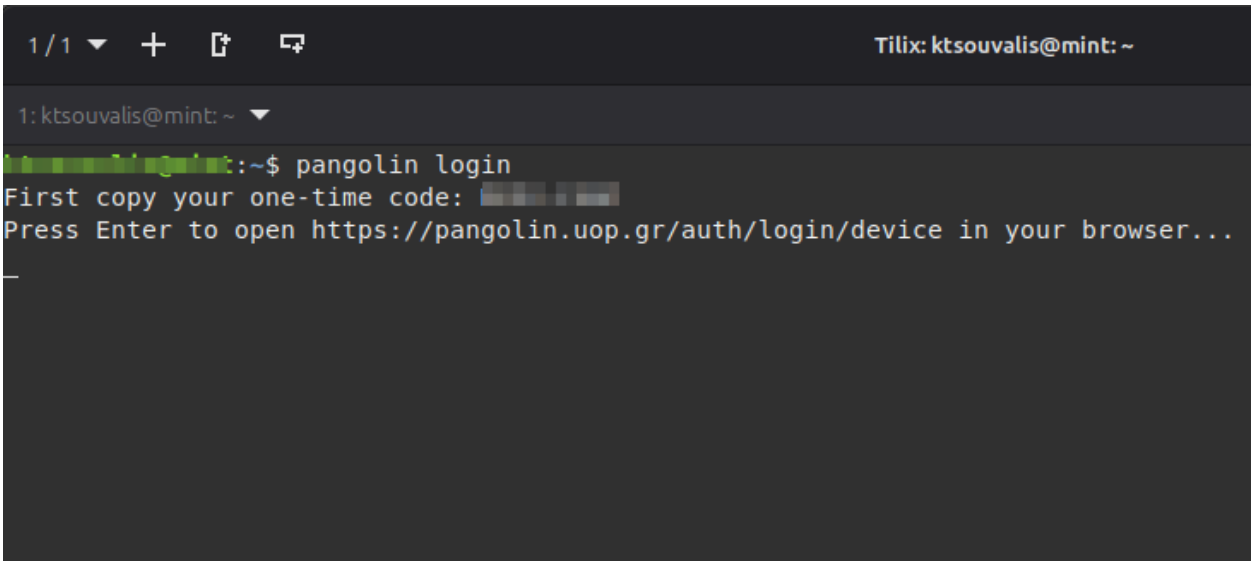


3. Πληκτρολογήστε https://pangolin.uop.gr



και πατήστε Enter

4. Στην επόμενη οθόνη, σημειώστε τον 8ψήφιο κωδικό που σας δίνει το `pangolin-cli` (ενδέχεται να μη σας χρειαστεί, αλλά καλό είναι να τον σημειώσετε/αντιγράψετε) και πατήστε `Enter`



5. Εδώ ξεκινά η διαδικασία πιστοποίησης χρήστη, της οποίας τα βήματα περιγράφονται στην παράγραφο 8.2 και στην εικόνα που προηγείται της συγκεκριμένης παραγράφου

ΣΥΜΒΟΥΛΗ (TIP)

Σε όλα τα λειτουργικά συστήματα, η εγκατάσταση πραγματοποιείται μία φορά ανά συσκευή. Δεν χρειάζεται επανεγκατάσταση για κάθε νέο πόρο στον οποίο αποκτάτε πρόσβαση.

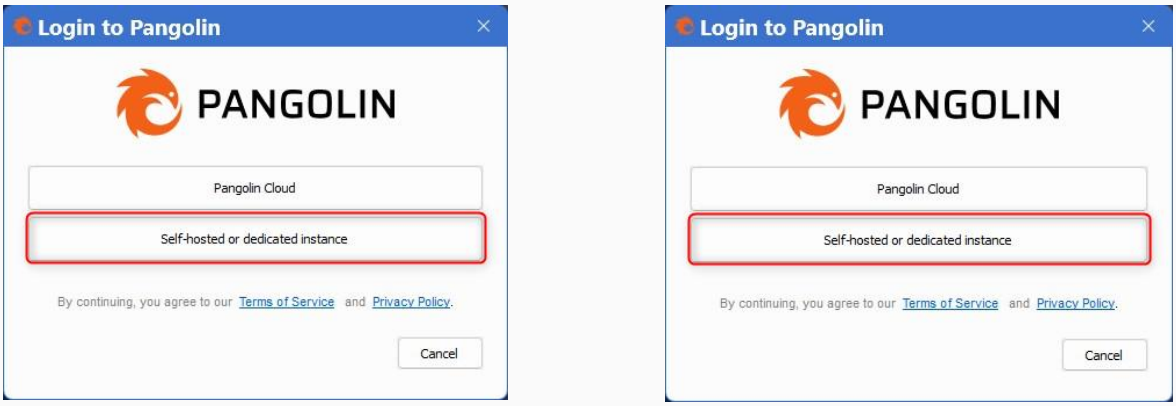
8. Πρώτη Σύνδεση και Ρύθμιση 2FA (OTP)

Κατά την πρώτη εκκίνηση, το πρόγραμμα θα σας ζητήσει τη διεύθυνση της πύλης (Pangolin Server URL) και τα στοιχεία του ιδρυματικού σας λογαριασμού, ώστε να ενεργοποιήσετε τον λογαριασμό σας στο Pangolin. Τα στοιχεία ενεργοποίησης χρειάζονται συνήθως μόνο μία φορά· στις επόμενες χρήσεις το πρόγραμμα θυμάται τη ρύθμιση.

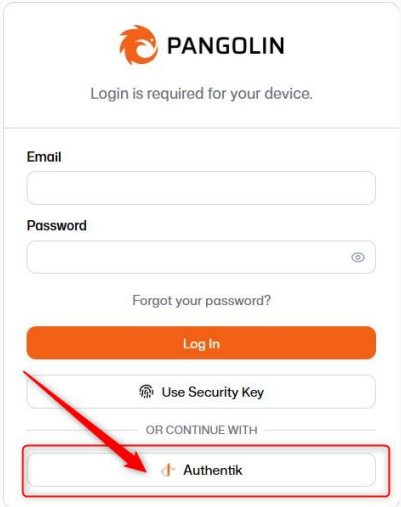
8.1 Άνοιγμα της Σελίδας Σύνδεσης

Υπάρχουν δύο τρόποι να ξεκινήσετε την ενεργοποίηση του λογαριασμού σας:

- Μέσω του Pangolin Client: κάντε κλικ στο εικονίδιο του προγράμματος στη γραμμή εργασιών, επιλέξτε «Login to Account» και έπειτα «Self-hosted or dedicated instance». Στο πεδίο Pangolin Server URL επικολλήστε https://pangolin.uop.gr/ και πατήστε «Login».
- Μέσω browser: επισκεφθείτε απευθείας τη διεύθυνση https://pangolin.uop.gr/ από τον browser σας και επιλέξτε «Authentik».



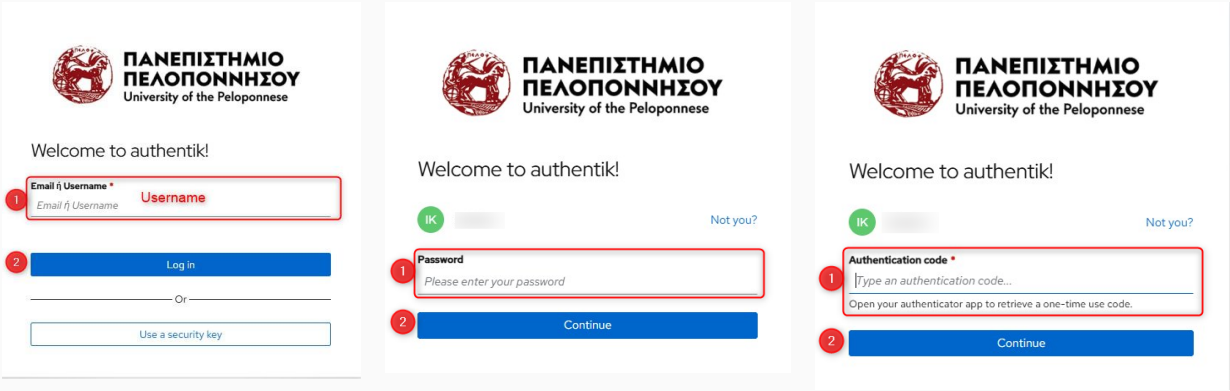
Pangolin Client - «Login to Account» και «Self-hosted or dedicated instance»· πεδίο εισαγωγής Server URL.



Pangolin - Κάνετε κλικ στο κουμπί Authentik

8.2 Ανακατεύθυνση για Ταυτοποίηση μέσω Authentik

Θα μεταφερθείτε αυτόματα στη σελίδα σύνδεσης Authentik του Ιδρύματος (https://auth.uop.gr/). Εισάγετε το όνομα χρήστη (username) και τον κωδικό πρόσβασης (password) του ιδρυματικού σας λογαριασμού.



Φόρμα σύνδεσης Authentik με πεδία username, password, OTP (εφόσον έχετε ήδη συνδεθεί προγενέστερα στο https://auth.uop.gr) και λογότυπο Ιδρύματος.

ΣΗΜΕΙΩΣΗ (NOTE)

Πατήστε το κουμπί «Continue» μόνο εφόσον στο επόμενο βήμα ρύθμισης 2FA επιθυμείτε η λήψη OTP να γίνεται μέσω εφαρμογής κινητού (Επιλογή Α, ενότητα 8.3).

8.3 Ρύθμιση Διπλής Επαλήθευσης Ταυτότητας (2FA)

Μετά την επιτυχή εισαγωγή του κωδικού πρόσβασης, το σύστημα ανιχνεύει ότι δεν έχετε ρυθμίσει ακόμη 2FA και σας οδηγεί αυτόματα στη ρύθμιση. Διατίθενται δύο επιλογές, με προτεινόμενη την Επιλογή Α.

8.3.1 Επιλογή Α — Επιβεβαίωση μέσω Εφαρμογής Authenticator (προτεινόμενη)

Μετά την επιλογή «Continue» εμφανίζεται αυτόματα μια οθόνη ρύθμισης 2FA που περιέχει ένα QR Code. Κρατήστε ανοιχτή αυτή την οθόνη στον υπολογιστή σας και ακολουθήστε τα παρακάτω βήματα στο κινητό σας τηλέφωνο:

1. Εγκαταστήστε στο κινητό σας μία εφαρμογή Authenticator (π.χ. Google Authenticator, Microsoft Authenticator, Aegis, FreeOTP, 2FAS, Bitwarden Authenticator).

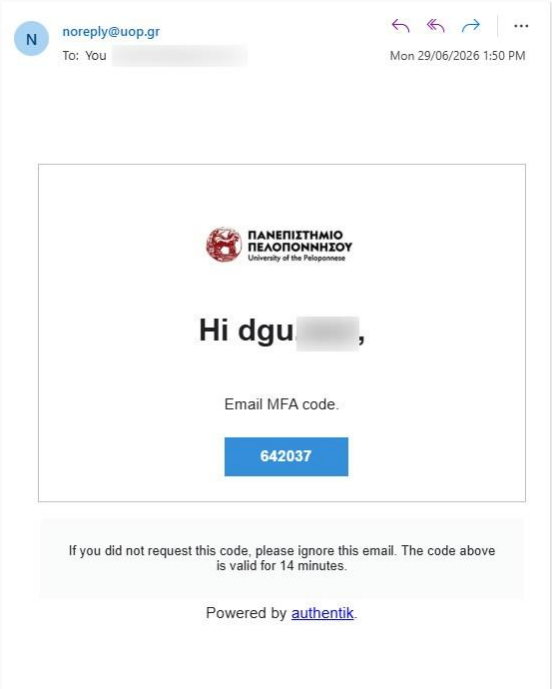
2. Συνδεθείτε με τον αντίστοιχο λογαριασμό σας στην εφαρμογή, εφόσον απαιτείται (π.χ. λογαριασμός Google ή Microsoft).
3. Σαρώστε το QR Code που εμφανίζεται στην οθόνη του υπολογιστή σας, χρησιμοποιώντας τη λειτουργία προσθήκης λογαριασμού της εφαρμογής.
4. Η εφαρμογή θα προσθέσει αυτόματα τον νέο λογαριασμό και θα αρχίσει να παράγει κωδικούς OTP που ανανεώνονται κάθε 30 δευτερόλεπτα.
5. Εισάγετε τον τρέχοντα 6ψήφιο κωδικό OTP στο πεδίο «TOTP Code» στην οθόνη του υπολογιστή σας και επιβεβαιώστε.

Αναλυτικός οδηγός σύνδεσης στο https://auth.uop.gr διατίθεται σε https://digital.uop.gr/2fa-authenticator

8.3.2 Επιλογή Β — Επιβεβαίωση μέσω E-mail

Εάν δεν επιθυμείτε τη λήψη κωδικού OTP μέσω κινητού, υπάρχει η εναλλακτική επιλογή λήψης κωδικού OTP στο προσωπικό σας e-mail.

1. Υποβάλετε σχετικό αίτημα μέσω της πλατφόρμας https://helpdesk.uop.gr/ προς τη Μονάδα Ψηφιακής Διακυβέρνησης.
2. Θα σας αποσταλούν οδηγίες ενεργοποίησης λήψης κωδικού OTP μέσω προσωπικού e-mail.
3. Μετά την ενεργοποίηση, σε κάθε σύνδεση μέσω Authentik θα εισάγετε τον κωδικό OTP που λαμβάνετε στο e-mail σας στο πεδίο «Authentication code».



Ενδεικτικό στιγμιότυπο λήψης OTP με e-mail.

8.4 Backup Codes και Ανάκτηση

Συνιστάται, εφόσον προσφέρεται από το σύστημα κατά τη ρύθμιση 2FA, να αποθηκεύσετε τους κωδικούς ανάκτησης (backup codes) σε ασφαλές, μη προσβάσιμο σε τρίτους μέρος (π.χ. password manager). Οι κωδικοί αυτοί χρησιμοποιούνται μόνο σε περίπτωση απώλειας πρόσβασης στη συσκευή σας Authenticator, και ο καθένας μπορεί να χρησιμοποιηθεί μία φορά.

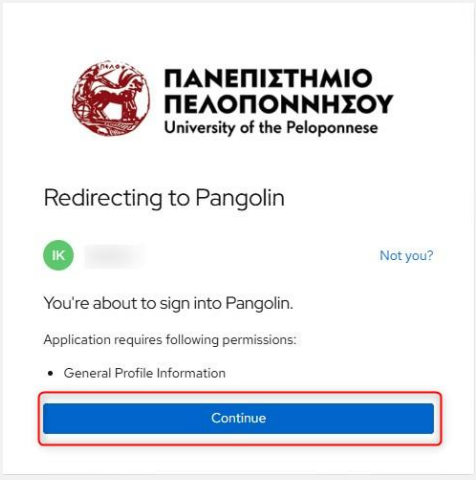
Σε περίπτωση απώλειας τόσο της συσκευής Authenticator όσο και των backup codes, ο χρήστης πρέπει να υποβάλει αίτημα στη Μονάδα Ψηφιακής Διακυβέρνησης μέσω https://helpdesk.uop.gr/ για επαναφορά της ρύθμισης 2FA, μετά από επιβεβαίωση ταυτότητας.

ΑΣΦΑΛΕΙΑ (SECURITY)

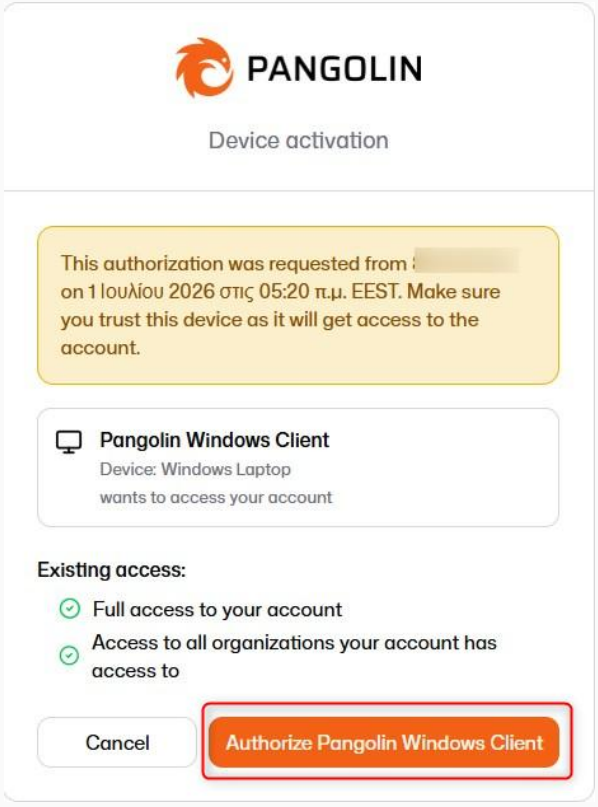
Μην αποθηκεύετε τους κωδικούς ανάκτησης σε απλό αρχείο κειμένου στην επιφάνεια εργασίας ή σε μη κρυπτογραφημένο σημείωμα. Προτιμήστε επαγγελματικό password manager.

8.5 Επιστροφή στο Pangolin και Σύνδεση

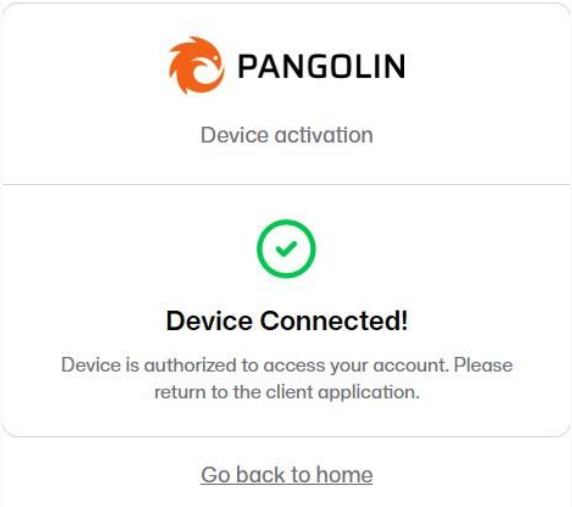
Μετά την επιτυχή ολοκλήρωση της πιστοποίησης (password + OTP), πατήστε το κουμπί Continue για να μεταφερθείτε πίσω στο Pangolin.



Εμφανίζεται το παράθυρο του Pangolin Client και κάνετε κλικ στο κουμπί '**Authorize Pangolin Windows Client**'



Παράθυρο Pangolin Client μετά την επιτυχή πιστοποίηση σε Authentik

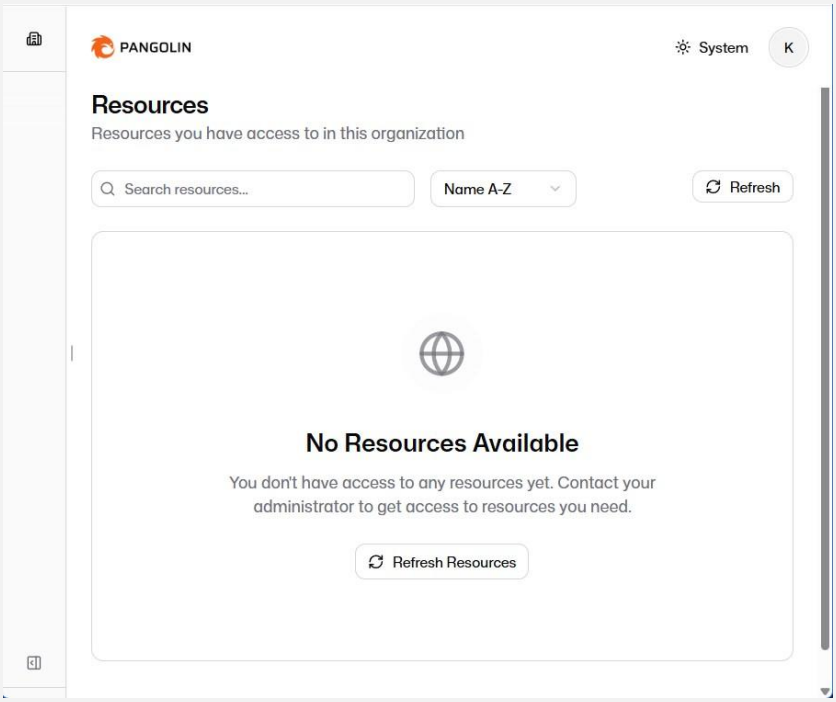


Παράθυρο Pangolin Client μετά κλικ στο κουμπί 'Authorize Pangolin Windows Client'

9. Καθημερινή Σύνδεση και Αποσύνδεση

9.1 Σύνδεση

Στις επόμενες χρήσεις, το πρόγραμμα Pangolin Client θυμάται τα στοιχεία ενεργοποίησης. Απλώς ανοίξτε το πρόγραμμα και πατήστε «Connect». Σε ορισμένες περιπτώσεις, ανάλογα με την πολιτική ασφαλείας, ενδέχεται να σας ζητηθεί εκ νέου ο κωδικός OTP.



Σελίδα επισκόπησης πόρων στους οποίους έχετε πρόσβαση

9.2 Αποσύνδεση

1. Όταν ολοκληρώσετε την εργασία σας, επιλέξτε «Αποσύνδεση / Disconnect» στο παράθυρο του Pangolin Client.

- Συστήνεται να αποσυνδέεστε πάντα όταν χρησιμοποιείτε κοινόχρηστο ή δημόσιο υπολογιστή.
- Σε προσωπική, αξιόπιστη συσκευή, μπορείτε να αφήσετε το πρόγραμμα συνδεδεμένο στο παρασκήνιο, εφόσον αυτό συνάδει με την πολιτική ασφαλείας του Ιδρύματος.

9.3 Session Timeout

Για λόγους ασφαλείας, οι συνεδρίες ταυτοποίησης λήγουν αυτόματα μετά από καθορισμένο χρονικό διάστημα αδράνειας ή μέγιστης διάρκειας. Σε περίπτωση λήξης (session timeout), θα χρειαστεί να επαναλάβετε τη διαδικασία σύνδεσης (password + OTP).

10. Πρόσβαση σε Linux Server μέσω SSH

Αφού ο Pangolin Client είναι συνδεδεμένος (ενεργό, πορτοκαλί εικονίδιο — βλ. ενότητα 9), ο εγκεκριμένος πόρος είναι προσβάσιμος μέσα από το ιδιωτικό δίκτυο του tunnel, χρησιμοποιώντας τη διεύθυνση IP (ή το εσωτερικό hostname) που σας έχει γνωστοποιηθεί κατά την έγκριση του αιτήματός σας (ενότητα 5.4).

10.1 Σύνδεση μέσω Τερματικού (Linux/macOS)

1. Βεβαιωθείτε ότι ο Pangolin Client είναι συνδεδεμένος.
2. Ανοίξτε το τερματικό (Terminal).
3. Εκτελέστε την εντολή: ssh <username>@<IP-ή-hostname-πόρου>, χρησιμοποιώντας το username λογαριασμού στον συγκεκριμένο server (όχι απαραίτητα το ιδρυματικό SSO username) και τη διεύθυνση που σας δόθηκε.
4. Κατά την πρώτη σύνδεση, ενδέχεται να εμφανιστεί προειδοποίηση επαλήθευσης αποτυπώματος (host key fingerprint) — επιβεβαιώστε με «yes», εφόσον αναγνωρίζετε τον πόρο.
5. Εισάγετε τον κωδικό πρόσβασης ή χρησιμοποιήστε το ιδιωτικό σας κλειδί SSH, ανάλογα με τη ρύθμιση πιστοποίησης του συγκεκριμένου server.

10.2 Σύνδεση μέσω Windows (PuTTY ή OpenSSH)

- Με το ενσωματωμένο OpenSSH client των Windows: ανοίξτε Command Prompt ή PowerShell και εκτελέστε ssh <username>@<IP-πόρου>, όπως στο Linux/macOS.
- Με το PuTTY: εισάγετε τη διεύθυνση IP/hostname στο πεδίο «Host Name», επιλέξτε θύρα 22 και τύπο σύνδεσης SSH, και πατήστε «Open».

10.3 Μεταφορά Αρχείων (File Transfer)

Για μεταφορά αρχείων προς/από τον Linux server μέσα από το ίδιο ασφαλές tunnel, μπορείτε να χρησιμοποιήσετε εργαλεία όπως scp, rsync ή sftp (γραμμή εντολών), ή γραφικά εργαλεία όπως το WinSCP ή το FileZilla (με πρωτόκολλο SFTP), στοχεύοντας στην ίδια διεύθυνση πόρου.

10.4 Logout και Λήξη Συνεδρίας

- Για έξοδο από τη συνεδρία SSH, πληκτρολογήστε exit ή πατήστε Ctrl+D.
- Η σύνδεση SSH είναι ανεξάρτητη από τη σύνδεση του Pangolin Client· το κλείσιμο της συνεδρίας SSH δεν αποσυνδέει αυτόματα το tunnel του Pangolin.
- Όταν ολοκληρώσετε όλη την εργασία σας, θυμηθείτε να αποσυνδέσετε και τον Pangolin Client (ενότητα 9.2), ιδίως σε κοινόχρηστη συσκευή.

10.5 Πολιτικές Ασφαλείας Συνεδρίας

ΑΣΦΑΛΕΙΑ (SECURITY)

Οι συνεδρίες SSH ενδέχεται να τερματίζονται αυτόματα μετά από παρατεταμένη αδράνεια, σύμφωνα με την πολιτική ασφαλείας του πόρου. Αποφεύγετε να αφήνετε ανοιχτές συνεδρίες SSH σε κοινόχρηστους υπολογιστές χωρίς επίβλεψη.

11. Πρόσβαση σε Windows Server μέσω Remote Desktop (RDP)

11.1 Σύνδεση από Windows

1. Βεβαιωθείτε ότι ο Pangolin Client είναι συνδεδεμένος.
2. Ανοίξτε την εφαρμογή «Σύνδεση Απομακρυσμένης Επιφάνειας Εργασίας» (Remote Desktop Connection, mstsc.exe).
3. Στο πεδίο «Υπολογιστής» εισάγετε τη διεύθυνση IP ή το hostname του Windows πόρου που σας έχει δοθεί.
4. Πατήστε «Σύνδεση» και, όταν ζητηθεί, εισάγετε το username και τον κωδικό πρόσβασης του λογαριασμού σας στον συγκεκριμένο server.
5. Αποδεχθείτε το πιστοποιητικό ασφαλείας, εφόσον εμφανιστεί σχετική προειδοποίηση (αναμενόμενο για εσωτερικούς servers χωρίς δημόσιο πιστοποιητικό).

11.2 Σύνδεση από macOS / Linux

Χρησιμοποιήστε την εφαρμογή Microsoft Remote Desktop (διαθέσιμη στο Mac App Store) ή εναλλακτικό RDP client (π.χ. Remmina σε Linux), εισάγοντας την ίδια διεύθυνση πόρου και τα διαπιστευτήρια του λογαριασμού σας στον server.

11.3 Ρυθμίσεις Συνεδρίας RDP

Ρύθμιση	Περιγραφή
Clipboard (Πρόχειρο)	Δυνατότητα αντιγραφής/επικόλλησης κειμένου μεταξύ τοπικού υπολογιστή και απομακρυσμένης συνεδρίας, εφόσον ενεργοποιηθεί στις τοπικές πόρους της σύνδεσης.
Drive Mapping (Χαρτογράφηση Δίσκων)	Δυνατότητα πρόσβασης σε τοπικούς φακέλους/δίσκους μέσα από την απομακρυσμένη συνεδρία, μέσω των ρυθμίσεων «Local Resources».
Ανάλυση Οθόνης (Screen Resolution)	Καθορίζεται στις ρυθμίσεις εμφάνισης (Display) πριν τη σύνδεση· συνιστάται προσαρμογή στην ανάλυση της τοπικής οθόνης για καλύτερη εμπειρία.
Disconnect	Διακοπή της απομακρυσμένης συνεδρίας χωρίς αποσύνδεση του χρήστη από τον server (η συνεδρία παραμένει ενεργή απομακρυσμένα).
Logout	Πλήρης αποσύνδεση του χρήστη από τον Windows server, με κλείσιμο όλων των ανοιχτών εφαρμογών της συνεδρίας.

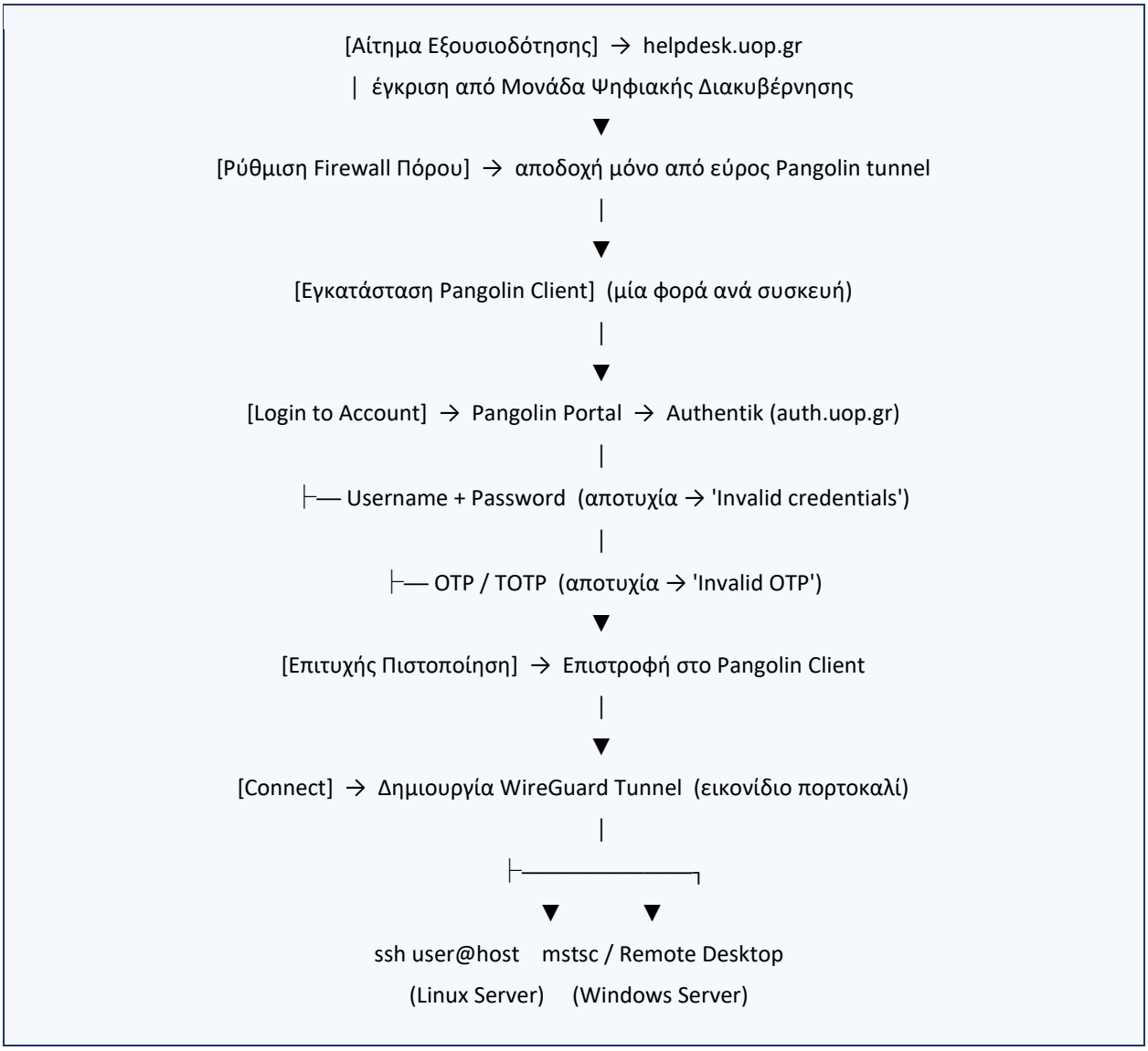
Ρύθμιση	Περιγραφή

ΠΡΟΣΟΧΗ (WARNING)

Η επιλογή «Disconnect» αφήνει τη συνεδρία ενεργή στον server (καταλαμβάνει πόρους). Σε servers με περιορισμένο αριθμό ταυτόχρονων συνεδριών, προτιμήστε πλήρες «Logout» όταν έχετε ολοκληρώσει την εργασία σας.

12. Διάγραμμα Ροής Πιστοποίησης και Πρόσβασης

Το παρακάτω διάγραμμα συνοψίζει το πλήρες σενάριο, από την υποβολή αιτήματος έως την ενεργή συνεδρία SSH/RDP:



Διάγραμμα 2 — Πλήρης ροή από το αίτημα εξουσιοδότησης έως την ενεργή απομακρυσμένη συνεδρία.

13. Πιθανά Σφάλματα και Επίλυση

Σφάλμα / Μήνυμα	Πιθανή Αιτία	Επίλυση
Invalid OTP / Wrong code	Λανθαρμένος ή ληγμένος κωδικός OTP, ή απόκλιση ρολογιού (clock drift) στη συσκευή.	Συγχρονίστε την ώρα της συσκευής σας αυτόματα μέσω δικτύου και δοκιμάστε ξανά με τον τρέχοντα κωδικό.
Wrong password	Λανθασμένος ιδρυματικός κωδικός πρόσβασης.	Επαληθεύστε τα στοιχεία σύνδεσης· αν έχετε ξεχάσει τον κωδικό, ακολουθήστε τη διαδικασία επαναφοράς ιδρυματικού λογαριασμού.
Expired session	Η συνεδρία ταυτοποίησης έληξε λόγω αδράνειας ή υπέρβασης μέγιστης διάρκειας.	Συνδεθείτε εκ νέου, επαναλαμβάνοντας password + OTP.
Unauthorized / 403	Δεν υπάρχει εγκεκριμένη εξουσιοδότηση πρόσβασης στον συγκεκριμένο πόρο.	Επιβεβαιώστε ότι το αίτημα εξουσιοδότησης (ενότητα 5) έχει εγκριθεί για τον συγκεκριμένο πόρο και χρήστη· επικοινωνήστε με τη Μονάδα Ψηφιακής Διακυβέρνησης.
Resource unavailable / 404	Λανθασμένη διεύθυνση πόρου, ή ο πόρος δεν είναι διαθέσιμος προς το παρόν.	Επιβεβαιώστε τη διεύθυνση IP/hostname από το e-mail έγκρισης· αν επιμένει, αναφέρετέ το μέσω ticket.
Connection timed out (SSH/RDP)	Ο Pangolin Client δεν είναι συνδεδεμένος, ή το firewall του πόρου δεν επιτρέπει ακόμη το εύρος του tunnel.	Επιβεβαιώστε ότι το εικονίδιο Pangolin Client είναι πορτοκαλί (ενεργή σύνδεση)· επικοινωνήστε με τον διαχειριστή του πόρου για επιβεβαίωση ρύθμισης firewall (ενότητα 6).
500 / Internal Server Error	Πρόσκαιρο πρόβλημα στην πλατφόρμα Pangolin ή Authentik.	Δοκιμάστε ξανά σε λίγα λεπτά· αν επιμένει, αναφέρετέ το στη Μονάδα Ψηφιακής Διακυβέρνησης.

Σφάλμα / Μήνυμα	Πιθανή Αιτία	Επίλυση
Client δεν εμφανίζει σύνδεση μετά το login	Καθυστέρηση δικτύου ή ανάγκη επανεκκίνησης του client.	Περιμένετε λίγα δευτερόλεπτα· αν δεν αποκατασταθεί, κλείστε και ανοίξτε εκ νέου τον Pangolin Client.

14. Καλές Πρακτικές Ασφαλείας

- Μην μοιράζεστε ποτέ τα στοιχεία ενεργοποίησης, τον κωδικό πρόσβασης ή τους κωδικούς OTP/backup με άλλα άτομα.
- Χρησιμοποιήστε ισχυρό, μοναδικό κωδικό πρόσβασης για τον ιδρυματικό σας λογαριασμό και αποφύγετε την επαναχρησιμοποίησή του σε άλλες υπηρεσίες.
- Χρησιμοποιήστε επαγγελματικό password manager για την ασφαλή αποθήκευση κωδικών και backup codes.
- Διατηρείτε τη συσκευή σας (κινητό με Authenticator, υπολογιστή με Pangolin Client) κλειδωμένη όταν δεν τη χρησιμοποιείτε (lock screen).
- Αποσυνδέεστε πάντα από κοινόχρηστους ή δημόσιους υπολογιστές μετά τη χρήση — τόσο από τη συνεδρία SSH/RDP όσο και από τον Pangolin Client.
- Μην εγκαθιστάτε τον Pangolin Client ή δεν αποθηκεύετε διαπιστευτήρια σε μη αξιόπιστες ή κοινόχρηστες συσκευές.
- Διατηρείτε ενημερωμένο το λειτουργικό σύστημα και το λογισμικό ασφαλείας (antivirus/firewall) της συσκευής σας.
- Αναφέρετε αμέσως στη Μονάδα Ψηφιακής Διακυβέρνησης τυχόν ύποπτη δραστηριότητα ή απώλεια/κλοπή συσκευής στην οποία είναι εγκατεστημένος ο Pangolin Client ή το Authenticator.
- Μην αφήνετε ανοιχτές, χωρίς επίβλεψη, ενεργές συνεδρίες SSH/RDP σε κοινόχρηστο χώρο.
- Χρησιμοποιήστε Key Pair Authentication και απενεργοποιήστε το Password Authentication στο SSH

ΚΑΛΗ ΠΡΑΚΤΙΚΗ (BEST PRACTICE)

Επανεξετάζετε περιοδικά (π.χ. κάθε εξάμηνο) τη λίστα πόρων στους οποίους έχετε ενεργή πρόσβαση και ζητήστε ανάκληση εξουσιοδοτήσεων που δεν χρειάζεστε πλέον, σύμφωνα με την αρχή του ελάχιστου απαιτούμενου δικαιώματος (principle of least privilege).

15. Συχνές Ερωτήσεις (FAQ)

1. Τι είναι το Pangolin και γιατί το χρησιμοποιεί το Πανεπιστήμιο;

Είναι η πλατφόρμα ασφαλούς απομακρυσμένης πρόσβασης που χρησιμοποιεί το Ίδρυμα ώστε οι εσωτερικοί servers να μην εκτίθενται απευθείας στο Internet, μέσω κρυπτογραφημένου WireGuard tunnel.

2. Χρειάζομαι VPN λογισμικό τρίτων για να χρησιμοποιήσω το Pangolin;

Όχι. Ο Pangolin Client είναι αυτόνομο πρόγραμμα που δημιουργεί το δικό του ασφαλές tunnel· δεν χρειάζεται επιπλέον VPN.

3. Πώς αποκτώ πρόσβαση σε έναν server;

Ο διαχειριστής του πόρου πρέπει να υποβάλει αίτημα στη Μονάδα Ψηφιακής Διακυβέρνησης μέσω helpdesk.uop.gr (ενότητα 5).

4. Μπορώ να ζητήσω εγώ ο ίδιος πρόσβαση χωρίς τον διαχειριστή του πόρου;

Η διαδικασία προβλέπει υποβολή του αιτήματος από τον διαχειριστή-υπεύθυνο του πόρου, ο οποίος εγκρίνει και τους χρήστες που θα έχουν πρόσβαση.

5. Πόσο χρόνο χρειάζεται η έγκριση ενός αιτήματος;

Ο χρόνος επεξεργασίας εξαρτάται από τη Μονάδα Ψηφιακής Διακυβέρνησης· θα ενημερωθείτε μέσω ticketing και e-mail.

6. Τι χρειάζομαι πριν εγκαταστήσω τον Pangolin Client;

Ενεργό ιδρυματικό λογαριασμό, εγκεκριμένο αίτημα πρόσβασης, σύνδεση στο Internet και εφαρμογή Authenticator στο κινητό σας.

7. Πού κατεβάζω τον Pangolin Client;

Από τον επίσημο σύνδεσμο λήψης https://pangolin.net/downloads, επιλέγοντας την έκδοση για το λειτουργικό σας σύστημα.

8. Χρειάζεται να εγκαθιστώ τον client σε κάθε νέο πόρο;

Όχι. Η εγκατάσταση γίνεται μία φορά ανά συσκευή· η πρόσβαση σε διαφορετικούς πόρους ελέγχεται από την εξουσιοδότηση, όχι από νέα εγκατάσταση.

9. Ποια διεύθυνση χρησιμοποιώ για την πύλη σύνδεσης;

https://pangolin.uop.gr/ — από εκεί γίνεται η ανακατεύθυνση στο Authentik για ταυτοποίηση.

10. Τι είναι το Authentik;

Ο πάροχος ταυτότητας (Identity Provider) του Ιδρύματος, που επαληθεύει το username/password και τον κωδικό OTP.

11. Ποια εφαρμογή Authenticator πρέπει να χρησιμοποιήσω;

Οποιαδήποτε συμβατή με TOTP εφαρμογή, π.χ. Google Authenticator, Microsoft Authenticator, Aegis, FreeOTP, 2FAS ή Bitwarden Authenticator.

12. Τι κάνω αν χάσω το κινητό μου με την εφαρμογή Authenticator;

Χρησιμοποιήστε τους backup codes, εφόσον τους έχετε αποθηκεύσει· διαφορετικά υποβάλετε αίτημα επαναφοράς 2FA στο helpdesk.uop.gr.

13. Μπορώ να λαμβάνω τον κωδικό OTP μέσω e-mail αντί για εφαρμογή κινητού;

Ναι, μέσω σχετικού αιτήματος στη Μονάδα Ψηφιακής Διακυβέρνησης (Επιλογή Β, ενότητα 8.3.2).

14. Γιατί προτιμάται η Επιλογή Α (εφαρμογή κινητού) έναντι του e-mail;

Η εφαρμογή Authenticator θεωρείται ασφαλέστερος δεύτερος παράγοντας, καθώς δεν εξαρτάται από την ασφάλεια του λογαριασμού e-mail.

15. Το username στο SSH/RDP είναι το ίδιο με το ιδρυματικό username SSO;

Όχι απαραίτητα· είναι το username λογαριασμού στον συγκεκριμένο server, το οποίο καθορίζεται από τον διαχειριστή του πόρου.

16. Γιατί λαμβάνω μήνυμα «Unauthorized» ή 403 όταν προσπαθώ να συνδεθώ;

Συνήθως σημαίνει ότι δεν υπάρχει ακόμη εγκεκριμένη εξουσιοδότηση για τον συγκεκριμένο πόρο/χρήστη. Ελέγξτε με τη Μονάδα Ψηφιακής Διακυβέρνησης.

17. Τι σημαίνει το πορτοκαλί χρώμα στο εικονίδιο του Pangolin Client;

Υποδεικνύει ότι η σύνδεση (tunnel) είναι ενεργή.

18. Μπορώ να συνδεθώ ταυτόχρονα σε πολλούς πόρους;

Ναι, εφόσον έχετε εξουσιοδότηση για περισσότερους από έναν πόρους, μπορείτε να ανοίξετε ξεχωριστές συνεδρίες SSH/RDP μέσα από το ίδιο ενεργό tunnel.

19. Χρειάζεται να είμαι συνδεδεμένος στο πανεπιστημιακό δίκτυο (Wi-Fi) για να χρησιμοποιήσω το Pangolin;

Όχι· το Pangolin λειτουργεί από οπουδήποτε υπάρχει πρόσβαση στο Internet.

20. Είναι ασφαλές να αφήνω τον Pangolin Client συνδεδεμένο στο παρασκήνιο;

Σε προσωπική, αξιόπιστη συσκευή είναι αποδεκτό· σε κοινόχρηστη συσκευή συνιστάται πάντα αποσύνδεση μετά τη χρήση.

21. Τι διαφορά έχει το «Disconnect» από το «Logout» σε RDP συνεδρία;

Το Disconnect αφήνει τη συνεδρία ενεργή στον server· το Logout την τερματίζει πλήρως.

22. Μπορώ να μεταφέρω αρχεία μέσω SSH;

Ναι, μέσω εργαλείων όπως scp, rsync, sftp ή γραφικών εφαρμογών SFTP (π.χ. WinSCP, FileZilla).

23. Μπορώ να χρησιμοποιήσω χαρτογράφηση τοπικών δίσκων (drive mapping) σε RDP συνεδρία;

Ναι, μέσω των ρυθμίσεων «Local Resources» στον RDP client σας, εφόσον επιτρέπεται από την πολιτική του πόρου.

24. Τι κάνω αν λάβω σφάλμα «Invalid OTP»;

Ελέγξτε ότι η ώρα της συσκευής σας είναι συγχρονισμένη αυτόματα και δοκιμάστε με τον τρέχοντα (μη ληγμένο) κωδικό.

25. Πόσο συχνά αλλάζει ο κωδικός OTP;

Συνήθως κάθε 30 δευτερόλεπτα, ανάλογα με τη ρύθμιση TOTP.

26. Πώς ζητάω ανάκληση πρόσβασης για έναν φοιτητή που αποχώρησε;

Ο επιβλέπων υποβάλλει ticket με θέμα «[PANGOLIN] Ανάκληση πρόσβασης – <username> – <όνομα πόρου» στο helpdesk.uop.gr.

27. Μπορεί να ανακληθεί η πρόσβασή μου χωρίς προειδοποίηση;

Ναι, σε περίπτωση παραβίασης πολιτικής ασφαλείας ή κατάχρησης πρόσβασης, το Τμήμα Πληροφορικής διατηρεί αυτό το δικαίωμα.

28. Τι κάνω αν ξεχάσω τον ιδρυματικό μου κωδικό πρόσβασης;

Ακολουθήστε τη διαδικασία επαναφοράς κωδικού του ιδρυματικού λογαριασμού SSO, ανεξάρτητα από το Pangolin.

29. Ποιον ενημερώνω αν υποψιάζομαι μη εξουσιοδοτημένη χρήση του λογαριασμού μου;

Επικοινωνήστε άμεσα με τη Μονάδα Ψηφιακής Διακυβέρνησης (ενότητα 18).

30. Λειτουργεί το Pangolin σε κινητό τηλέφωνο ή tablet;

Η χρήση του παρόντος οδηγού αφορά κύρια σε σταθερό/φορητό υπολογιστή· για κινητές συσκευές συμβουλευτείτε τη Μονάδα Ψηφιακής Διακυβέρνησης για διαθεσιμότητα αντίστοιχου client.

16. Γλωσσάρι Τεχνικών Όρων

Όρος	Επεξήγηση
Access Policy	Πολιτική που καθορίζει ποιοι χρήστες έχουν δικαίωμα πρόσβασης σε ποιους πόρους και υπό ποιες προϋποθέσεις.
Authentication	Διαδικασία επιβεβαίωσης της ταυτότητας ενός χρήστη (π.χ. μέσω password και OTP).
Authentik	Ο Identity Provider (IdP) που χρησιμοποιεί το Ίδρυμα για ταυτοποίηση χρηστών.
Authenticator App	Εφαρμογή κινητού που παράγει κωδικούς OTP/TOTP για δεύτερο παράγοντα πιστοποίησης.
Authorization	Διαδικασία ελέγχου αν ένας ταυτοποιημένος χρήστης έχει δικαίωμα πρόσβασης σε συγκεκριμένο πόρο.
Backup Codes	Εφεδρικοί κωδικοί μίας χρήσης που χρησιμοποιούνται για ανάκτηση πρόσβασης σε περίπτωση απώλειας της συσκευής 2FA.
Clipboard	Πρόχειρο αντιγραφής/επικόλλησης που μπορεί να μοιράζεται μεταξύ τοπικού υπολογιστή και απομακρυσμένης συνεδρίας.
Client (Pangolin Client)	Πρόγραμμα που εγκαθίσταται στη συσκευή του χρήστη και δημιουργεί το WireGuard tunnel.
Clock Drift	Απόκλιση του ρολογιού μιας συσκευής, που μπορεί να προκαλέσει αποτυχία επαλήθευσης κωδικού TOTP.
Credentials	Διαπιστευτήρια ταυτοποίησης (π.χ. username και password).
DNS (Domain Name System)	Σύστημα μετατροπής ονομάτων τομέα (π.χ. pangolin.uop.gr) σε διευθύνσεις IP.
Drive Mapping	Χαρτογράφηση τοπικών δίσκων ώστε να είναι προσβάσιμοι μέσα από απομακρυσμένη συνεδρία RDP.
Encryption	Κρυπτογράφηση· μετατροπή δεδομένων σε μη αναγνώσιμη μορφή χωρίς το κατάλληλο κλειδί αποκρυπτογράφησης.
Firewall	Λογισμικό ή συσκευή που ελέγχει και φιλτράρει την εισερχόμενη/εξερχόμενη κίνηση δικτύου βάσει κανόνων.
Firmware	Λογισμικό χαμηλού επιπέδου ενσωματωμένο σε συσκευή δικτύου (π.χ. router).

Όρος	Επεξήγηση
HOTP (HMAC-based One-Time Password)	Παραλλαγή OTP που βασίζεται σε μετρητή αντί για χρόνο.
Host Key	Κρυπτογραφικό κλειδί που ταυτοποιεί έναν SSH server· χρησιμοποιείται για επαλήθευση κατά την πρώτη σύνδεση.
HTTPS	Πρωτόκολλο HTTP με κρυπτογράφηση TLS/SSL, χρησιμοποιείται για ασφαλή πρόσβαση σε ιστοσελίδες.
Identity Provider (IdP)	Σύστημα που διαχειρίζεται και επαληθεύει ταυτότητες χρηστών (στην περίπτωσή μας, το Authentik).
Internal Network	Εσωτερικό δίκτυο του Ιδρύματος, μη απευθείας προσβάσιμο από το Internet.
IP Address	Αριθμητική διεύθυνση που προσδιορίζει μοναδικά μια συσκευή σε ένα δίκτυο.
Lock Screen	Λειτουργία κλειδώματος οθόνης μιας συσκευής όταν δεν χρησιμοποιείται.
MFA (Multi-Factor Authentication)	Πιστοποίηση πολλαπλών παραγόντων· συνδυασμός δύο ή περισσότερων ανεξάρτητων μεθόδων επιβεβαίωσης ταυτότητας.
OAuth2	Πρότυπο εξουσιοδότησης που επιτρέπει σε εφαρμογές να αποκτούν περιορισμένη πρόσβαση σε λογαριασμούς χρηστών.
OIDC (OpenID Connect)	Επέκταση του OAuth2 για ταυτοποίηση (authentication), βασισμένη σε JSON Web Tokens.
OTP (One-Time Password)	Κωδικός πρόσβασης μίας χρήσης, με περιορισμένη χρονική ισχύ.
Overlay Network	Εικονικό δίκτυο που δημιουργείται πάνω από ένα υπάρχον φυσικό δίκτυο (π.χ. μέσω WireGuard tunnel).
Pangolin	Η πλατφόρμα ασφαλούς απομακρυσμένης πρόσβασης που χρησιμοποιεί το Ίδρυμα.
Pangolin Portal	Σημείο εισόδου (pangolin.uop.gr) για την ενεργοποίηση λογαριασμού και τη δρομολόγηση προς το Authentik.
Password Manager	Εφαρμογή ασφαλούς αποθήκευσης και διαχείρισης κωδικών πρόσβασης.
Port (Θύρα)	Αριθμητικό σημείο επικοινωνίας σε μια διεύθυνση IP, π.χ. θύρα 22 για SSH, 3389 για RDP.

Όρος	Επεξήγηση
Provider	Στο πλαίσιο IdP, η οντότητα που παρέχει υπηρεσίες ταυτοποίησης (π.χ. Authentik).
Public Key / Private Key	Ζεύγος κρυπτογραφικών κλειδιών που χρησιμοποιείται π.χ. για πιστοποίηση SSH χωρίς κωδικό πρόσβασης.
QR Code	Δισδιάστατος γραμμωτός κώδικας που χρησιμοποιείται για γρήγορη μεταφορά δεδομένων ρύθμισης (π.χ. μυστικό TOTP) σε εφαρμογή κινητού.
RDP (Remote Desktop Protocol)	Πρωτόκολλο της Microsoft για απομακρυσμένη πρόσβαση σε γραφικό περιβάλλον Windows.
Resource (Πόρος)	Εσωτερικός server, VM ή υπηρεσία στην οποία παρέχεται εξουσιοδοτημένη πρόσβαση μέσω Pangolin.
RFC (Request for Comments)	Επίσημο έγγραφο τεχνικού προτύπου, π.χ. για πρωτόκολλα Internet.
Reverse Proxy	Διακομιστής που δέχεται αιτήματα εκ μέρους εσωτερικών servers και τα προωθεί σε αυτούς, αποκρύπτοντας τη δομή του εσωτερικού δικτύου.
SAML (Security Assertion Markup Language)	Πρότυπο ανταλλαγής δεδομένων ταυτοποίησης και εξουσιοδότησης μεταξύ IdP και εφαρμογών.
Session (Συνεδρία)	Χρονικό διάστημα κατά το οποίο ένας ταυτοποιημένος χρήστης παραμένει συνδεδεμένος σε ένα σύστημα.
Session Timeout	Αυτόματη λήξη συνεδρίας μετά από καθορισμένο χρόνο αδράνειας ή μέγιστης διάρκειας.
SFTP (SSH File Transfer Protocol)	Πρωτόκολλο ασφαλούς μεταφοράς αρχείων μέσω SSH.
Single Sign-On (SSO)	Μέθοδος ταυτοποίησης που επιτρέπει πρόσβαση σε πολλαπλές υπηρεσίες με ένα μόνο σύνολο διαπιστευτηρίων.
SSH (Secure Shell)	Πρωτόκολλο ασφαλούς απομακρυσμένης πρόσβασης σε γραμμή εντολών συστημάτων τύπου Linux/Unix.
TCP/IP	Βασική σουίτα πρωτοκόλλων επικοινωνίας δικτύων, στα οποία βασίζεται το Internet.

Όρος	Επεξήγηση
Terminal	Περιβάλλον γραμμής εντολών για αλληλεπίδραση με ένα λειτουργικό σύστημα.
Ticketing System	Σύστημα καταγραφής και διαχείρισης αιτημάτων υποστήριξης (helpdesk.uop.gr).
TLS/SSL	Πρωτόκολλα κρυπτογράφησης επικοινωνίας δικτύου, βάση του HTTPS.
TOTP (Time-based One-Time Password)	Παραλλαγή OTP που βασίζεται στον τρέχοντα χρόνο, ανανεώνεται συνήθως κάθε 30 δευτερόλεπτα.
Tunnel	Κρυπτογραφημένο ιδιωτικό κανάλι επικοινωνίας μεταξύ δύο σημείων μέσα από ένα μη έμπιστο δίκτυο (π.χ. το Internet).
Two-Factor Authentication (2FA)	Ειδική περίπτωση MFA με ακριβώς δύο παράγοντες πιστοποίησης.
Username	Όνομα χρήστη που ταυτοποιεί έναν λογαριασμό σε ένα σύστημα.
VM (Virtual Machine)	Εικονική μηχανή· λογισμικό που προσομοιώνει έναν ανεξάρτητο υπολογιστή πάνω σε φυσικό εξοπλισμό.
VPN (Virtual Private Network)	Ιδιωτικό εικονικό δίκτυο που δημιουργεί κρυπτογραφημένη σύνδεση πάνω από δημόσιο δίκτυο.
WireGuard	Σύγχρονο, ελαφρύ πρωτόκολλο VPN/tunnel με ισχυρή κρυπτογράφηση, στο οποίο βασίζεται το Pangolin.
Zero Trust	Μοντέλο ασφαλείας στο οποίο καμία σύνδεση δεν θεωρείται έμπιστη εξ ορισμού· απαιτείται ρητή ταυτοποίηση και εξουσιοδότηση για κάθε αίτημα πρόσβασης.

17. Παράρτημα Α — Συντομογραφίες και Πρότυπα Πιστοποίησης

17.1 Συντομογραφίες

Συντομογραφία	Πλήρης Όρος
2FA	Two-Factor Authentication
IdP	Identity Provider
IP	Internet Protocol
MFA	Multi-Factor Authentication
OIDC	OpenID Connect
OTP	One-Time Password
RDP	Remote Desktop Protocol
SAML	Security Assertion Markup Language
SFTP	SSH File Transfer Protocol
SSH	Secure Shell
SSO	Single Sign-On
TOTP	Time-based One-Time Password
VM	Virtual Machine
VPN	Virtual Private Network

17.2 Σχετικά Πρότυπα Πιστοποίησης

Πρότυπο	Σύντομη Περιγραφή
OAuth 2.0 (RFC 6749)	Πρότυπο εξουσιοδότησης που επιτρέπει σε εφαρμογές περιορισμένη πρόσβαση σε πόρους εκ μέρους χρήστη.
OpenID Connect (OIDC)	Επίπεδο ταυτοποίησης πάνω από το OAuth 2.0, χρησιμοποιείται από συστήματα IdP όπως το Authentik.
SAML 2.0	Πρότυπο XML-based για ανταλλαγή δηλώσεων ταυτοποίησης/εξουσιοδότησης μεταξύ IdP και υπηρεσιών.
TOTP (RFC 6238)	Πρότυπο παραγωγής κωδικών OTP βασισμένων στον χρόνο.

Πρότυπο	Σύντομη Περιγραφή
HOTP (RFC 4226)	Πρότυπο παραγωγής κωδικών OTP βασισμένων σε μετρητή.
WireGuard Protocol	Σύγχρονο πρωτόκολλο VPN με ενσωματωμένη ισχυρή κρυπτογράφηση, στο οποίο βασίζεται το Pangolin tunnel.

18. Επικοινωνία και Υποστήριξη

Για οποιοδήποτε πρόβλημα, απορία ή αίτημα σχετικό με την πρόσβαση μέσω Pangolin, επικοινωνήστε με τη Μονάδα Ψηφιακής Διακυβέρνησης:

Στοιχείο Επικοινωνίας	**Λεπτομέρειες**
Σύστημα Ticketing	https://helpdesk.uop.gr/
E-mail Υποστήριξης	dgu@uop.gr

ΣΗΜΕΙΩΣΗ (NOTE)

Για αιτήματα νέας πρόσβασης ή ανάκλησης πρόσβασης χρησιμοποιείτε πάντα το σύστημα ticketing (helpdesk.uop.gr) με τη μορφή θέματος που περιγράφεται στην ενότητα 5 — όχι τηλεφωνική ή προφορική επικοινωνία.