Single Sign-On

COMPLETE SYSTEM ADMIN AND SECURITY SUITE

One secure gateway to every network element

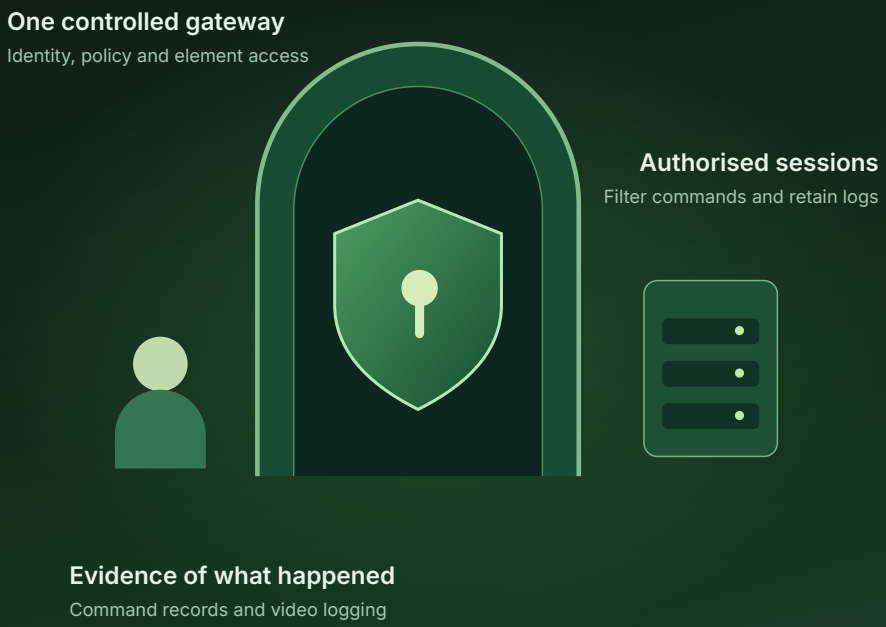
A Security Policy Manager and proxy server that control who reaches which element, with what commands, and record everything they do. Deployed at Mobilink.

LOGIN FLOW
3-way

SESSION TYPES
4

LOG TYPES
3

AND EXTERNAL DBS
LDAP



Security Policy Manager

Central policy for users and elements.

Security Proxy Server

Sessions pass through a controlled proxy.

Flexible authentication

Password, system-generated keys or RFID.

OPERATIONAL CONTEXT

A clearer way to work

A Security Policy Manager and proxy server that control who reaches which element, with what commands, and record everything they do. Deployed at Mobilink.

01

Shared passwords

Engineers log in directly with credentials that are hard to control.

02

No audit trail

It is difficult to prove who ran which command on which element.

03

Scattered administration

Access rights are managed separately on each system.

THE CHANGE IN DAILY OPERATIONS

Before	With SSO
– Direct element logins	✓ Proxy-controlled sessions
– Shared credentials	✓ Individual authentication
– No command restrictions	✓ Per-element filtering
– Partial logs	✓ Command and video logs
– Unrecorded vendor access	✓ Recorded, auditable access

AN OPERATIONAL SCENARIO

Control an engineering session

An engineer needs access to a network element. Administrators need to control the permitted commands and retain a record of the session.

One	Full	Per element	Video
Login point	Session audit	Access control	Session playback

CAPABILITIES 1

The capabilities that do the work

Explore the core functions of Single Sign-On and the operational tasks they support.

01

Security Policy Manager

Central policy for users and elements.

02

Security Proxy Server

Sessions pass through a controlled proxy.

03

Flexible authentication

Password, system-generated keys or RFID.

04

Command filtering

Per-element command and protocol filtering.

05

Video logging

Lossless differential PNG in HD, 256-colour or greyscale.

06

NMS integration

SNMP traps report events to your NMS.

DESIGNED AROUND THE USERS

Security Central policy and full audit.

Admins One place for access rights.

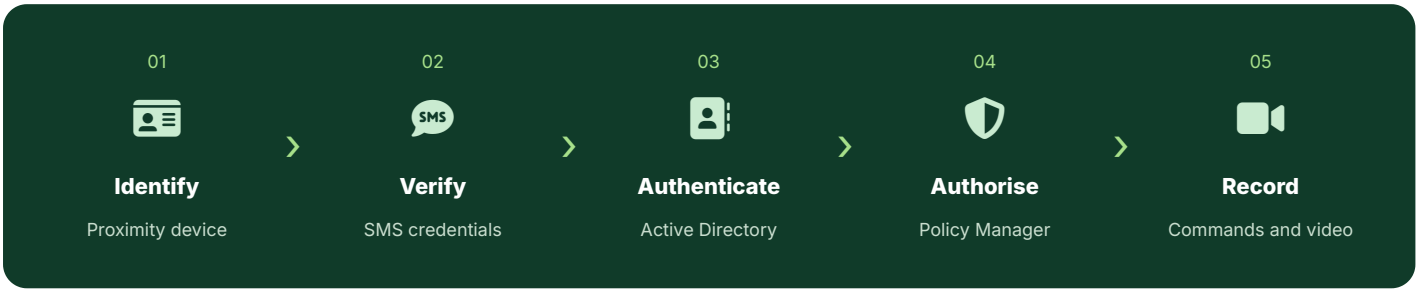
Engineers One login to permitted elements.

Vendors Controlled, recorded third-party access.

WORKFLOW

From the first step to the outcome

A connected sequence makes the handoffs and responsibilities easier to follow.



01 Log in
Users pass the configured authentication flow.

02 Check policy
The Policy Manager resolves allowed elements.

03 Open session
SSH, Telnet, FTP or GUI runs through the proxy.

04 Filter
Disallowed commands and protocols are blocked.

05 Audit
Commands, video and internal logs are retained.

A PRACTICAL WALKTHROUGH

Control an engineering session

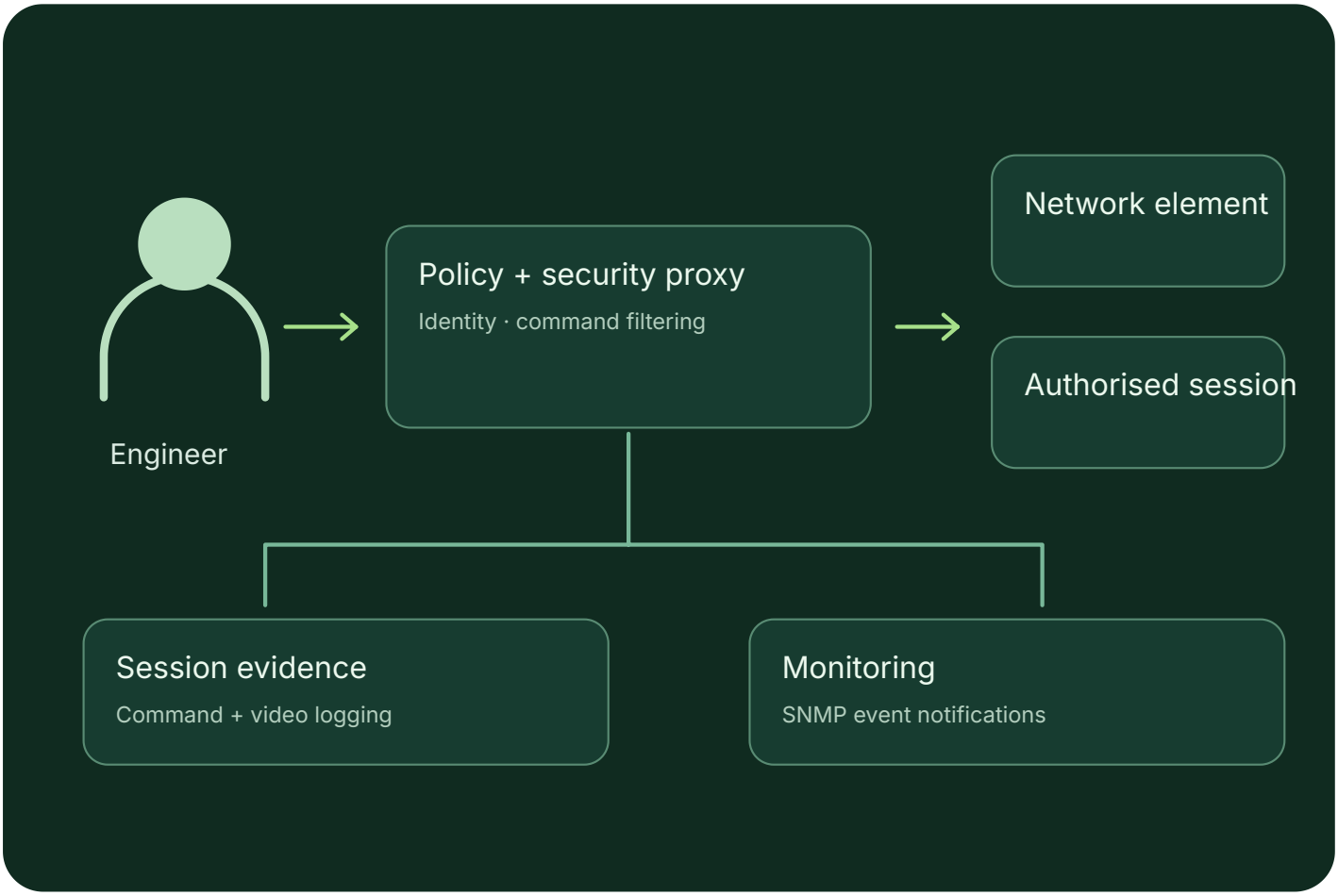
An engineer needs access to a network element. Administrators need to control the permitted commands and retain a record of the session.

Follow identity verification into policy-authorised proxy access. Review command filtering and session logging alongside the events passed to network monitoring.

ARCHITECTURE & HANDOFFS

A controlled route to network access

Identity checks and a security proxy sit between an engineer and the network element, with session evidence retained.



Conceptual product flow · Single Sign-On

01

Verify identity through the configured authentication flow.

02

Use policy and command filtering to control element access.

03

Retain session logs and notify network monitoring through SNMP traps.

DISCUSS YOUR ENVIRONMENT

Confirm the source systems, responsibilities and integration boundaries during the walkthrough. The diagram explains the product concept; the deployment scope is agreed for your environment.

TECHNOLOGY 1

Understand the connected pieces

Formats, protocols and tools in the product scope, with plain-language explanations for technical and business readers.

SSH
Encrypted remote command-line access.

Telnet
Legacy remote command-line access, still found on older equipment.

FTP
File transfer to and from network elements.

GUI
Sessions on graphical management applications.

LDAP
Standard protocol for user directories.

Oracle
Oracle enterprise database.

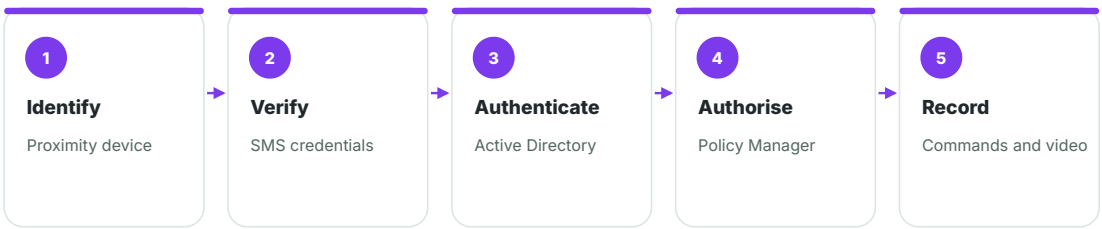
SQL Server
Microsoft relational database.

DB2
IBM enterprise database.

Sybase
SAP Sybase enterprise database.

RFID
Proximity cards or tags used to identify a user.

THE SSO OPERATING FLOW



INTEGRATION PLANNING

Agree the source systems, supported versions, data ownership and access requirements during discovery. Validate the relevant interfaces against your environment before production rollout.

SPECIFICATIONS 1

The scope in detail

Use these product details as the starting point for a technical discussion.

Area	Product scope
Authentication	Username/password, system-generated keys, RFID; three-way proximity, SMS and Active Directory flow
User stores	LDAP, internal database, or external Oracle, SQL Server, DB2 or Sybase
Session access	SSH, Telnet, FTP, GUI
Logging	Commands, video (lossless differential PNG), internal logs

ASSURANCE & NEXT STEPS

Prepare for a successful rollout

Match the product scope to your people, systems and operating requirements.

PRODUCT ASSURANCE

- **Three-way login**
- **Per-element command filtering**
- **Command and video logging**
- **SNMP traps to the NMS**

PLAN THE ENGAGEMENT

01

Discover

Review your current process, source systems, users and constraints. Identify the operational problem the first phase should solve.

02

Demonstrate

Follow identity verification into policy-authorised proxy access. Review command filtering and session logging alongside the events passed to network monitoring.

03

Validate

Agree the applicable product scope, access controls, integration checks and acceptance criteria. Confirm deployment and support responsibilities.

04

Handover

Plan user guidance, operational ownership and support contacts. Confirm the reporting cadence and review process for the agreed scope.

START A CONVERSATION

Explore SSO with our team.

Bring your operational scenario. We will walk through the relevant workflow and discuss a suitable scope.

info@excelerongroup.com

www.excelerongroup.com · Lahore, Pakistan