



// CASE STUDY

Consolidating Remote Access and File Transfer at a Large Electric Utility

Replacing remote access and file transfer tools with one secure OT platform.

Electric Utilities

Access & File Transfer Consolidation

2 Products, 1 Platform

// CHALLENGE

Two legacy products, one renewal deadline, and no room for risk

The utility is one of the largest electric utilities in the United States, serving millions of customers across its service territory. Its OT team manages the control systems that keep operations running — environments where every remote connection is a potential path from a compromised endpoint into critical infrastructure.

Remote access had evolved into two separate legacy products: one for remote sessions, another for file transfer. Each carried its own credentials, its own attack surface, and its own renewal cycle. When the renewal window approached, the team saw an opportunity to stop patching the status quo and consolidate onto a single platform built for OT.

The stakes were high enough that the purchase could not be a vendor-pitch decision. Before anything would be bought, the platform had to clear the utility's formal third-party risk assessment — a security review applied to any vendor touching operational systems.

// APPROACH

Lab-validated, risk-reviewed, and integrated with the directory the team already runs

Evaluation began where OT teams prefer to make decisions: in the lab. A hands-on technical session walked through the capabilities that mattered most — authentication, authorization, remote application

access, secure file transfer, full session recording, and central management. The decision to move forward then went through the utility's own gate: a formal third-party risk assessment the platform had to pass before purchase.

Deployment paired the Critical System Gateway with central management and federated identity directly with the utility's Active Directory. Directory groups matched into the platform mean permissions inherit automatically, so the team never maintains per-user access lists. Administrators verified permission behavior end to end before rollout, with high-availability protection for critical locations.

// PHASED ROLLOUT

From lab evaluation to quarterly business reviews

01 • EVALUATE

Hands-on lab validation and risk review

A technical lab session covered authentication, authorization, remote application access, file transfer, session recording, and central management — then the purchase cleared a formal third-party risk assessment.

03 • OPERATE

Positive adoption and quarterly reviews

The first production check-in confirmed successful implementation and positive user feedback, with minor issues triaged and quarterly business reviews established.

02 • DEPLOY

Production rollout with directory-integrated permissions

Gateway and management plane installed, Active Directory federated with group-synced permission inheritance, admin permissions verified end to end, and high availability in place for critical locations.

Why it matters: The utility bought on its own security standards — lab-validated and risk-reviewed — which is why the rollout produced adoption rather than friction.

We replaced two separate products with one platform, and the team's feedback since go-live has been positive — the directory integration means access works the way we already worked.

OT SECURITY LEAD, LARGE ELECTRIC UTILITY

// RESULTS

2 → 1

Two legacy products — remote access and file transfer — replaced by a single platform, with positive user feedback at the first production check-in

**Under
90
days**

From purchase decision to production rollout with directory integration, including the utility's own lab validation and formal third-party risk assessment

**100%
synced**

User permissions inherit automatically from matched Active Directory groups — no per-user access lists to build or maintain

**Risk-
approved**

Purchase cleared the utility's formal third-party risk assessment before a single production asset was touched

// WHY IT MATTERS

Utilities are consolidating access tools — and the file transfer piece is often forgotten

Large utilities run OT environments that grew tool by tool over decades: a VPN here, a remote-desktop product there, a separate file-transfer path somewhere else. Every tool is another set of credentials, another renewal, and another surface for attackers to probe. The consolidation mandate is spreading across the sector — one platform, one policy, one audit trail.

File transfer is the quiet half of the problem. Remote access platforms frequently leave it out, forcing utilities to keep a second legacy product alive just to move patches, backups, and configuration files. Xona's moderated file transfer — quarantine, scan, approval, and audit on every move — lets the same platform carry both workloads.

For utilities staring down their next renewal cycle, the question is not whether to consolidate but what the consolidated platform must prove: can it pass a real third-party risk assessment, integrate with the directory the team already runs, and be adopted without friction? Those were the exact gates this deployment had to clear.

// NEXT STEP

See consolidation work on your own systems

A guided evaluation stands up a gateway in under half an hour — no network re-architecture, no agents, and nothing to remove if you decide against it.

xonasystems.cominfo@xonasystems.com