

# UCOS<sup>®</sup>

## Remote Access Server

# UCOS Remote Access Server

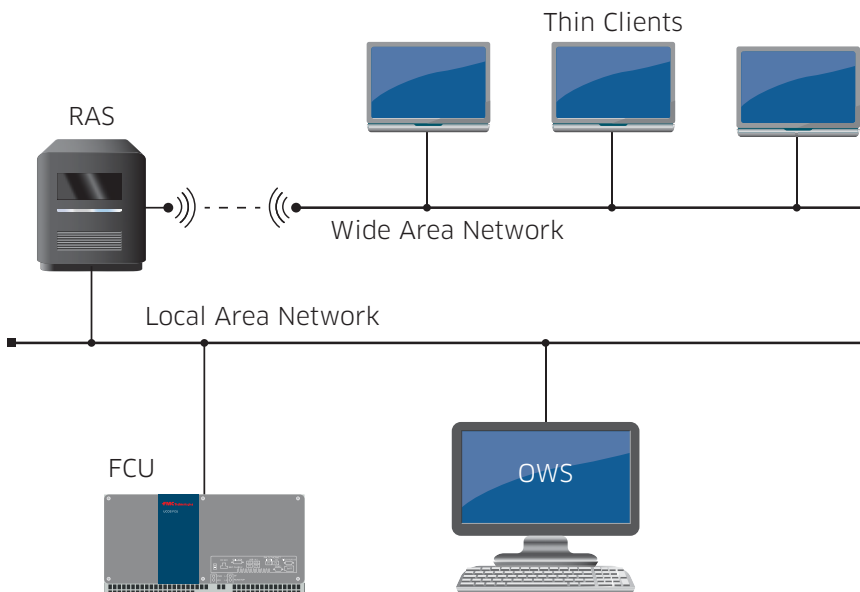
The UCOS Remote Access Server (RAS) supports secure, remote, browser-based access to a SCADA System. It can support varying numbers of remote users based on the capabilities of the underlying server. Remote users connect to the SCADA system using a browser and by providing a user name and password.

Connections to the RAS may be limited to view-only or may be given full operating capabilities.

Security may be defined to limit access by any and all remote users, or it may be configured on a per-user basis.

## The RAS features:

- Can be configured for view-only access
- Same graphics available on OWS & RAS
- Provides filtered controls data from a remote site over a public network



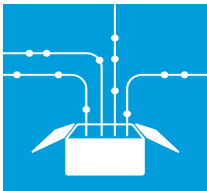
Using RAS to connect thin clients.

# Configuration | Connectivity | Security



## RAS Configuration

- Once Microsoft Terminal Services software is installed on a server, that server becomes a Terminal Server
- When UCOS OWS software is installed on the terminal server, it becomes a UCOS RAS
- The RAS is installed on the Local Area Network where it can quickly and easily interact with other key UCOS components such as the EWS or FCU



## Connectivity

- One or more thin clients can connect to the RAS simultaneously
- The RAS will establish a separate RDP session for each Thin Client
- The Microsoft Terminal Services settings control access for each thin client



## Security

- An authenticated thin client user may launch a UCOS runtime session
- Access to the UCOS Runtime Session is restricted using user credentials that can be linked to the Windows Authentication configuration
- Once a user gains Access to the UCOS Runtime Session that user can only Access functions defined within their Privilege profile
- Privilege profiles typically span from View Only to Full Access where users can send commands, change setpoints, acknowledge alarms, troubleshoot logic, etc.

## Licenses

A single tiered license must be purchased for the Terminal Server. The tiers are 5, 10, 25 and 50 Thin Clients. No licenses required for the Thin Clients.

**Example:** The 5 Thin Client Terminal Server UCOS license will allow a user to run up to 5 simultaneous RDP Sessions each running one UCOS Runtime Session.

# Access & Privilege Implications (Security)

1. **Access:** Secure access to the UCOS system is two tiered. (Both are responsibilities of Site IT)
  - a.) Tier 1: IT standards for secure access into the facility via FOB-based security access, VPN client access, etc.
  - b.) Tier 2: Security implications of how to access the UCOS network via Terminal Services.
2. **Privileges:** Once secure access has been gained, UCOS has configuration options that allow a finer granularity to permit/revoke access to screens, devices, commands, setpoints etc.
  - a.) Screen Access: Terminal Server is a great candidate for UCOS Workstation Profiles. With this feature, you can limit screen access to No access, Read-Only, and Full Access per security group. This also limits which alarms can be acknowledged from alarm viewer.
  - b.) Device Access: After creating one or more Remote Access security group within UCOS, Device Group Security can be configured to limit UCOS Device access per security group and/or user. If a user and/or a security group does not have access to certain UCOS Devices within that Device Group, those devices will NOT appear in screens and any Runtime application like Alarm Viewer, Trend, Device Diagnostics, etc.
  - c.) Control Access: After creating one or more Remote Access security group within UCOS, general Security Group specific profiles can be used to restrict access to commands and setpoints.

**Important Note:** If a user is required to access both the remote and local systems with no change to their privileges, no additional privilege configuration is necessary in UCOS as all security groups and users can be made accessible by all RDP Sessions from the Terminal Server.

## UCOS Runtime Session User Management

Each UCOS runtime session knows which user is logged in and which security group they belong to. This information is known to each runtime using local data. Scripts can run on the workstation to determine who is logged in which can then affect (update) FCU Global Data. This Global Data can then be read by other workstations and be used to execute their own scripts which enable pop-up warnings, automatic log outs, etc.

In general this means a UCOS system can be designed to design a project specific runtime session user management system (push/pull/lockout/warn/etc.) Who is logged in can also be displayed.

For example, a warning may appear stating “Wilson Jones has logged in remotely, you will automatically be logged out in 45 seconds”

# Definitions

**Access:** The ability of someone or something to access a restricted system (E.G. Locked Door or UCOS Runtime)

**Global Data (UCOS):** Data owned by an FCU (global as when a tag changes on an FCU it is propagated to all required workstations)

**Local Area Network (LAN):** A computer network that links devices within a building or group of adjacent buildings.

**Local Data (UCOS):** Data owned by a workstation (local as each workstation can have a different value)

**Microsoft Terminal Services:** Software that enables remote access

**OWS Thin Client Access Tier (UCOS):** A UCOS license which allowing a maximum number of Thin Clients to access UCOS any given time (Tiers: 5, 10, 25, 50).

**Privilege:** The ability of a user to manipulate a specific control variable within a system (E.G. Light switch in a room or specific valve command in UCOS)

**RDP Session:** A single exchange period hosted on a server by Windows and used by a thin client for remote monitoring and control

**Remote Access Server (UCOS):** A Terminal Server with UCOS installed and licensed with one of the OWS Thin Client access tiers below.

**Runtime Session (UCOS):** A single exchange period hosted on a workstation (or RDP session) by UCOS and used to monitor and control the UCOS Runtime system.

**Terminal Server:** A server running licensed Microsoft Terminal Services

**Thin Client:** A lightweight computer designed to remote into a server (only used as a portal and does not run UCOS software locally)

**Wide Area Network:** A computer network in which the computers connected may be far apart, generally having a radius of half a mile or more.

**Windows Authentication:** Functionality that ensures only users with necessary credentials can access key operating system components.



TechnipFMC  
UCOS products and services  
1 Sterling  
Irvine, CA 92618

UCOSSupport@FMCTI.com  
949-238-4195