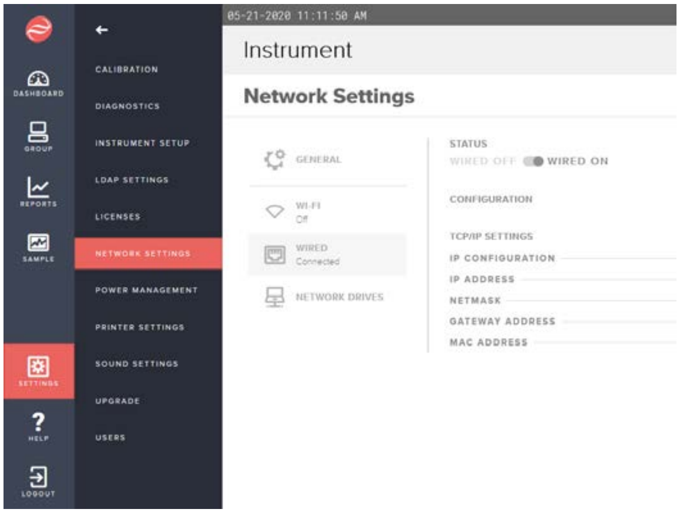
MET ONE 3400+ INFORMATION TECHNOLOGY IMPLEMENTATION GUIDE

This whitepaper explains how to implement the powerful integration technologies included in the MET ONE 3400+ within your information technology infrastructure.

The MET ONE 3400+ is designed to provide compliance confidence. Simplifying integration with your information technology infrastructure is key to achieving that goal. In this paper, the major integration features of the MET ONE 3400+ are described along with basic instructions on using these features.

Wired Connectivity

The MET ONE 3400+ is designed for easy wired networking for setup and when the wireless option wasn't purchased or when wireless infrastructure isn't available. The MET ONE 3400+ includes an 802.3 10/100 Ethernet port with auto negotiation and auto MDI/MDI-X for wired connectivity. The instrument defaults to DHCP, which means you can plug the instrument in to your network and it will self-configure with an IP address. Logging into the instrument as an Administrator, you can review this configuration via the Settings : Network Settings page.



05-21-2020 11:11:50 AM

Instrument

Network Settings

WI-FI Off

WIRED Connected

STATUS

WIRED OFF WIRED ON

CONFIGURATION

TCP/IP SETTINGS

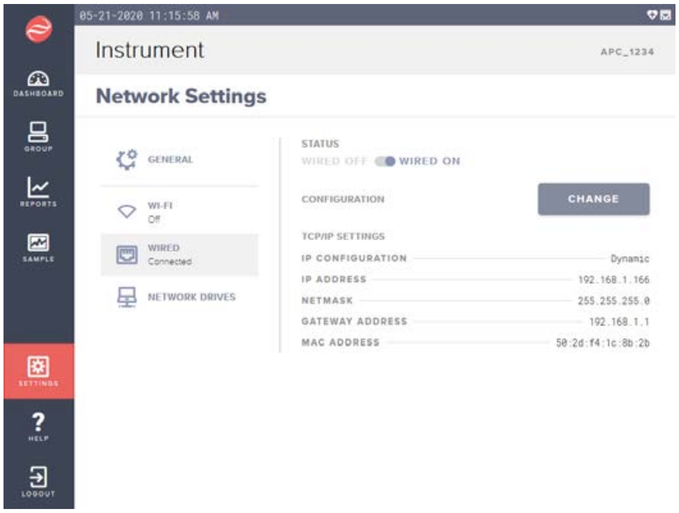
IP CONFIGURATION

IP ADDRESS

NETMASK

GATEWAY ADDRESS

MAC ADDRESS



05-21-2020 11:15:58 AM

Instrument APC_1234

Network Settings

WI-FI Off

WIRED Connected

STATUS

WIRED OFF WIRED ON

CONFIGURATION

TCP/IP SETTINGS

IP CONFIGURATION Dynamic

IP ADDRESS 192.168.1.166

NETMASK 255.255.255.0

GATEWAY ADDRESS 192.168.1.1

MAC ADDRESS 50:2d:f4:1c:8b:2b

From this page, you can select the WIRED option to review the status of the cabled Ethernet connection, see the assigned IP address, or manually configure IP V4 settings for the instrument, including IP address, netmask, and gateway. You can also see the encoded MAC address of the cabled interface if you need to configure your DHCP server or network security for a whitelisted or fixed MAC address.

Once you have the IP address, you can use an external web browser to control and configure the instrument. See the section on Web Browser in this paper for more details.

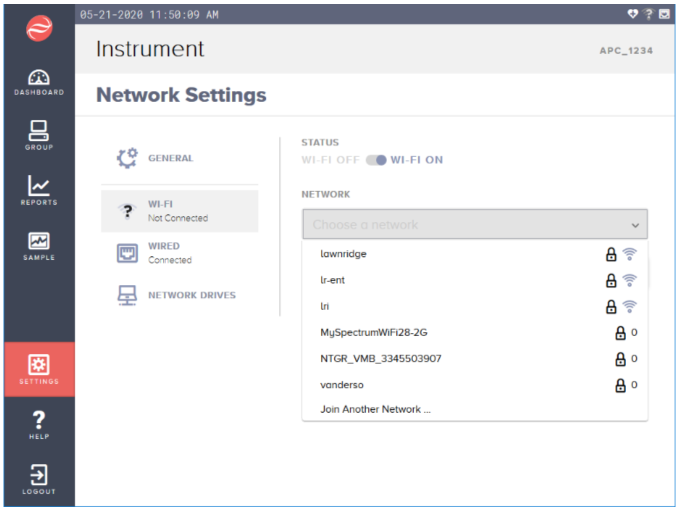
There is also an option here to disable the wired Ethernet port of the instrument. This can be helpful if you are configuring a wireless network only and want to prevent other outside access. The front panel interface will always be available to reconfigure this option.

Wireless Connectivity

The MET ONE 3400+ includes an optional 802.11b/g (Wi-Fi) wireless interface with full security capability, including 802.1x certificate-based authentication using WPA EAP (PEAP, TLS, and TTLS variants) and WPA2/PSK. Once the Wi-Fi is enabled, instruments scan for available networks and display them along with their signal strength. When you select a network, its security settings (PSK / EAP) will be automatically detected, and you will be prompted to select the correct variant and for the required credentials. Alternatively, you can enter the SSID manually using the "Join Another Network" prompt and you will be prompted to manually select the security settings and enter the required credentials.

All of the wireless setting below are configured by Administrators. Once you have successfully configured the instrument these setting will be retained for other users. The wireless adapter can be powered down via this screen to conserve power or fully secure the interface if it isn't used.

When selecting network security, the following options are available: Open Network, WPA2-PSK, WPA EAP PEAP, WPA EAP TLS, and WPA EAP TTLS. The WPA EAP options offer the best security and control over instruments that can access or monitor your network.



05-21-2020 11:50:09 AM

Instrument APC_1234

Network Settings

STATUS: WI-FI OFF / WI-FI ON

WI-FI: Not Connected

WIRED: Connected

NETWORK: Choose a network

lawnridge
lr-ent
lri
MySpectrumWiFi28-2G 0
NTGR_VMB_3345503907 0
vanderso 0
Join Another Network ...

Open Network

No credentials are required; the instrument will join the network. There is no encryption of any network traffic, so only higher-level protocols (HTTPS, TLS, etc.) will protect your data. Anyone in range can monitor traffic, spoof as an access point, or impersonate a server. Even with instrument MAC whitelisting or other security implementation, this is not recommended.

WPA2-PSK

The instrument will prompt for the Pre-Shared Key (PSK). This is an older form of Wi-Fi security where all devices are given the same key or password. Any device with the PSK can join the network or monitor traffic. While this provides more security than an open network, it isn't recommended for enterprise wireless. Changing the PSK credentials requires updating every wireless device on the network, so it doesn't happen, and control of the credential can be lost. If using PSK, always use a randomly generated key to avoid common dictionary attacks published on the Internet.

WPA EAP PEAP

The instrument will prompt for Password, Identity, optional CA Certificate file, and an optional Anonymous Identity. These will come from your wireless security system or RADIUS server. CA Certificates must be in the PEM format.

WPA EAP TLS

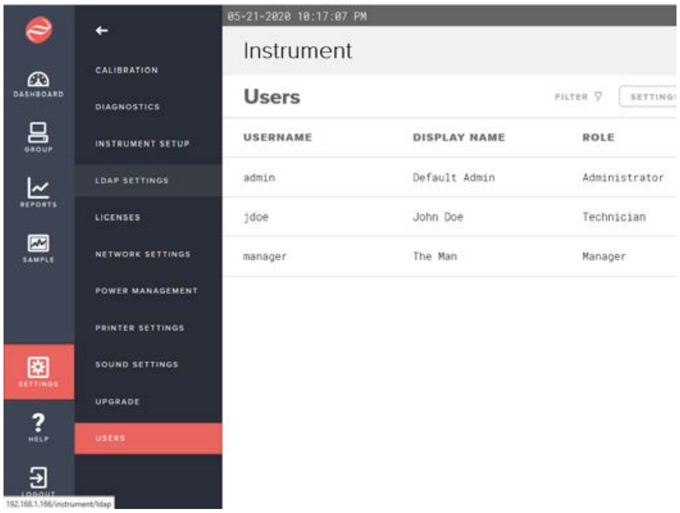
The instrument will prompt for Identity and Password. A Client Certificate and CA Certificate can be optionally added as well. The client certificate must be in the PFX format, while the CA certificate must be in the PEM format.

WPA EAP TTLS

The instrument will prompt for Password, Identity, optional CA Certificate file, and an optional Anonymous Identity. These will come from your wireless security system or RADIUS server. CA Certificates must be in the PEM format.

Configuring Users

The MET ONE 3400+ offers two ways of configuring and managing users. Users can be configured in a locally encrypted database, or the instrument can connect to your Windows Active Directory server via LDAP to authenticate using their Windows credentials.



USERNAME	DISPLAY NAME	ROLE
admin	Default Admin	Administrator
jdoe	John Doe	Technician
manager	The Man	Manager

User Groups and Privileges

Local or Active Directory users can be configured in three levels of access privileges: Administrators, Managers, and Technicians. Administrators have full control over the configuration of the instrument, users, and network capabilities and would typically be IT system administrators. Managers can configure, release, or archive the Electronic SOPs used to guide daily work. Technicians are locked to only executing the released SOPs and reporting the results of those samples; they can't change the SOP or instrument configuration.

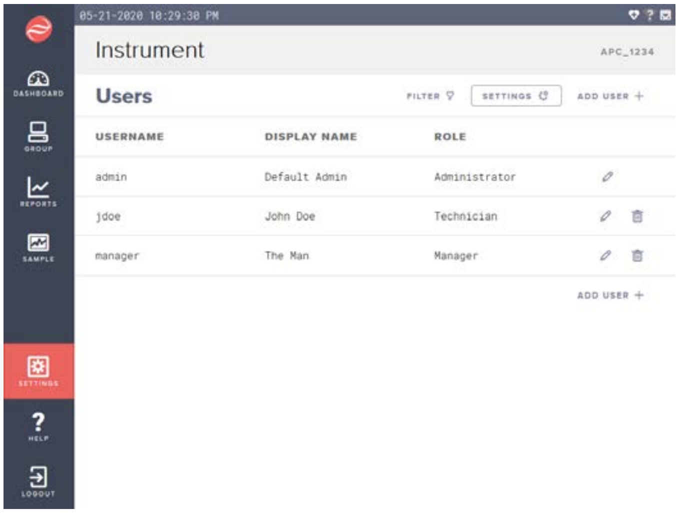
Local Users

Administrators can configure local users on the machine itself. These are stored in a secure, encrypted database in the instrument and include optional Beckman Coulter data integrity rules for password complexity and timeouts. The Beckman Coulter data integrity compliance rules include the following:

- Passwords expire after 90 days
- Passwords must be at least 10 characters in length
- Passwords must meet the following complexity requirements
    - One upper case alpha character
    - One lower case alpha character
    - One numeric value and a special character (i.e., !, @, #, $, %, ^, &)
- Passwords cannot be one of the last 10 most recent passwords
- After 5 failed login attempts the account will be locked for 30 minutes

Users can be added, edited, unlocked, or deleted from the Settings : Users screen. There is no practical limit to the number of users that can be configured in the instrument, so a search filter is provided to quickly locate a user of interest. The Settings gear on the Users screen is where Data Integrity Compliance rules can be turned on for local users.

When editing a user, the display name is set, along with the user name and their access privileges. The Administrator setting up the account will set a temporary password. When the new user logs in for the first time, they will be prompted to change their password.

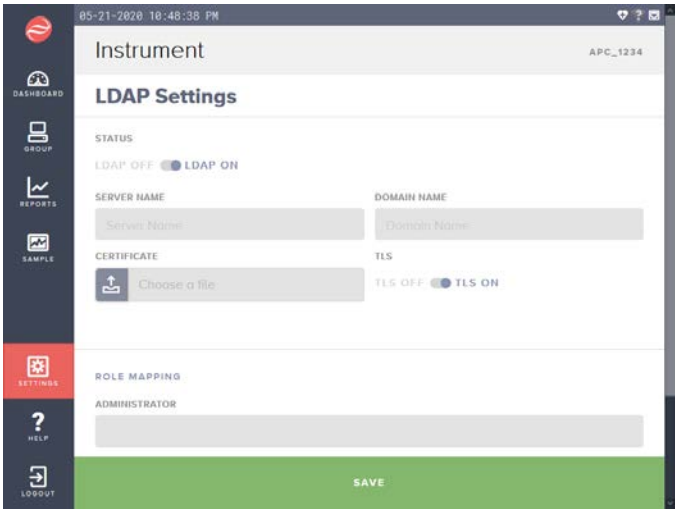


USERNAME	DISPLAY NAME	ROLE
admin	Default Admin	Administrator
jdoe	John Doe	Technician
manager	The Man	Manager

In the event you lose access to your Administrator accounts, Beckman Coulter can look up a one-day password to a specific instrument that will allow you to access the users page and reset the administrator password. This one-day password is randomly generated based on your instrument's serial number and date; there are no fixed backdoor passwords in the device.

When machines participate in a group, the database is replicated across the machines in the group, meaning user changes are updated in all the instruments when they connect to the network. See the Machine Groups and Data Replication section of this document for more details.

LDAP User Management



05-21-2020 10:48:38 PM

Instrument APC_1234

LDAP Settings

STATUS

LDAP OFF ● LDAP ON

SERVER NAME: Server Name

DOMAIN NAME: Domain Name

CERTIFICATE: Choose a file

TLS: TLS OFF ● TLS ON

ROLE MAPPING

ADMINISTRATOR

SAVE

LDAP (Lightweight Directory Access Protocol) or Active Directory is a protocol that allows users to be authenticated on a central server. This means your user credentials from your PC can be used on the MET ONE 3400+. User groups on your server control access and authority on the instrument. Password rules and user management is handled by the IT team running your servers. Instruments cache passwords for up to 1 week, so users only need to log in to the instrument while connected to the network periodically to keep LDAP settings up to date.

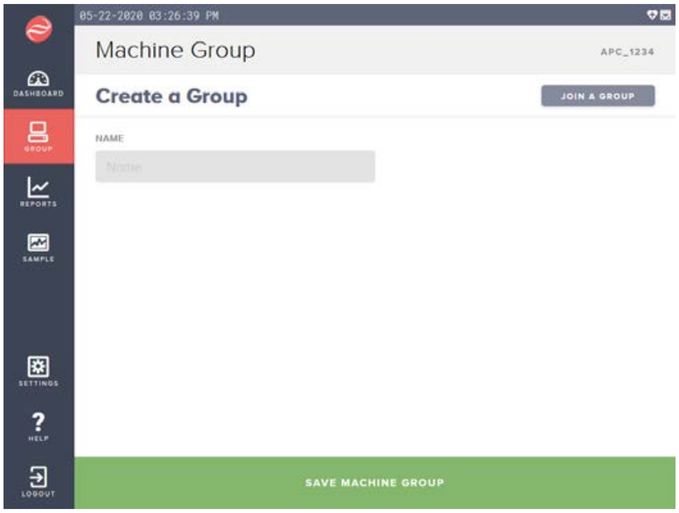
Once LDAP is turned on, you will be prompted for a Server Name and a Domain Name for your Active Directory server. Active Directory can be configured with or without TLS and a CER file is uploaded when TLS is configured.

Users should be placed into groups on your Active Directory server to manage their access to the MET ONE 3400+. At the bottom of the LDAP page, group names can be provided for the Administrator, Manager, and Technician levels. Only users in one of these three groups will be allowed to log in to the instrument.

Name Services

A hostname can be assigned to each particle counter to allow for easy management and network access using names instead of IP addresses which can change when using DHCP for IP address management. From the Settings : Network Settings page, simply enter the hostname for device being operated and click save. Once the hostname has been set, this can be used to connect to the instrument via the web browser or other network tools as needed.

Machine Groups and Data Replication



05-22-2020 03:26:39 PM

Machine Group APC_1234

Create a Group

JOIN A GROUP

NAME: Name

SAVE MACHINE GROUP

MET ONE 3400+'s can be assigned to become a member of a group of machines. When securely connected to a machine group, each MET ONE 3400+ will share user configuration, SOP configuration, and sample data to enable any machine in the group to have a complete view of the environmental monitoring status. A lightweight protocol connects the instruments to exchange uniquely identified true copies of data and to insure all instruments are in sync. Instruments self-form a dynamic hierarchy to allow the system to scale to hundreds of particle counters. The data replication scheme automatically checks for differences in the database. When changes are identified, the system will update to the most current versions of the configuration records. For sample data, the instruments will compare their databases and then share any new samples the instrument has taken. This process cascades throughout the instruments to insure all instruments have the most current view of the configuration and sampling campaign. When combined with Wi-Fi and a robust infrastructure, each technician can immediately see the state of the cleanroom sampling and take immediate action to complete monitoring before exiting the clean room.

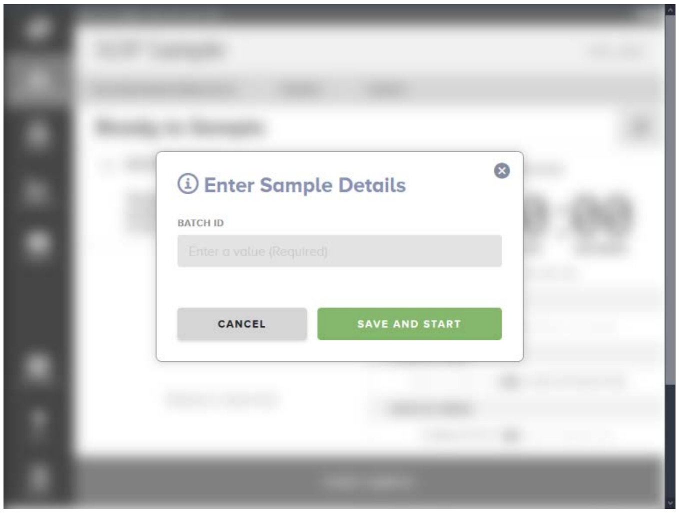
To set up a new instrument group, select a group name and configure it on the first instrument. Note the IP address of that instrument. For subsequent instruments to be joined to the group, just enter the IP address of the original machine. Once the instruments join the group, the IP address isn't used again, so the instruments can reconfigure via DHCP as needed.

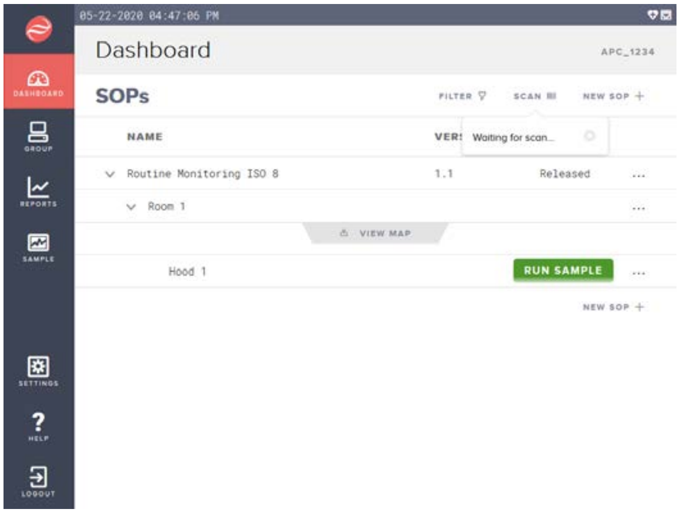
If an instrument leaves a group, all data for the audit trail, samples, and SOPs will be purged from that instrument, however if other instruments are still in the group, the data will be maintained in their databases. Only when the last instrument in a group is removed will the data be permanently lost. The instrument leaving the group will retain its local user database, including users copied from the group.

Data exchanges are performed in a TLS tunnel to prevent unauthorized snooping on the data, and only MET ONE 3400+ instruments are equipped with the credentials to access these groups. To enable Machine Group Data Replication across subnets, make sure ports X, Y, and Z are open for IP traffic.

Barcode Integration

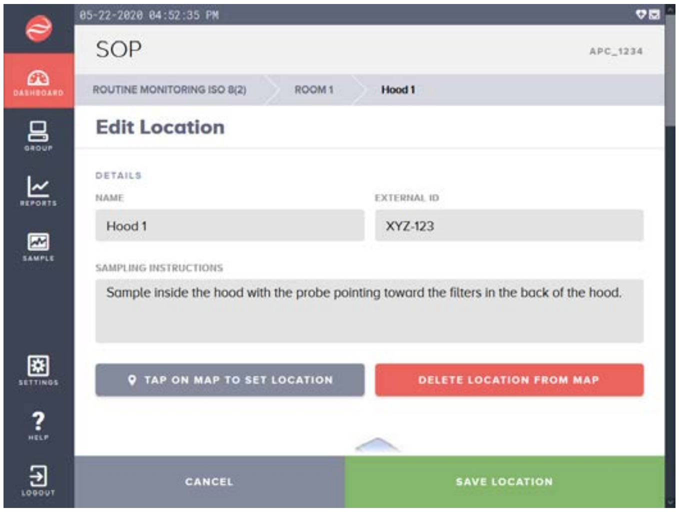
A USB barcode reader can be used to input characters into data entry fields in the instrument. This allows for error free transcription of any paper-based workflow into the electronic workflow of the MET ONE 3400+, including sample IDs, batch IDs, or other information your workflow needs captured with a sample. During SOP configuration, any number of user defined fields can be created and associated with locations. When sampling starts, those fields are requested of the technician, who can use a barcode scanner to accurately capture the required data.





Another feature allows a barcode to be associated with a location. A technician selects a mode to scan for that barcode when they arrive at the location. SOP sampling for that location can be started automatically to ensure technicians are visiting the correct locations.

During SOP setup, the barcode placed at each physical location can be scanned and associated with the location in the SOP. This gives you the flexibility to print or create your own strings of characters on the barcode. The External ID field is used to capture the barcode scan.



NAME: Hood 1

EXTERNAL ID: XYZ-123

SAMPLING INSTRUCTIONS: Sample inside the hood with the probe pointing toward the filters in the back of the hood.

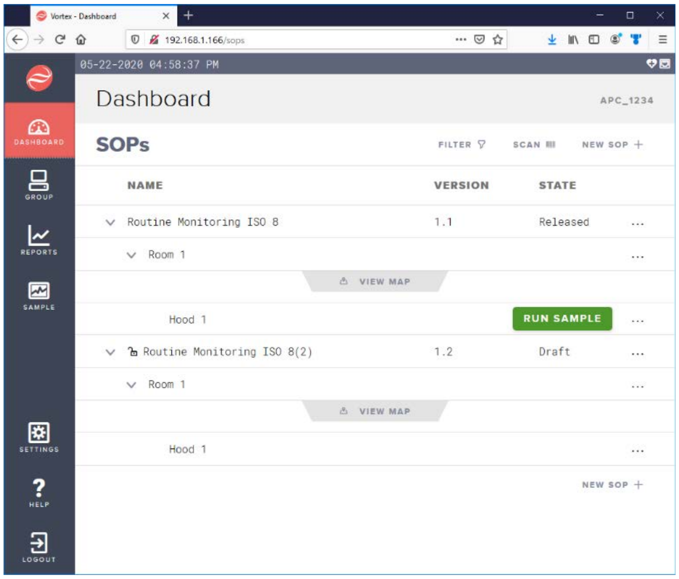
The barcode and reader can be any device which presents as a Human Interface Device (HID) or keyboard, so it is also possible to use 2-D, 3-D, or QR Codes in your workflow, if your reader can interpret the scan. RF-ID tags are also possible if your RF-ID tag reader has a close, selective range and presents the RF-ID code as a keyboard entry into the system.

The MET ONE 3400+ has been tested with several models of HID devices, but it will be up to the customer to validate the equipment they choose to use in their application.

Web Browser

The user interface on the instrument is fully available on any machine running a modern web browser (Chrome or Firefox). The experience is identical, so the web browser can be used for SOP configuration, user management, or training on a projector or big screen. At the conclusion of sampling, a web browser connected to one machine in the group used for monitoring can download all the data in a single, electronically signed report.

Alternatively, an instrument can be installed into a remote location and fully controlled for sampling via a remote web interface, allowing for central control or remote operation in areas where technicians are not permitted.



05-22-2020 04:58:37 PM

Dashboard

APC_1234

SOPs

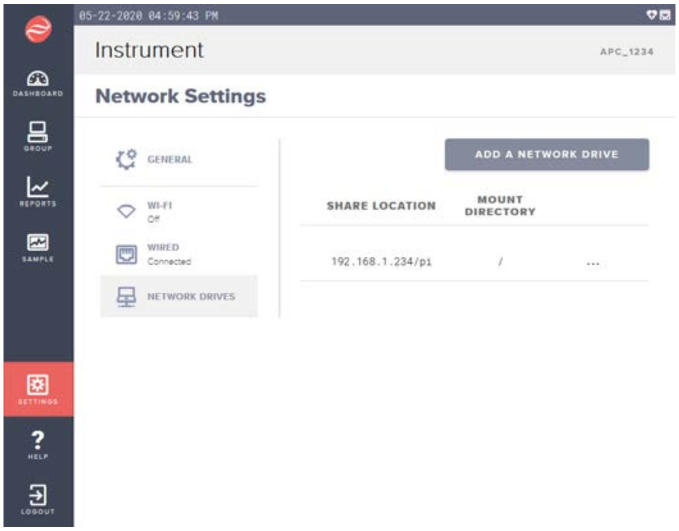
NAME	VERSION	STATE
Routine Monitoring ISO 8	1.1	Released
Room 1		
Hood 1		
Routine Monitoring ISO 8(2)	1.2	Draft
Room 1		
Hood 1		

To browse the instrument across subnets, make sure port X is open for IP traffic.

Network Shares

Within the MET ONE 3400+, Windows Network Shares can be configured to allow a technician to generate a report and upload it to that directory. Windows authentication controls rights and access to the share using tools already commonly deployed in most enterprises. Other reporting or configuration can be uploaded or downloaded to the shared directory straight from the instrument – no outside software or thumb drive required.

The standard Microsoft Windows networking ports (X, Y, Z) for file sharing should be open for sharing across subnets.



05-22-2020 04:59:43 PM

Instrument

APC_1234

Network Settings

WI-FI: Off

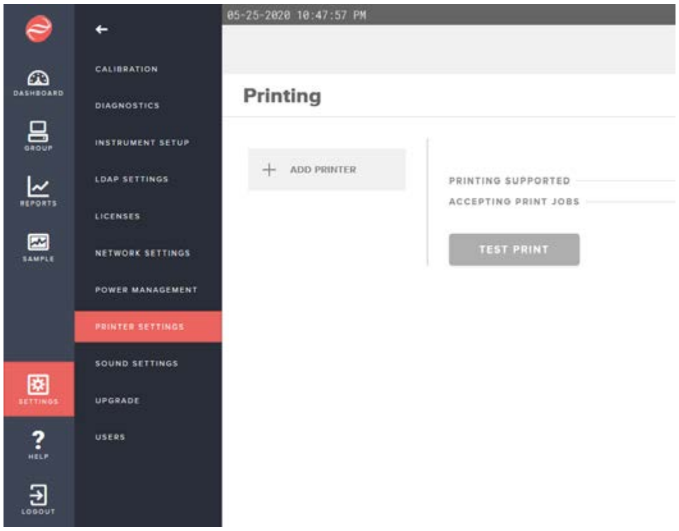
WIRED: Connected

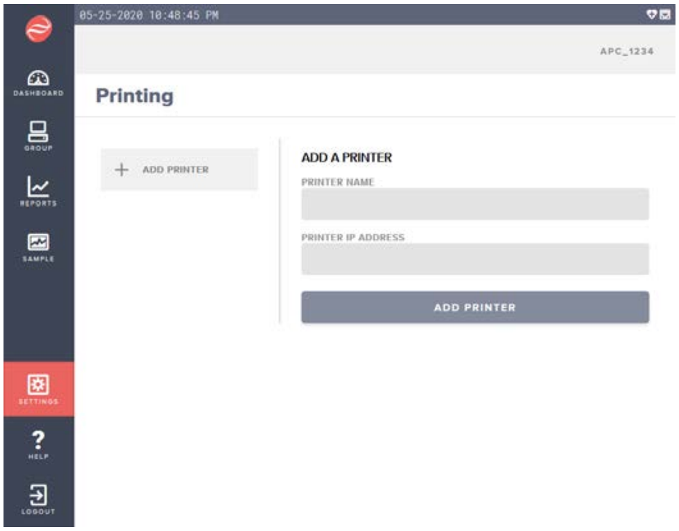
SHARE LOCATION	MOUNT DIRECTORY
192.168.1.234/pi	/

Network Printing

MET ONE 3400+ supports connectivity with external network based printers. For customers still using a paper based workflow, reports can now go directly to a printer, rather than using the internal thermal printer and scanning / photocopying. Tangible, long lasting results are available at the press of a button on the screen of the instrument. The MET ONE 3400+ uses Internet Printing Protocol to print to most compatible printers. Select the Settings : Printer Settings option to configure your printer. When the Add Printer button is selected, the instrument will prompt you for the printer name (to appear in the instrument) and its IP address.

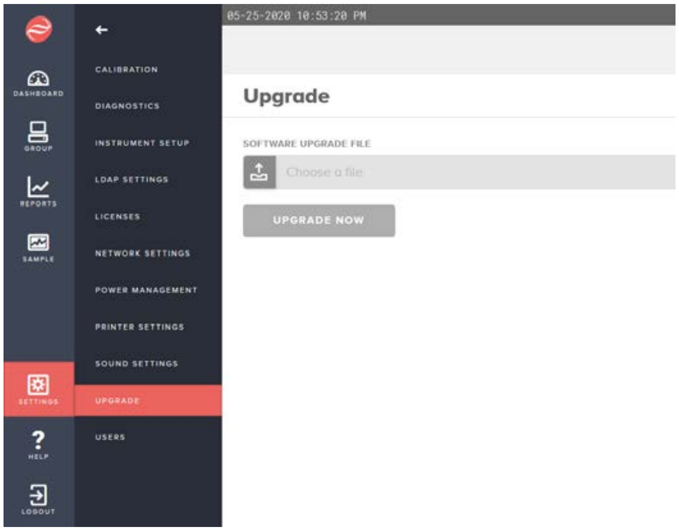
Network printing uses IP ports X, Y, and Z to connect to the printer.





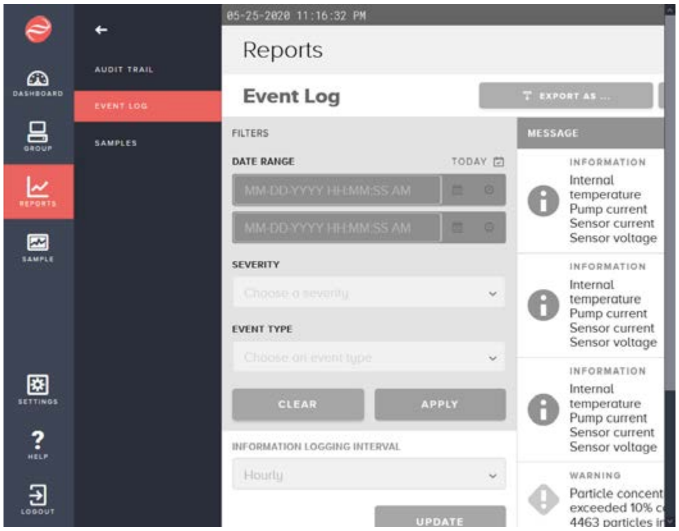
Firmware Upgrades

The software and operating system can be upgraded as necessary to add features and receive the latest updates. Upgrade files can be procured from Beckman or your local authorized representative and then uploaded to the MET ONE 3400+ via a USB thumb drive or through the web browser on your desktop. Only Administrator users can perform an instrument firmware upgrade. Browse to the instrument to Settings : Upgrade, select the upgrade file from your desktop, then kick off the upgrade. After processing the upgrade file, the instrument is back online with the new software version. Only files digitally signed by Beckman will be processed. Always review the release notes of any software upgrade to understand its impact on existing configuration data, machine groups, new features, and your verification and validation system.



Internal Logs

Internal operating parameters are periodically logged in the instrument to aid in troubleshooting intermittent failures. These logs can be reviewed by Beckman authorized service personnel to help quickly resolve any hardware issues or to provide training on best practices for operating the instrument to avoid any problems. Navigate to the Reports : Event Log screen. From here a report of the log can be exported, filtered by date, severity, or event type. The instrument will default to only capturing informational events once per week, but in the event of intermittent operating errors not otherwise captured in the logs, the Information Logging Interval can be set to daily or hourly. An Administrator can delete the log as needed.



05-25-2020 11:16:32 PM

Reports

Event Log

FILTERS

DATE RANGE TODAY

MM-DD-YYYY HH:MM:SS AM

MM-DD-YYYY HH:MM:SS AM

SEVERITY

Choose a severity

EVENT TYPE

Choose an event type

INFORMATION LOGGING INTERVAL

Hourly

MESSAGE

INFORMATION
Internal temperature
Pump current
Sensor current
Sensor voltage

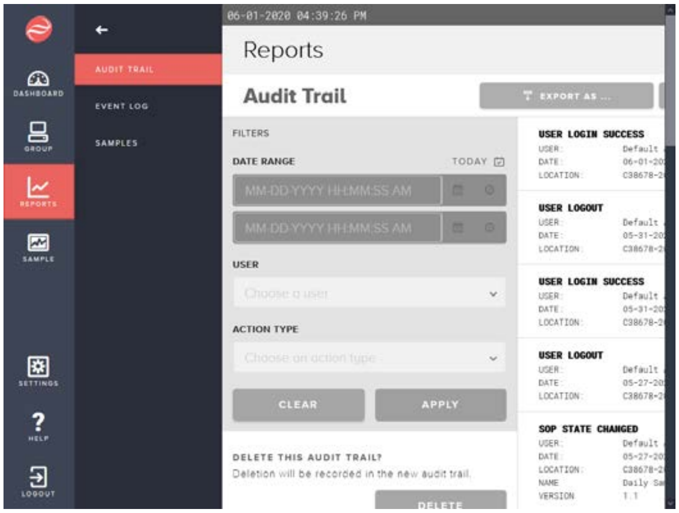
INFORMATION
Internal temperature
Pump current
Sensor current
Sensor voltage

INFORMATION
Internal temperature
Pump current
Sensor current
Sensor voltage

WARNING
Particle concent
exceeded 10% c
4463 particles ir

Audit Trail

A GMP grade audit trail is included in the instrument, including information on logins, logouts, power events, sampling, electronic signatures, SOP updates, and other critical actions taken on the instrument. The audit trail is available from Reports : Audit Trail. The audit trail has search and filtering capabilities allowing you to quickly zero in on the dates and types of audit events and users involved. The audit trail is shared across all instruments in a machine group, allowing a single portal view to the audit trail of your entire instrument fleet. Audit trail reports are electronically signed and can then be printed or exported to your desktop when browsing to the instrument, or to a network share or USB thumb drive.



06-01-2020 04:39:26 PM

Reports

Audit Trail

FILTERS

DATE RANGE TODAY

MM-DD-YYYY HH:MM:SS AM

MM-DD-YYYY HH:MM:SS AM

USER

Choose a user

ACTION TYPE

Choose an action type

DELETE THIS AUDIT TRAIL?
Deletion will be recorded in the new audit trail.

USER LOGIN SUCCESS
USER: Default
DATE: 06-01-20
LOCATION: C38678-2

USER LOGOUT
USER: Default
DATE: 05-31-20
LOCATION: C38678-2

USER LOGIN SUCCESS
USER: Default
DATE: 05-31-20
LOCATION: C38678-2

USER LOGOUT
USER: Default
DATE: 05-27-20
LOCATION: C38678-2

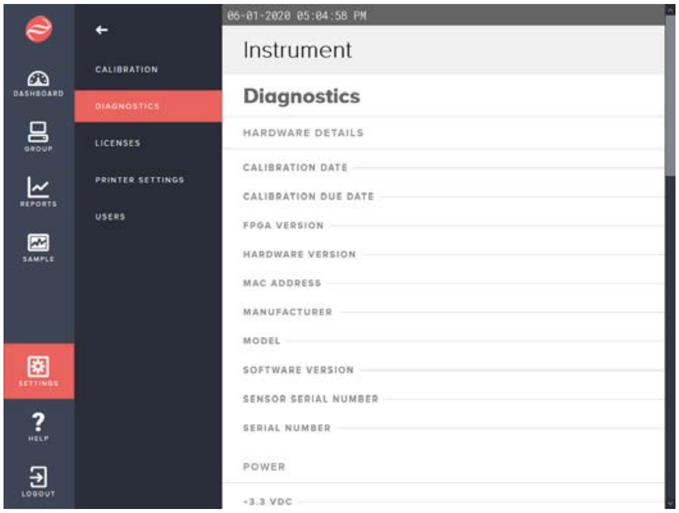
SOP STATE CHANGED
USER: Default
DATE: 05-27-20
LOCATION: C38678-2
NAME: Daily Sa
VERSION: 1.1

Only Administrator level users will be presented with an option to delete the audit trail. The deletion will be recorded in the new audit trail with the date, time, and user name of the user with Administrator privileges.

Internal Database Management

The database used to manage sample data and instrument configuration is internally managed and requires no external intervention or maintenance. From the Settings : Diagnostics page, database file system utilization can be monitored. If the database is filling, an administrator can export and delete samples.

By utilizing the machine group function, any spare device can serve as a full system backup and can even be located off site for disaster recovery purposes. Any new device can be joined to the machine group and will replicate the samples, SOPs, and users from the backup instrument.



06-01-2020 05:04:58 PM

Instrument

Diagnostics

HARDWARE DETAILS

CALIBRATION DATE

CALIBRATION DUE DATE

FPGA VERSION

HARDWARE VERSION

MAC ADDRESS

MANUFACTURER

MODEL

SOFTWARE VERSION

SENSOR SERIAL NUMBER

SERIAL NUMBER

POWER

+3.3 VDC