Honeywell

Experion PKS

Experion Mobile Access User's Guide

EPDOC-XX72-en-431A
February 2015

Release 431

Document	Release	Issue	Date
EPDOC-XX72-en-431A	431	0	February 2015

Disclaimer

This document contains Honeywell proprietary information. Information contained herein is to be used solely for the purpose submitted, and no part of this document or its contents shall be reproduced, published, or disclosed to a third party without the express permission of Honeywell International Sàrl.

While this information is presented in good faith and believed to be accurate, Honeywell disclaims the implied warranties of merchantability and fitness for a purpose and makes no express warranties except as may be stated in its written agreement with and for its customer.

In no event is Honeywell liable to anyone for any direct, special, or consequential damages. The information and specifications in this document are subject to change without notice.

Contents

About this guide

This guide is intended primarily for engineers and system administrators who are responsible for installing, configuring, and supporting Experion Mobile Access.

It describes:

- Planning considerations
- Considerations for ensuring the security of your Experion Mobile Access system
- Installation procedures, including how to uninstall
- Mandatory and optional configuration procedures
- Operating instructions
- Management procedures
- Troubleshooting

Revision history

Revision	Date	Description
A	February 2015	Initial release of document.

About Experion Mobile Access

Experion Mobile Access enables mobile users to access key process data and alarms on a web browser, optimized for smaller handheld devices. The data routing between the handheld device and the Experion eServer is managed by Honeywell OneWireless^{TM} Network.

With Experion Mobile Access, operators and field technicians can use handheld computers, such as the Dolphin® 99EX, to view Experion process data, alarms, and trends, and if enabled, to control what is happening, while they are outside of the control room.

Experion Mobile Access is qualified for the following point types:

- CDA
- TPS
- SCADA

Experion Mobile Access can be used to:

- View alarm groups within the operator's scope of responsibility.
- View alarms for points within the operator's scope of responsibility.
- Modify and acknowledge alarms, if enabled, for points within the operator's scope of responsibility.
- View history for a point and, if supported by the mobile device, see live updates to history.
- View a list of alarms, known as the alarm dashboard.

Online help is available for each Experion Mobile Access display.

Because Experion Mobile Access is designed to complement rather than replace Station, it does not provide full Station functionality. For example:

- Experion Mobile Access provides text-based information and does not support custom displays.
- Operators cannot change their Experion password using Experion Mobile Access. This needs to be done on eServer.
- If you use Electronic Signatures, you cannot modify points with Experion Mobile Access.
- You can only acknowledge an alarm from the point's faceplate.
- Alerts are not supported in Experion Mobile Access.

For a visual comparison of Station versus Experion Mobile Access, see the "Experion Mobile Access vs. Station faceplates" topic.

As soon as you install Experion Mobile Access it is ready to use. However, by following the recommendations and guidelines in this document you can make it easier for operators and field technicians to access Experion data, alarms, and trends.

Experion Mobile Access supports internationalization/localization.

Related topics

"Experion Mobile Access vs. Station faceplates" on page 53

Planning for Experion Mobile Access

Honeywell recommends Experion Mobile Access be installed on a dedicated eServer node. That node can connect to any node with a release supported by DSA interoperability.

For more information on interoperability, refer to the Experion eServer Specification, available for download from the Honeywell Process Solutions Web site (http://www.honeywellprocess.com).

- Configuration of Experion Mobile Access is the same as configuration of eServer. For more information, see the “eServer” topic in the “Configuring the DMZ firewall” section of the *Network and Security Planning Guide*.
- Experion Mobile Access is supported with the OneWireless network.
- Honeywell recommends using the Honeywell-supported OneWireless and Dolphin® devices: Dolphin 9900ni and Dolphin 99EX.

Attention

It is very important that, when preparing your Experion network, including preparing for OneWireless, you read the ‘Network Planning’ topic in the *Network and Security Planning Guide*.

Security considerations for Experion Mobile Access

Related topics

"Experion Mobile Access topology" on page 12
"Security best practice for handheld devices" on page 13

Experion Mobile Access topology

The topology diagram below shows the recommended configuration of Experion Mobile Access on the Experion network.

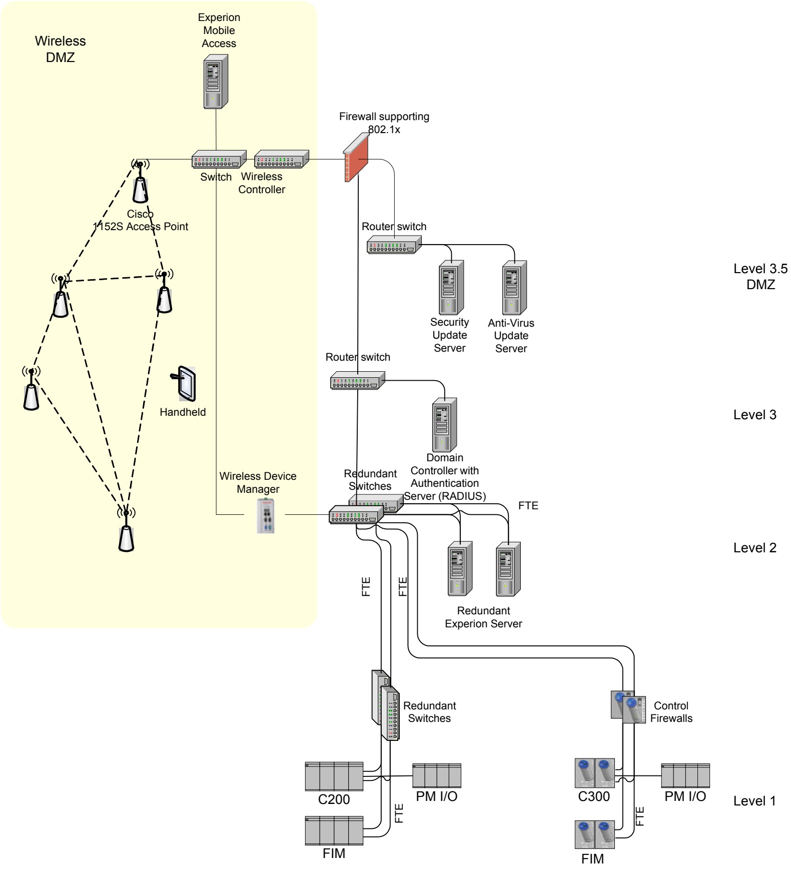


Figure 1: Experion Mobile Access topology

Security best practice for handheld devices

The following guidelines help operators maximize the security of the network while using a handheld device.

- Ensure logins and passwords are not saved in the browser.
- Log off before shutting down the browser.
- Never take the device off site, as data may be stored in the browser’s cache.
- Create a shortcut to Experion Mobile Access on the device. This ensures you are always connecting to Experion Mobile Access.

Installing and removing Experion Mobile Access

Related topics

"Installing Experion Mobile Access" on page 16

"Obtaining an SSL certificate for Experion Mobile Access" on page 17

"Removing Experion Mobile Access" on page 18

"Removing an SSL certificate" on page 19

Installing Experion Mobile Access

Installation of Experion Mobile Access is an optional component as part of eServer installation.

Obtaining an SSL certificate for Experion Mobile Access

To secure communication from mobile devices to the Experion eServer, it is necessary to install a valid certificate on the eServer node. You can obtain the certificate from a commercial certificate authority such as *VeriSign* or you can generate it using on site Certificate Authority (CA). Windows Server editions provide full featured Certificate Authority implementation that can be used for this purpose. Mobile clients must have certificate of the CA that issued eServer certificate installed in order to trust the eServer. eServer certificate's purpose is to authenticate eServer to the Mobile Client and to encrypt traffic between the two.

In order to limit access to the wireless network, it is critical to use WPA2 in Enterprise Mode with EAP-TLS selected as an authentication method. EAP-TLS requires mobile devices to have a certificate installed that verifies their identity. Device certificates can be purchased from commercial CA or generated by on-site CA as described above. WPA2 requires that a wireless device authenticate with a RADIUS server first before being granted network access. The certificate presented by the mobile device during initial negotiation is used to determine if access should be allowed or denied. RADIUS server matches Common Name present in the mobile device certificate with a white list of names allowed to access the network. The wireless device and the RADIUS server use mutual authentication to verify each other's identity based on certificates presented by each side during the negotiation process. The certificate of the wireless device must be trusted by the RADIUS server (have corresponding CA certificate and pass other certificate validity checks). The RADIUS server certificate must be trusted by the wireless device in a similar manner.

The same certificate authority may be used to generate certificates for eServer authentication and for WPA2 RADIUS authentication. Private (local to site) CA is preferred for RADIUS authentication.

Attention

A default self-signed certificate is generated as part of the Experion Mobile Access installation and is automatically installed within the local machines certificate store. If you do not purchase a certificate from a trusted provider, you will see an authentication error every time you browse to the Experion Mobile Access URL. Opt to continue to the site. Seeing this authentication error does not mean that the communication channel is any less secure, it just means that the browser does not know where the certificate came from. Experion Mobile Access is still communicating via SSL.

To obtain an SSL certificate for Experion Mobile Access from VeriSign

1. Go to http://www.verisign.com.
2. Click `Buy SSL Certificates`.
   Purchase an SSL Certificate.
3. On the eServer, browse to **Start** > **All Programs** > **Administrative Tools** > **IIS Manager**.
4. Click **Server Certificates**.
5. From the **Actions** sidebar, click **Import**.
6. Browse for the certificate and enter the password.
7. Click **OK**.

Removing Experion Mobile Access

To remove Experion Mobile Access

1. From eServer choose **Start** > **Control Panel**.
2. In large or small icon view, choose **Programs and Features**.
3. From the **Uninstall or change a program** list, click **Experion Mobile Access**.
4. At the top of the list, click **Uninstall/Change**.
5. Follow the instructions to complete the removal process.

Removing an SSL certificate

While it won't cause any issues to leave the SSL certificate on eServer after removing Experion Mobile Access, it is good practice to remove it.

Prerequisites

You need administrator privileges to perform this task.

To remove an SSL certificate

1. Open Microsoft Management Console on the eServer machine. To do this, select **Start** > **Run** then type `mmc`. Click **OK**.

   The Microsoft Management Console appears.
2. Choose **File** > **New**.
3. Choose **File** > **Add/Remove Snap-in**.
4. From the **Available snap-ins** list click **Certificates**. Click **Add >**.
5. In the **Certificates snap-in** window, check the **Computer account** option.
6. Click **Next** then **Finish**.
7. Click **OK**.
8. From the left-hand pane, expand **Personal** then click **Certificates**.
9. From the right-hand pane, right-click the certificate name (the certificate name appears in the **Issued By** column as *RootTrustedCA<computername>*).
10. Choose **Delete**.
11. From the left-hand pane, expand **Trusted Root Certification Authorities** then click **Certificates**.
12. From the right-hand pane, right-click the certificate name (the certificate name appears in the **Issued By** column as *RootTrustedCA<computername>).*
13. Choose **Delete**.
14. Choose **File** > **Exit** to close Microsoft Management Console.

Configuring Experion Mobile Access

Related topics

“Setting up operator access” on page 22
“Setting up alarm groups” on page 23
“Setting up history” on page 24
“Browser settings” on page 25
“Setting time-out” on page 26
“Configuring precision values for point parameters” on page 27

Setting up operator access

Operators are setup on a server-by-server basis. This means that any operators you set up on a server only impact that server.

Attention

By default the ‘modify’ link on the faceplate and access to the editable faceplate page are disabled. If you want to enable Experion Mobile Access to let operators modify faceplate values, contact your Honeywell representative.

The following are recommendations for setting up operators for Experion Mobile Access use:

- If operators only need to use Experion Mobile Access, ensure that their accounts are configured to not share with other applications, such as eServer.

  To prevent operators configured for Experion Mobile Access from using other forms of interaction with the eServer (such as eServer Standard Access or eServer Premium Access), go to the **Station Access** tab in *Configuration Studio* and ensure all the check boxes are not selected for that operator.
- Honeywell recommends you have a separate account for each Experion Mobile Access operator. This makes it clear who is on the server and who has acknowledged alarms using Experion Mobile Access. It also creates a more robust audit trail.
- Ensure the operator has the minimum scope of responsibility required for their role. Only grant '`view only`' access to assets in the operator’s scope of responsibility.
- Ensure that operator account passwords are set to expire after 90 days.
- Remember to provide a URL to operators so they can access Experion Mobile Access. The default URL is `https://servername/EMA`, where `servername` is the computer name of the eServer.

For more information about operator access, accounts, and scope of responsibility, see the following topics in the *Server and Client Configuration Guide*:

- "Operator-based security configuration checklist"
- "About scope of responsibility"
- "Configuring system security"
- "Operator definition, General tab"
- "Operator definition, Advanced tab"

Setting up alarm groups

The data that can be accessed via Experion Mobile Access is based on alarm groups, which can consist of a hierarchy of other groups (or points). Operators access the data associated with these groups and points by navigating up and down the hierarchy and clicking on links.

When implementing Experion Mobile Access, it is important to be aware that operators can only navigate down an alarm group structure if they have scope of responsibility (SOR) for all of the parent alarm groups. If they don’t, there is no link for them to click on. Note, however, that if there is no link to follow, operators can still locate points by doing a wildcard search. The search results return the first 80 points (alphabetically) in the operator's scope of responsibility.

Attention

Honeywell strongly recommends all points have the same SOR level as the alarm group they are within.

With Experion Mobile Access you can either use existing alarm groups or you can create specific alarm groups. When creating or modifying alarm groups for use with Experion Mobile Access, ensure that you:

- Include no more than 10 points per group
- Do not have more than five ‘child’ groups in a group
- Do not have more than four levels in an alarm group hierarchy

Exceeding these recommendations may result in:

- Excessive data usage (and consequently higher data costs for the end user)
- Poor device responsiveness and performance due to the extra data load

For more information on scope of responsibility see “About scope of responsibility” in the *Server and Client Configuration Guide*.

Related topics

“Using alarm groups” on page 31

“Searching for a point” on page 35

Setting up history

- It is important to consider the type of history that operators need to access from Experion Mobile Access and ensure that the relevant points are assigned to the appropriate history collection.
- Once history has been set up in Experion, it is available in Experion Mobile Access.

For more information on setting up history, see “History collection and archiving” in the *Server and Client Configuration Guide*.

Related topics

“Accessing point history” on page 36

Browser settings

The following describes browser settings and how they affect your Experion Mobile Access:

- JavaScript

  To enable live update of faceplates, enable JavaScript on your handheld device’s browser.

- Autocomplete

  To ensure security of logins, Honeywell strongly recommends that you disable your browser’s autocomplete feature.

Setting time-out

By default, Experion Mobile Access is set to time out after 1 minute. You can change the time-out value (up to 60 minutes) by following the steps below.

> **Attention**
>
> To maximize security when using mobile devices, Honeywell recommends the lowest possible time-out setting you can comfortably manage.

1 Make a backup of the XML configuration file *`C:\Program Files (x86)\Honeywell\Server\EMA\Website\Web.config`*.

2 Using a text editor, such as Notepad, edit *`C:\Program Files (x86)\Honeywell\Server\EMA\Website\Web.config`*.

3 Find the `sessionState` field and change it to the desired value (in minutes). The range is between 1 and 60 minutes.

For example, for a time-out of 5 minutes: `sessionState cookieless="UseCookies" mode="InProc" timeout="5"/`

If you set a value greater than the maximum value of 60, Experion Mobile Access will default back to 1 minute.

4 Find the *`forms`* field and change *`timeout`* to the desired value (in minutes). The range is between 1 and 60 minutes.

For example, for a time-out of 5 minutes: `<forms loginUrl="~/login.aspx" name=".QSWebAuth" path="/" protection="All" slidingExpiration="true" timeout="5" cookieless="UseCookies">`

If you set a value greater than the maximum value of 60, Experion Mobile Access will default back to 1 minute.

5 Save the *`Web.config`* file.

> **Attention**
>
> Editing the *`web.config.xml`* file at any time will cause the application to automatically restart. All connected clients will need to log in again.

6 Set the idle time-out for the application pool.

- **a** Open **IIS**.
- **b** In the **Connections** pane, expand the server node and click **Application Pools**.
- **c** Right-click **Default App pool** and select **Set Application Pool Defaults**.
- **d** Set the desired time-out in minutes.
- **e** Restart **IIS**.

Configuring precision values for point parameters

By default, Experion Mobile Access displays point parameter values (PV, SP, and OP) with a precision of two decimal points (for example, 32.56). You can change the number of decimal points (up to 10) by following the steps below.

1 Make a backup of *`C:\Program Files\Honeywell\Server\EEMA\Website\Web.config`*.

2 Open *`C:\Program Files\Honeywell\Server\EEMA\Website\Web.config`*.

3 Find the `precision` field and change it to the desired value. The range is between 0 and 10.

4 Save the *`web.config`* file.

Attention

Editing the *`web.config.xml`* file at any time will cause the application to automatically restart. All connected clients will need to log in again.

Operating Experion Mobile Access

Related topics

"Starting Experion Mobile Access" on page 30
"Using alarm groups" on page 31
"Using faceplates" on page 32
"Modifying parameter values and acknowledging alarms" on page 33
"Viewing alarms" on page 34
"Searching for a point" on page 35
"Accessing point history" on page 36
"Accessing online help" on page 37
"Security best practice for handheld devices" on page 13

Starting Experion Mobile Access

Prerequisites

Your handheld device must be connected to the wireless network connected to Experion.

Attention

This document does not cover how to connect a handheld device to the wireless network.

To start Experion Mobile Access

1. On your handheld device launch your web browser.
2. Type the URL *`https://servername/EMA`*, where *`servername`* is the name of the eServer.
   Alternatively, if configured in your system, click the shortcut to launch Experion Mobile Access.

   Tip

   If this is the first time you display this page, you may want to add it to your list of favorites so that you don't have to type the URL each time.

3. Log on using your Experion Mobile Access account and password.

   Attention

   If you do not use your Experion Mobile Access session for 1 minute, you will need to log in again.

   Attention

   A default self-signed certificate is generated as part of the Experion Mobile Access installation and is automatically installed within the local machines certificate store. If you do not purchase a certificate from a trusted provider, you will see an authentication error every time you browse to the Experion Mobile Access URL. Opt to continue to the site. Seeing this authentication error does not mean that the communication channel is any less secure, it just means that the browser does not know where the certificate came from. Experion Mobile Access is still communicating via SSL.

Using alarm groups

A group is a collection of points, which represent information about a particular part of your Experion system. Because groups can be organized into hierarchies, a group may include other groups.

For more information about alarm groups, see the "About alarm groups" topic in the *Operator's Guide*.

Tasks you can perform with alarm groups

- Click a group name to view the points and subgroups within the group.
- Next to the alarm group is an alarm icon. This is the highest urgency alarm that occurred in that alarm group. If it is flashing, that means one or more alarms in that group have not been acknowledged.
- Click **Up** to navigate to the immediate parent group. In the point listing you can see the present value of each point along with its alarm icon on the right.
- From an alarm group click **Home** to navigate to the top level group in the hierarchy.

  Note that you can only navigate down a group structure if you have permission to access all of its parent groups. If you don't, then you can use still locate a specific point or group by using the **Search** function.
- Click a point name to view the parameter values and alarm details for the point.
- Click **Show detail** to see more information about a group, such as the location and the full name of the group.
- Click **Hide detail** to hide the additional information.

Related topics

"Searching for a point" on page 35

"Setting up alarm groups" on page 23

Using faceplates

Attention

By default the ‘modify’ link on the faceplate and access to the editable faceplate page are disabled. If you want to enable Experion Mobile Access to let operators modify faceplate values, contact your Honeywell representative.

A point is a collection of information about your Experion system. A point can be used to represent a pump, a motor, a process controller, or a part thereof.

For more information on faceplates, see “Faceplates” in the *Server and Client Configuration Guide*.

- The parameter values shown on the faceplate in Experion Mobile Access are the values current when you clicked the point name.
- Click **Refresh** to see the updated values.
- Values are automatically refreshed every 5 seconds. To stop this, click **Stop Live Updates**. To restart automatic refresh, click **Start Live Updates**.

  Note that you will only see live updates if it has been configured as the default on the server and if JavaScript has been enabled on the browser.
- Click **Modify** if you want to change any parameter values and acknowledge an alarm. The **Modify** option will only appear if you have permission to modify parameters for that point.
- Click **More** to view details of the point including the asset location on the server, description and server name.
- Click the history icon (next to the parameter) to see the historical parameter values for the point. Note that history is available only if the point parameter has been assigned to history.

Modifying parameter values and acknowledging alarms

Attention

By default the ‘modify’ link on the faceplate and access to the editable faceplate page are disabled. If you want to enable Experion Mobile Access to let operators modify faceplate values, contact your Honeywell representative.

To change parameter values, type the new value for any of the displayed parameters and click **Submit** to save all the values you have changed.

To acknowledge an alarm, select the **Ack Alarm** check box and click **Submit**. When you acknowledge an alarm, the current alarm is acknowledged as well as any unacknowledged alarms that existed for the point when you called up the alarm dashboard.

Click **Cancel Modify** to undo any changes you have made to parameter values and return to the faceplate.

Viewing alarms

For a full list of Experion alarm icons and their meaning, see “Alarm Summary columns” in the *Operator’s Guide*.

- The alarm dashboard shows 20 of the most recent point alarms arranged in order of urgency (most urgent first). To browse through the 100 top priority alarms, click **[21–40]**, **[41–60]**, and so on, at the bottom of the screen.
- The number in parentheses under the alarm icon indicates the number of times the alarm has already occurred. The alarm information also includes (on the right-hand side) information about the alarm condition (and sub-condition, where applicable).
- Use your browser’s refresh to update the alarm list.
- The alarm icons in Experion Mobile Access are the same as those used on Experion Station displays. For example, a white exclamation mark in a red flashing square means an urgent priority, unacknowledged alarm.

  You cannot acknowledge alarms from the dashboard.

Searching for a point

Use the **Search** display to find a point. To access the search box from a faceplate, click the **Search** link.

To search for a point

- Type the name of the point and click **Search**.
  If you do not know the name of the point, you can use wildcard characters:
  - Use `*` to represent one or more unknown characters. For example, type `FC*` to find the points *FC001*, *FC002*, *FC003*, and so on.

    Tip

    You only need to use the wildcard at the beginning of a string. For example, `Level1*` will find points ‘Level1Chiller,’ ‘Level1EastChiller.’

    A search containing only `*` may yield undesirable search results.
  - Use `?` to represent a single unknown character. For example, type `FC?00` to find the points *FC100*, *FC200*, *FC300*, and so on.

Related topics

“Using alarm groups” on page 31
“Setting up alarm groups” on page 23

Accessing point history

History shows a trend of the historical parameter values for a point. You can view history for any point's parameter provided:

- It is a numerical parameter, e.g. PV
- History has been configured for that point

To access a point's history

1. Make sure you are in faceplate view.
2. Click on the icon to the left of the parameter. If history has not been configured for that point, a message will tell you so.
3. If you want to change the amount of history you see, from the **History type** list choose:
   - **Fast history**
   - **Recent history**
   - **Shift history**
4. Click **Show numeric history** to see historical parameter values in a data table format. Click **Hide numeric history** to hide the tabulated values.

Related topics

"Setting up history" on page 24

Accessing online help

To access online help

- Click **Help** on each display.

Security best practice for handheld devices

The following guidelines help operators maximize the security of the network while using a handheld device.

- Ensure logins and passwords are not saved in the browser.
- Log off before shutting down the browser.
- Never take the device off site, as data may be stored in the browser’s cache.
- Create a shortcut to Experion Mobile Access on the device. This ensures you are always connecting to Experion Mobile Access.

Managing Experion Mobile Access

Related topics

“Setting up an additional user” on page 40

“Adding handheld devices” on page 41

“Restarting Service Framework” on page 42

“Restarting the IIS Web Server” on page 43

“Restarting/Recycling the Application Pool” on page 44

Setting up an additional user

For details on creating operator accounts see “Operator-based security configuration checklist” in the *Server and Client Configuration Guide.*

For more information on administration of users in Experion, see “Administering users” in the *System Administration Guide*.

Adding handheld devices

There are no extra considerations when adding a handheld device to the network. If you are not using a Dolphin handheld computer, the default style sheet will be applied.

Be aware that Experion Mobile Access running on a non-Dolphin device will, for the most part, look the same as it does on the Dolphin. However, there may be some visual discrepancies, which do not affect performance in any way.

Restarting Service Framework

To restart Service Framework

1. On the server node, browse to **Start** > **All Programs** > **Administrative Tools** > **Services** or **cmd** > **services.msc**.
2. Scroll to the service ‘Experion PKS Service Framework,’ right-click and select either **start** or **restart**.

Related topics

“Restarting the IIS Web Server” on page 43
“Error: This page cannot be displayed” on page 49

Restarting the IIS Web Server

To restart the IIS Web Server

1 On the server node browse to **Start** > **All Programs** > **Administrative Tools** > **IIS Manager**.

2 Select the server name then under **Actions** click **Restart**.

Related topics

“Restarting Service Framework” on page 42
“Error: This page cannot be displayed” on page 49

Restarting/Recycling the Application Pool

To restart or recycle the Application Pool

1. On the server node, browse to **Start** > **All Programs** > **Administrative Tools** > **IIS Manager**.
2. Expand the server name node, expand **Sites** then select **Default Websites**. Under **Actions** select **View Applications**.
3. Confirm that the Application Pool is set to ‘DefaultAppPool (v2.0).’ If it is not, right-click and select **Advanced Settings** and set it to ‘DefaultAppPool (v2.0).’
4. Return to the server name node and select **Application Pools** just beneath it. Select **DefaultAppPool** and then under **Actions** select **Recycle**, **Stop** then **Start**.

Related topics

“Service unavailable” on page 51

Troubleshooting for Experion Mobile Access

This section provides information about troubleshooting, diagnostics, and error messages that appear while using Experion Mobile Access.

Related topics

Live updates are not working

The faceplate data is not updating automatically.

Diagnostic check

Make sure the browser isn’t hung by refreshing the browser.

Cause

JavaScript needs to be enabled in the browser for live updates to work.

Solution

In the browser enable JavaScript.

Cause

Experion Mobile Access needs to be configured so that live update is set to *True* as the default.

Solution

1. On eServer, run Experion Mobile Access in a browser.
2. Click **Configuration**.
3. In the **Default to Live Updates** list, click **True**.

Can navigate to login page but cannot log in

The operator can navigate to the Experion Mobile Access home page, but cannot log in.

Diagnostic check

URL is correct, user name and password are valid.

Cause

- Incorrect login credentials.
- Cookies disabled on the browser.

Solution

- In Station, check that the operator login credentials are correct.
- Ensure you have cookies enabled on the web browser. Experion Mobile Access stores the user's session state in a cookie. This is part of browser configuration.

For more information on setting up and configuring operator access, see "Operator definition, General tab" and "Operator definition, Advanced tab" in the *Server and Client Configuration Guide*

Cannot acknowledge an alarm

The operator cannot see the **Ack Alarm** check box.

Diagnostic check

Check the operator’s scope of responsibility.

Cause

The operator’s scope of responsibility does not allow acknowledging alarms.

Solution

If the user is meant to be able to acknowledge alarms, change their scope of responsibility in eServer.

For more information about scope or responsibility see:

- “Scope of responsibility asset permissions” in the *Server and Client Configuration Guide*.
- “Guidelines for defining scope of responsibility” in the *Server and Client Configuration Guide*.

Error: This page cannot be displayed

Error in the browser: *Error: This page cannot be displayed.*

Diagnostic check

Determine if the server is available by navigating to `https://servername`, where `servername` is the name of the eServer.

Cause

The server is unavailable for some reason.

Solution

If you see an IIS banner, then the server is available.

If you see a page connection error, then there is a server issue. Check the server settings and restart IIS Web Server.

For more information on configuring eServer, see 'eServer configuration procedures' in the *Server and Client Configuration Guide*.

Related topics

“Restarting Service Framework” on page 42
“Restarting the IIS Web Server” on page 43

Server Error 403 - Access is Denied

Error in the browser: *Server Error 403 – Access is Denied*

Diagnostic check

Check the URL. It should be `https://servername/EMA`, where `servername` is the name of the eServer.

Cause

Unencrypted (http) connections are disabled by default.

Solution

Enter the following URL into your browser: `https://servername/EMA`, where `servername` is the name of the eServer.

Service unavailable

Error in the browser: *HTTP Error 503. The service is unavailable.*

Diagnostic check

On the server, open IIS Manager, navigate to the Application Pools page and check the status of the ‘Default App Pool.’ In its correct state it should be ‘started.’

Cause

This can occur if the Web site’s Application pool (which hosts the ASP.NET worker process) has experienced problems or stopped/crashed.

Solution

Restart/Recycle the application pool.

Related topics

“Restarting/Recycling the Application Pool” on page 44

Experion Mobile Access vs. Station faceplates

This section displays and describes the differences between the major Experion Mobile Access faceplates and their Station equivalents.

A typical Station faceplate is divided into four major zones:

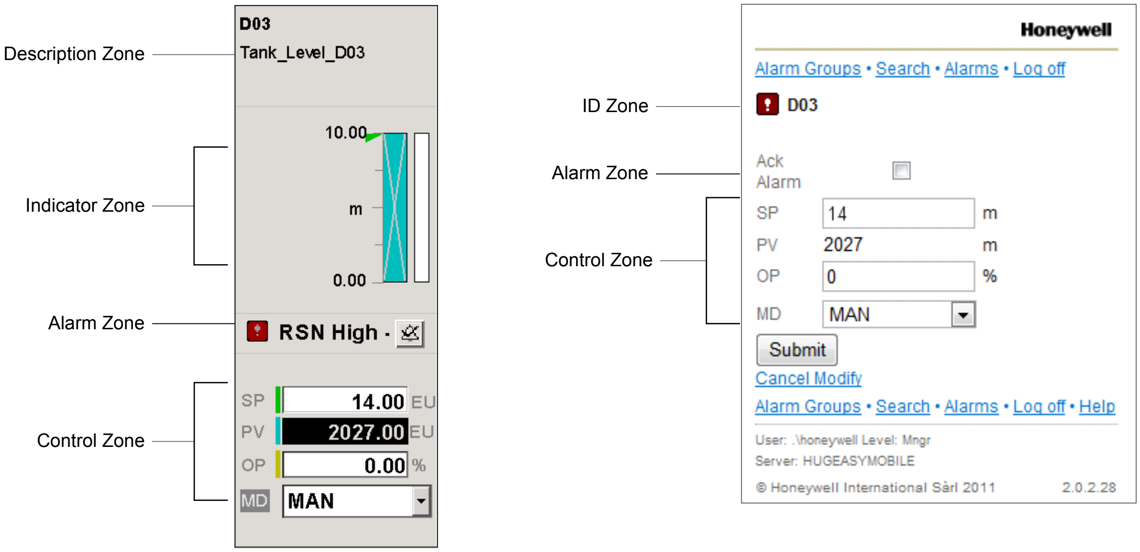
1. Description Zone. Shows the point ID, description and status.
2. Indicator Zone. Shows PV, set point and related information.
3. Alarm Zone. Shows the most recent, highest priority, unacknowledged alarm.
4. Control Zone. Contains the buttons and boxes you use to control the point.

A typical Experion Mobile Access faceplate is divided into three major zones:

1. ID Zone. Shows the point ID.
2. Alarm Zone. Shows a check box for acknowledging the alarm.
3. Control Zone. Contains the buttons and boxes you use to control the point.

The following section shows five of the most commonly used faceplates in both Station and Experion Mobile Access. The Experion Mobile Access faceplates (on the right of each image) are shown as if you are modifying the point. Modifying points is disabled by default. Note that the faceplates may look slightly different from the images shown, depending on the browser you are using.

Analog



D03
Tank_Level_D03

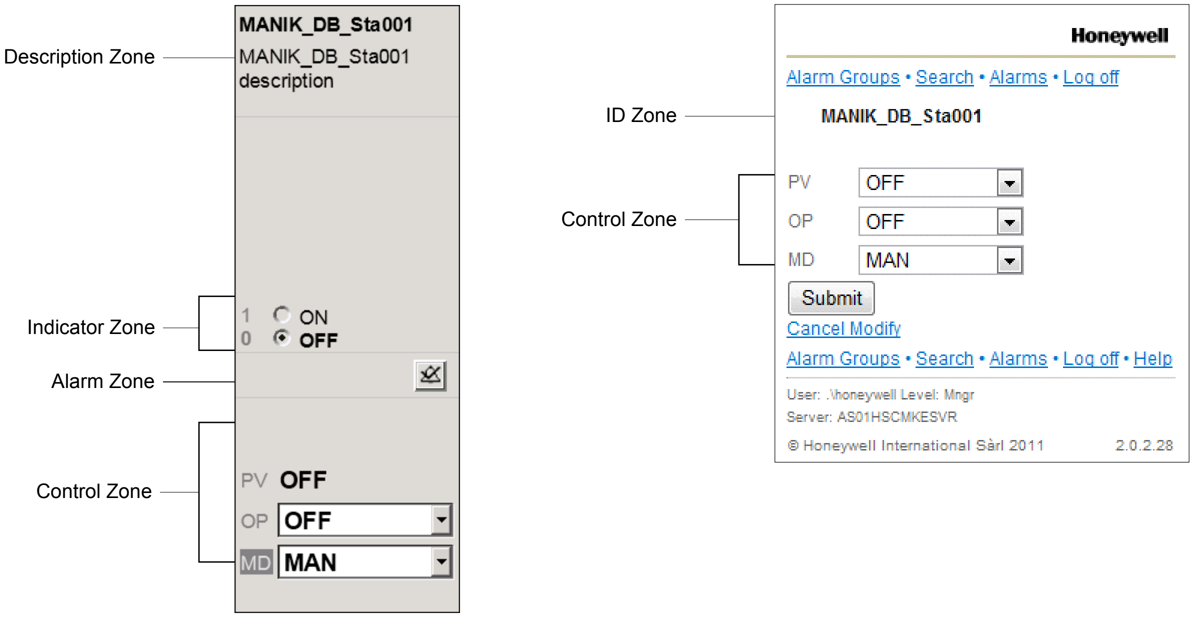
SP 14.00 EU
PV 2027.00 EU
OP 0.00 %
MD MAN

D03
Ack Alarm □
SP 14 m
PV 2027 m
OP 0 %
MD MAN

User: .\honeywell Level: Mngr
Server: HUGEASYMOBILE
© Honeywell International Sàrl 2011 2.0.2.28

Figure 2: Analog point on a Station faceplate and on an Experion Mobile Access faceplate

Status



MANIK_DB_Sta001
MANIK_DB_Sta001 description

1 ○ ON
0 ● OFF

PV OFF
OP OFF
MD MAN

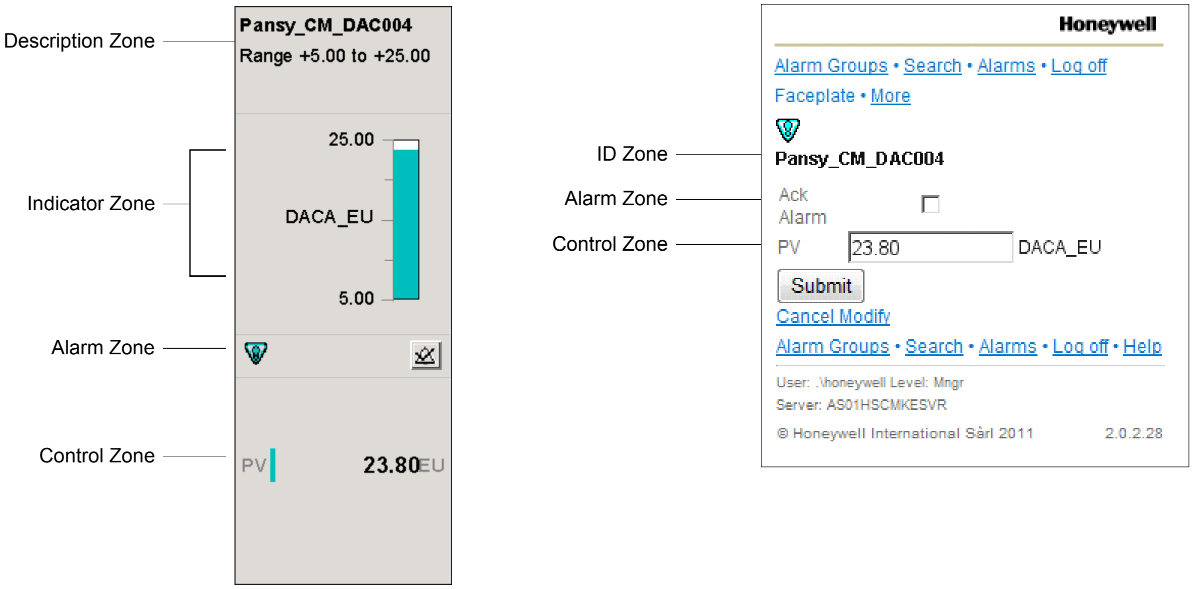
MANIK_DB_Sta001

PV OFF
OP OFF
MD MAN

User: .\honeywell Level: Mngr
Server: AS01HSCMKESVR
© Honeywell International Sàrl 2011 2.0.2.28

Figure 3: Status point on a Station faceplate and on an Experion Mobile Access faceplate

DACA



Pansy_CM_DAC004
Range +5.00 to +25.00

PV 23.80EU

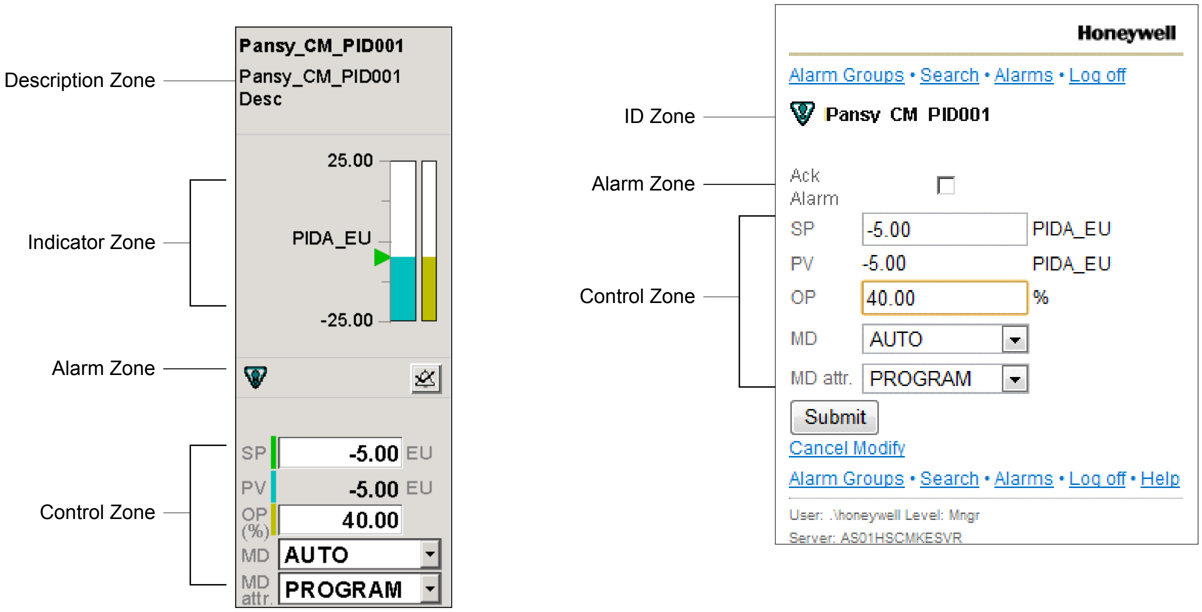
Pansy_CM_DAC004

Ack Alarm □
PV 23.80 DACA_EU

User: .\honeywell Level: Mngr
Server: AS01HSCMKESVR
© Honeywell International Sàrl 2011 2.0.2.28

Figure 4: DACA point on a Station faceplate and on an Experion Mobile Access faceplate

PID



Pansy_CM_PID001
Pansy_CM_PID001 Desc

25.00
PIDA_EU
-25.00

SP -5.00 EU
PV -5.00 EU
OP (%) 40.00
MD AUTO
MD attr. PROGRAM

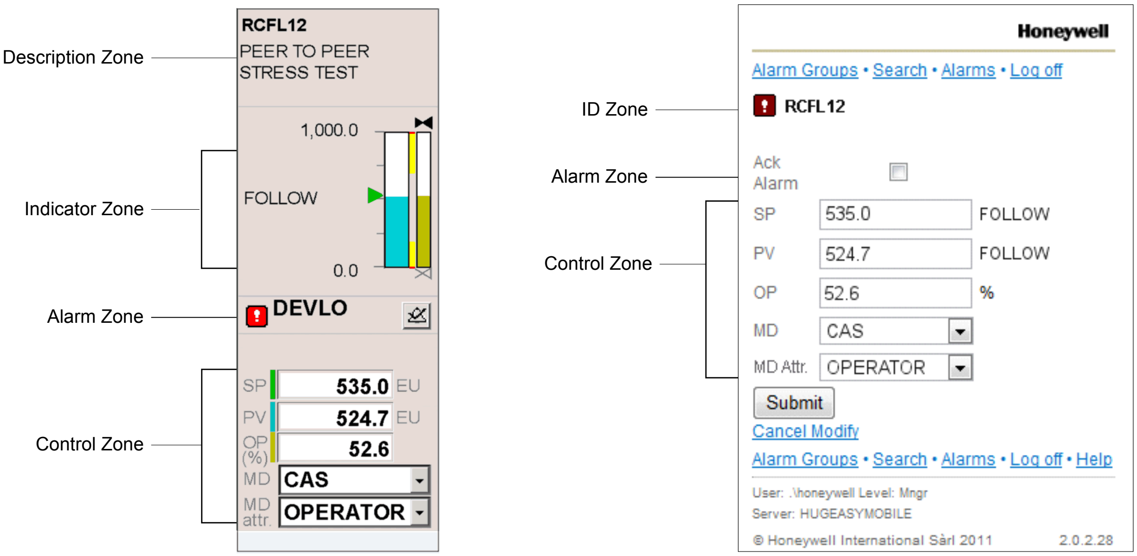
Pansy CM PID001

Ack Alarm □
SP -5.00 PIDA_EU
PV -5.00 PIDA_EU
OP 40.00 %
MD AUTO
MD attr. PROGRAM

User: .\honeywell Level: Mngr
Server: AS01HSCMKESVR

Figure 5: PID point on a Station faceplate and on an Experion Mobile Access faceplate

TPS



RCFL12
PEER TO PEER STRESS TEST

1,000.0
FOLLOW
0.0

DEVLO

SP 535.0 EU
PV 524.7 EU
OP (%) 52.6
MD CAS
MD attr. OPERATOR

RCFL12

Ack Alarm □
SP 535.0 FOLLOW
PV 524.7 FOLLOW
OP 52.6 %
MD CAS
MD Attr. OPERATOR

User: .\honeywell Level: Mngr
Server: HUGEASYMOBILE
© Honeywell International Sàrl 2011 2.0.2.28

Figure 6: TPS point on a Station faceplate and on an Experion Mobile Access faceplate

Related topics

"About Experion Mobile Access" on page 7

Supported faceplates

The following Experion faceplates are supported on Experion Mobile Access. For more information on these faceplates, refer to the "About detail and group displays" topic in the *Control Building User's Guide*.

Faceplate name	Category
sysdtltpsanalgacc_fp.htm	TPS
sysdtltpsanalgin_fp.htm	TPS
sysdtltpsanalout_fp.htm	TPS
sysdtltpscounter_fp.htm	TPS
sysdtltpscountreu_fp.htm	TPS
sysdtltpsdevctl_fp.htm	TPS
sysdtltpsdigcomp_fp.htm	TPS
sysdtltpsdigin_fp.htm	TPS
sysdtltpsdiginout_fp.htm	TPS
sysdtltpsdigout_fp.htm	TPS
sysdtltpsllsummer_fp.htm	TPS
sysdtltpsnonpv_fp.htm	TPS
sysdtltpsnumeric_fp.htm	TPS
sysdtltpsoutput_fp.htm	TPS
sysdtltpspid_fp.htm	TPS
sysdtltpsposprop_fp.htm	TPS
sysdtltpspvoutput_fp.htm	TPS
sysdtltpsrampsoak_fp.htm	TPS
sysdtltpsswitch_fp.htm	TPS
sysdtltpstimer_fp.htm	TPS
sysdtlacc_fp.htm	SCADA
sysdtlana_fp.htm	SCADA
sysdtlana_TDC_EC_fp.htm	SCADA
sysDtlana_TDC_ECPID_fp.htm	SCADA
sysDtlAna_TDC_ECPIDRB_fp.htm	SCADA
sysDtlAna_TDC_Template_fp.htm	SCADA
sysdtlsta_fp.htm	SCADA
sysdtlcda_fp.htm	Process
sysdtldaca_fp.htm	Process
SysDtlDataacqa_fp.htm	Process

Faceplate name	Category
SysDtlDevctl1a_fp.htm	Process
sysdtldevctla_fp.htm	Process
sysdtlfirstouta_fp.htm	Process
sysdtlflaga_fp.htm	Process
sysdtlgrpcaprbka_fp.htm	Process
sysdtlhtmotora_fp.htm	Process
sysdtlibva_fp.htm	Process
sysdtlltmotora_fp.htm	Process
sysdtlpida_fp.htm	Process
sysdtlpidpla_fp.htm	Process
sysdtlpidplalta_fp.htm	Process
sysdtlpospa_fp.htm	Process
sysdtlrampa_fp.htm	Process
sysdtlrcma_fp.htm	Process
SysDtlRegctla_fp.htm	Process
sysdtlscma_fp.htm	Process
sysdtlsolenoida_fp.htm	Process
sysdtlsvppida_fp.htm	Process
sysdtlswa_fp.htm	Process
sysdtltima_fp.htm	Process
SysDtlTimera_fp.htm	Process
sysdtltota_fp.htm	Process
SysDtlTotalizera_fp.htm	Process
sysdtlUCMA_fp.htm	Process
sysdtlvalvedampera_fp.htm	Process
sysdtlvalvedampera_inch_fp.htm	Process
sysdtlffai_fp.htm	FF-system
sysdtlffao_fp.htm	FF-system
sysdtlffdevice_fp.htm	FF-system
sysdtlffdi_fp.htm	FF-system
sysdtlffdo_fp.htm	FF-system
sysdtlffmai_fp.htm	FF-system
sysdtlFFPID_fp.htm	FF-system
sysdtlacea_fp.htm	Etools-system
sysdtlaga38detaila_fp.htm	Etools-system
sysdtlaga38grossa_fp.htm	Etools-system
sysdtlaga78detaila_fp.htm	Etools-system
sysdtlaga78grossa_fp.htm	Etools-system
sysdtlaga98detaila_fp.htm	Etools-system
sysdtlaga98grossa_fp.htm	Etools-system
sysdtlceea_fp.htm	Etools-system

Faceplate name	Category
sysdtlceeacea_fp.htm	Etools-system
sysdtlceescea_fp.htm	Etools-system

Notices

Trademarks

Experion®, PlantScape®, SafeBrowse®, TotalPlant®, and TDC 3000® are registered trademarks of Honeywell International, Inc.

OneWireless™ is a trademark of Honeywell International, Inc.

Other trademarks

Microsoft and SQL Server are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Trademarks that appear in this document are used only to the benefit of the trademark owner, with no intention of trademark infringement.

Third-party licenses

This product may contain or be derived from materials, including software, of third parties. The third party materials may be subject to licenses, notices, restrictions and obligations imposed by the licensor. The licenses, notices, restrictions and obligations, if any, may be found in the materials accompanying the product, in the documents or files accompanying such third party materials, in a file named third_party_licenses on the media containing the product, or at http://www.honeywell.com/ps/thirdpartylicenses.

Documentation feedback

You can find the most up-to-date documents on the Honeywell Process Solutions support website at:

http://www.honeywellprocess.com/support

If you have comments about Honeywell Process Solutions documentation, send your feedback to:

hpsdocs@honeywell.com

Use this email address to provide feedback, or to report errors and omissions in the documentation. For immediate help with a technical problem, contact your local Honeywell Process Solutions Customer Contact Center (CCC) or Honeywell Technical Assistance Center (TAC) listed in the “Support and other contacts” section of this document.

How to report a security vulnerability

For the purpose of submission, a security vulnerability is defined as a software defect or weakness that can be exploited to reduce the operational or security capabilities of the software.

Honeywell investigates all reports of security vulnerabilities affecting Honeywell products and services.

To report a potential security vulnerability against any Honeywell product, please follow the instructions at:

https://honeywell.com/pages/vulnerabilityreporting.aspx

Submit the requested information to Honeywell using one of the following methods:

- Send an email to security@honeywell.com.

  or

- Contact your local Honeywell Process Solutions Customer Contact Center (CCC) or Honeywell Technical Assistance Center (TAC) listed in the “Support and other contacts” section of this document.

Support

For support, contact your local Honeywell Process Solutions Customer Contact Center (CCC). To find your local CCC visit the website, https://www.honeywellprocess.com/en-US/contact-us/customer-support-contacts/Pages/default.aspx.

Training classes

Honeywell holds technical training classes on Experion PKS. These classes are taught by experts in the field of process control systems. For more information about these classes, contact your Honeywell representative, or see http://www.automationcollege.com.

Index