The Allworx family of products includes a set of features that are designed to enable support personnel to externally monitor the phone system and receive notifications of interesting events. These features do not require feature keys to enable, and are built on industry-standard protocols and mechanisms to allow anyone to easily add tracking of Allworx products to their existing network and equipment monitoring infrastructure.

System Event Logging with Severity Levels

Since the inception of the product, the Allworx server has maintained a System Event log that captures information at runtime regarding the current state and operation of the server. This log can be viewed or downloaded from the admin UI, and is also the basis for many of the notification and monitoring features that are discussed here.

Beginning in Release 7.5[1], each log message in the system was assigned a severity level consistent with those defined in the "BSD Syslog Protocol" RFC 3164 and "The Syslog Protocol" RFC 5424. These severity levels are as follows:

- Emergency (0): system is unusable (e.g. boot failed...)
- Alert (1): action must be taken immediately (e.g. shutdown the warp field generator now...)
- Critical (2): critical conditions (e.g. internal operation unexpectedly failed...)
- Error (3): error conditions (e.g. CO line is dead...)
- Warning (4): warning conditions (e.g. Admin login failures)
- Notice (5): normal but significant condition (e.g. Dialplan enabled)
- Informational (6): informational messages (e.g. New phone on port 13)
- Debug (7): debug-level messages (e.g. +++ IEC [7.5.0.0:sipDialog.c 2021])

The implementation of these message levels within the Allworx is such that levels Emergency (0) through Informational (6) are intended to provide information that would be of use to Installation and Support personnel in monitoring and diagnosing operation of the Allworx server, while the Debug (7) level is intended primarily for Allworx development and technical support (which is why the Debug level messages are often encoded with internal details, while the other levels provide more understandable descriptions of what is being logged).

Although not technically part of external monitoring, it should also be noted that the display of the System Event log on the server provides a mechanism to filter the current view of the log by one or more of the severity levels, with the default filter being set to display Emergency (0) through Informational (6).

---

1. Prior to Release 7.5, all messages were classified as either Error (3) or Debug (7)

Syslog Event Transmission

In addition to capturing the System Event Log on its internal storage (which is done by default with a fixed storage size), the Allworx Server also provides a mechanism for this event log information to be transmitted to an external "collector" (as defined in RFC 3164). This functionality can be enabled from the Allworx admin UI under ***Maintenance > Tools > Syslog – System Events***, where you can specify the IP Address and Port of a device that will receive the Syslog event transmission (note that the Allworx server must have a network route available to reach the specified IP Address/Port).

The data that is transmitted from the Allworx server to the Syslog collector is the same data that is included in the Allworx server's built in System Event Log – message, severity level, timestamp, and source server identifier[1].

There are a variety of commercially available and free Syslog collector applications available for multiple platforms that can be used to receive the Syslog Event Transmission from the Allworx server. Depending on the application, they can offer such features as being able to collect transmissions from multiple sources (Allworx servers and/or other Syslog-capable devices), log filtering, reporting and notification on specific criteria. An additional advantage of using a Syslog collector to collect data from an Allworx server is that the storage capacity for log data can be greatly increased – rather than depending on the fixed size event log storage capability of the Allworx server; all log data can be collected and archived without older data being overwritten.

---

1. The exact content of the log message varies by firmware release. For example, releases prior to 7.5 supported SysLog transmissions, but only with the two severity levels supported in those versions.

Auto Notification

The Allworx server supports a built-in mechanism to send email notification of the occurrence of specific system events. Auto Notification is configured from the Allworx admin UI under **Reports > Auto Notification.** This feature allows for events to be selected by text string matching (Release 7.4 and later) and/or by Syslog severity level (Release 7.5 and later). When messages occur that match the selected criteria, they are emailed to all configured email addresses[1]. Note that any valid email address will be used, which allows for email to text message as well as standard email.

The figure below illustrates an example system configuration for Auto Notification. In the example, notifications will be emailed for all events of severity Emergency, Alert, Critical or Error, and also for any events containing the string 'Application started successfully' or 'tSip: Temporarily blocking'. Enabling Message Severity Filtering for the levels in the example would be a standard mechanism to receive notifications from an Allworx server of "non-standard" events that would not require any external monitoring applications.

---

1.   The Allworx server must be configured to allow email to be sent. See the *Allworx Server Administrator's Guide* for details.

SNMP

Beginning in Release 7.4, both the Allworx server and phones[1] include support for a Simple Network Management Protocol (SNMP) agent. The SNMP agent runs on the server and phone and services requests from network management applications to retrieve data used for monitoring the device.

The SNMP version implemented by Allworx is SNMPv2c, as defined in RFCs 1901-1908. Allworx agents implement the GET Protocol Data Units (PDUs) GET, GETNEXT and GET-BULK, and do not support SET or Traps.

The following Management Information Bases (MIBs) are supported:

- SYSTEM-MIB (MIB-II.system(1))
- INTERFACES-MIB
- (MIB-II.interfaces(2))
- IP-MIB
- (MIB-II.ip(4))
- ICMP-MIB
- (MIB-II.icmp(5))
- TCP-MIB
- (MIB-II.tcp(6))
- UDP-MIB
- (MIB-II.udp(7))
- SNMP-MIB

- (MIB-II.snmp(11))
- HOST-RESOURCES-MIB
- (MIB-II.hr(25))
- NETWORK-SERVICES-MIB
- (MIB-II.application(27))
- SIP-COMMON-MIB
- (MIB-II.sipCommon-MIB(149))
- SIP-UAMIB
- (MIB-II.sipUAMIB(150))
- SIP-SERVER-MIB
- (MIB-II.sip[a] Server(151))

a.   SIP-SERVER-MIB is only supported by the Allworx server, not supported by the phones.

For more detailed information about SNMP support (including feature configuration, protocol details, supported OID values and expected values in each of the supported MIBs), please refer to the document **_SNMP User's Guide_** which is available in the 'Documentation' section of the Allworx Partner Portal.

There are a variety of commercially available and free SNMP applications available for multiple platforms that can be used to collect SNMP data from Allworx servers and phones. Depending on the application, they can offer such features as being able to collect data from multiple sources (Allworx servers, phones and/or other SNMP-capable devices), data filtering, reporting and notification on specific criteria.

---

1.   Allworx Reach does not support SNMP.