



## Tech Overview : Managing QQ Instant Messenger by Two Default Rules

Instant messaging software has been used commonly among business communication because of its convenience. However, it has also been used by employees for their personal activities. The abuse of instant messaging software has a detrimental impact on productivity. Besides, employees transferring files by instant messaging software may slow down network performance and leak out confidential business information. For the reasons above, more and more businesses install Internet security devices to manage the usage of instant messaging software.

The Nusoft Internet Recorder is designed to manage various kinds of instant messaging software, such as Windows Live Messenger, Yahoo! Messenger, Skype, QQ Messenger, etc. To manage the software, the users need to know the default rule settings very well. For managing the usage of Windows Messenger, Yahoo! Messenger and Skype, the users only have to select the default rule. However, for managing the usage of QQ Messenger, more steps are required.

The reason why managing QQ Messenger requires more steps is that QQ Messenger uses encryption. The Nusoft Internet Recorder can only record the content of users whose account and password have been verified or authenticated by the device. For example, if the IT administrator allows all users or all authenticated users to log in QQ Messenger the Internet recorder can only record the login and logout times of the users, not the content of their messages.

There are two settings for recording the content of the QQ Messenger, namely, **Accept : Valid password** and **Accept : Authenticated user with valid password**.

### Scenario : Allowing the users with permitted passwords

The IT administrator can allow the users with permitted passwords by selecting **Accept : Valid password / Drop : Invalid password** under **Behavior Management > IM Management > Default Rule**. The user or the IT administrator then needs to go to the webpage (enter the interface's IP address appended with **qq** in the address field, e.g., <http://192.168.1.1/qq>) for password verification.



Figure 1. Allowing the Users with Permitted Passwords



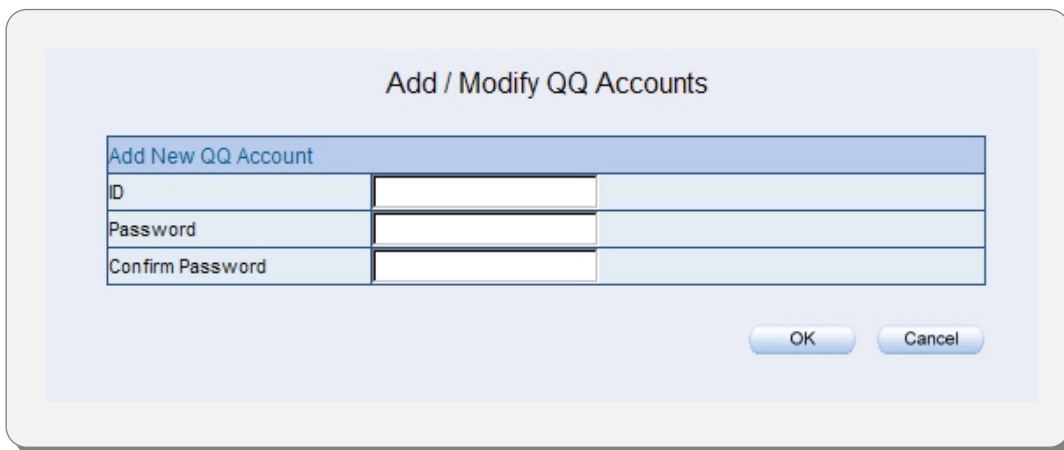


Figure 2. Entering the Account and Password

**Scenario: Allowing the authenticated users with permitted passwords**

Once the IT administrator allows the authenticated users with permitted passwords by selecting **Accept : Authenticated user with valid password / Drop : Unauthenticated user or invalid password** under **Behavior Management > IM Management > Default Rule**. The user or the IT administrator then needs to go to the webpage ( enter the interface's IP address appended with **auth** in the address field, e.g., <http://192.168.1.1/auth> ) for password verification.



Figure 3. Allowing the Authenticated Users with Permitted Passwords



The image shows a software dialog box for authentication. It is divided into two main sections: 'Authentication' and 'IM Protocol'.  
The 'Authentication' section, highlighted with a red box, contains two input fields: 'Name' and 'Password', both with a '(Max. 128 characters)' label.  
The 'IM Protocol' section contains several sub-sections, each with an 'Account' field and a '(Max. 128 characters)' label:  
- MSN: One 'Account' field.  
- Yahoo: One 'Account' field.  
- ICQ / AIM: One 'Account' field.  
- QQ: Three fields: 'Account', 'Password', and 'Confirm Password', each with a '(Max. 128 characters)' label. This entire sub-section is highlighted with a red box.  
- Gadu-Gadu: One 'Account' field.  
At the bottom right of the dialog box, there are two buttons: 'OK' and 'Cancel'.

Figure 4. Entering the Accounts and Passwords for Authentication and Verification



## Product News : Preventative Management and Incident Recording

The growing ease of access that people have to the Internet, and technologies that provide greater bandwidth, is ensuring the Internet's penetration into enterprises and our daily lives continues to grow. However, as users embrace all the benefits it has to offer, a large percentage of users are unaware of the pitfalls that it can bring.

Most Internet users ignore even the most basic practices for safe Internet usage. As a result, when users download software for various purposes, they are unaware of any hidden malicious code or threats that could allow hackers with direct access into the enterprise's private network. A recent news report highlighted this danger when a government worker ignored Internet usage policies by downloading the P2P software client "Foxy" for the purposes of downloading movies onto their work computer. However, the software was used as stepping-stone by a hacker to leak highly confidential documents from the government's network.

To counteract the possibility of confidential information being leaked, enterprises need a device capable of both preventing and recording compromises in network security. However, to the detriment of the majority of enterprises, emphasis is placed on attacks originating from outside the local network. In addition, the majority of firewalls only provide a partial solution to an enterprise's security concerns

Internet Recorder provides the perfect complement to firewalls by rectifying these deficiencies.

Features:

### ◆ Preventative Management

To prevent any network breaches or incidents before they arise, the Nusoft Internet Recorder provides preventative management. IT administrators can effectively regulate software access, such as P2P and instant messaging applications, for each employee according to the appropriateness of the software in regards to the company's network policy.

**Application Management -- Currently Supported Applications:**

Peer-to-Peer Sharing, Multimedia Streaming, Online Gaming, VPN Tunneling and Remote Controlling.

**Instant Messaging Management -- Currently Supported Software:**

Windows Live Messenger, Skype, Yahoo! Messenger, ICQ / AIM, QQ Messenger, Google Talk, Gadu-Gadu and Web IM.

### ◆ Incident Recording

Apart from providing preventative management, incident recording is another essential tool. To ensure enterprises are equipped with the benefits of Internet-based communication software for business, the Nusoft Internet Recorder can regulate which software to grant employees with and provide highly detailed recordings of any communication. Thus if any breaches in conduct occur, evidence for the courts can be easily produced.

**Internet Services Recording -- Currently Supported Services:**

SMTP, POP3/IMAP, HTTP/HTTPS, Web-Based Email, FTP, TELNET, Instant Messaging, Web SMTP and Web POP3

The Nusoft Internet Recorder preventative management and incident recording protects enterprises' sensitive information assets, providing a valuable tool to assist enterprises.



	Preventative Management	Incident Recording
Purpose	The Nusoft Internet Recorder prevents the leakage of confidential information and employees' use of applications and instant messaging software.	The Nusoft Internet Recorder can permit any communication tools deemed essential for conducting business with clients and customers. However all communication will be recorded, thus any misuse can be used as evidence in the courts.
Management Capabilities	<p>Provides Application Management of:</p> <ul style="list-style-type: none"> <li> Peer-to-Peer Sharing</li> <li> Multimedia Streaming</li> <li> Online Gaming</li> <li> VPN Tunneling</li> <li> Remote Controlling</li> </ul> <p>Provides Instant Messaging Management of:</p> <ul style="list-style-type: none"> <li> Windows Live Messenger</li> <li> Skype</li> <li> Yahoo! Messenger</li> <li> QQ Messenger</li> <li> Google Talk</li> <li> ICQ / AIM</li> <li> Gadu-Gadu</li> </ul>	<p>Records the following services:</p> <ul style="list-style-type: none"> <li> SMTP</li> <li> POP3/IMAP</li> <li> HTTP/HTTPS</li> <li> Web-Based Email</li> <li> FTP</li> <li> TELNET</li> <li> Web POP3</li> <li> Web SMTP</li> <li> Instant Messaging</li> </ul>