IMbrella
Version Overview

Deerfield.com
4241 Old 27 South
Gaylord, MI 49735
800.599.8856
sales@deerfield.com
http://www.deerfield.com

IMbrella Software Version Overview

Organizations seeking to manage instant messaging on their networks have essentially three choices:

- Program a proxy server and reconfigure every IM client
- Buy an expensive IM gateway appliance
- Install the IMbrella solution that meets your needs

Proxy servers and appliances require costly IT resources and create single points of failure. Neither qualifies as economical choices for secure instant messaging in small and medium sized organizations.

IMbrella is a superior choice for secure instant messaging. Easily deployed, IMbrella installs on any PC with access to your network and analyzes all traffic to detect, manage and archive IM.

IMbrella is invisible to your employees and **requires no extra hardware**, client applications or desktop maintenance. **Flexible licensing** allows you to add as few or as many features as you wish.

This "Version Overview" will outline the basic differences of the IMbrella license stratifications.

Additional IMbrella information is available from the IMbrella web site.

IMbrella Blocker

Using IMbrella Blocker

To start using IMbrella Blocker, first make sure that IMbrella is monitoring the conversations of the PCs that you have selected. **DO NOT TURN ON BLOCKING YET.**

Verify that IMbrella is monitoring by clicking on the **LIVE MESSAGES** button:

You will see messages that just occurred. You can refresh this by clicking on the **REFRESH** button.

Next click on the **BLOCK USER** icon:

And you will be prompted with a screen to turn block ALL IM. Check the item **Block All Instant Messaging** and click **Save**. The PCs that are managed by IMbrella will no longer be allowed to do instant messaging.

How does IMbrella Blocker work? Why is it better than just shutting down IM ports or using other methods?

IMbrella Blocker blocks all of your Instant Messaging using the following technologies: If the IM packet contains the signature for instant messaging, the TCP/IP connection is immediately "reset". Each type of IM system (AOL, MSN, Yahoo!, etc.) has its own signature within the TCP/IP byte stream. IMbrella watches for these signatures and immediately terminates the connection.

If you attempt to shut down instant messaging by shutting off ports normally associated with AOL, MSN, etc., the AOL/MSN/etc. client will attempt to bypass that port and conduct the IM conversation over another port, such as the HTTP port (port 80).

If you attempt to shut down instant messaging by prohibit access to the URL associated with the servers that process AOL, MSN, etc., there are many well-known tricks to get around referencing that URL.

IMbrella GateKeeper

Using IMbrella GateKeeper

To start using IMbrella GateKeeper, first make sure that IMbrella is monitoring the conversations of the PCs that you have selected. **DO NOT TURN ON GATEKEEPING YET.**

Verify that IMbrella is monitoring by clicking on the **LIVE MESSAGES** button:

You will see messages that just occurred. You can refresh this by clicking on the **REFRESH** button.

Next click on the **GATEKEEPER** icon:

You will be prompted with a screen to **Enable Gatekeeper - Control who can use Instant Messaging**. Check the item **Enable GateKeeper** . Select users that you want to **ALLOW** or **BLOCK** from instant messaging, and click **Save**.

You can also schedule the days and hours you want to allow Instant Messaging for users who are blocked. Select **Block / Schedule IM Usage**, and click on the days when IM is allowed, and specify the time period when it is allowed, then click **Save**.

The PCs that are managed by IMbrella will no longer be allowed to do instant messaging unless the user (based on Instant Message screen name) was set to ALLOW, or the time is during one of the time periods you permit.

How does IMbrella GateKeeper work? Why is it better than just shutting down IM ports or using other methods?

IMbrella Blocker blocks all of your Instant Messaging using the following technologies:

Each type of IM system (AOL, MSN, Yahoo!, etc.) has its own signature within the TCP/IP byte stream. IMbrella uses this signature to determine if it's an instant message. If the IM packet contains the signature for instant messaging, then the day & time is checked. If it is in the permissible time period, the IM conversation is permitted to occur.

If it is NOT in the permissible time period, the user's Instant Message address (screen name) is checked for ALLOW vs. BLOCK. If it is set as BLOCK, the TCP/IP connection is immediately "reset", which terminates the login and prevents the instant message conversation from occurring.

If you attempt to shut down instant messaging by shutting off ports normally associated with AOL, MSN, etc., the AOL/MSN/etc. client will attempt to bypass that port and conduct the IM conversation over another port, such as the HTTP port (port 80).

If you attempt to shut down instant messaging by prohibit access to the URL associated with the servers that process AOL, MSN, etc., there are many well-known tricks to get around referencing that URL.

IMbrella Blocker Plus

Using IMbrella Blocker Plus

To start using IMbrella Blocker, first make sure that IMbrella is monitoring the conversations of the PCs that you have selected. **DO NOT TURN ON BLOCKING YET.**

Verify that IMbrella is monitoring by clicking on the **LIVE MESSAGES** button:

You will see messages that just occurred. You can refresh this by clicking on the **REFRESH** button.

Next click on the **BLOCK** icon:

And you will be prompted with a screen to turn block ALL IM. Check the item **Block All Instant Messaging**.

Next select the menu item **Block / Schedule IM Usage** and click on the days when IM is allowed, and specify the time period when it is allowed, then click **Save**.

The PCs that are managed by IMbrella will no longer be allowed to do instant messaging except for the time you specified.

How does IMbrella Blocker Plus work? Why is it better than just shutting down IM ports or using other methods?

IMbrella Blocker blocks all of your Instant Messaging using the following technologies:

If the IM packet contains the signature for instant messaging, then the day & time is checked. If it is NOT in the permissible time period, the TCP/IP connection is immediately "reset". Each type of IM system (AOL, MSN, Yahoo!, etc.) has its own signature within the TCP/IP byte stream. IMbrella watches for these signatures and immediately terminates the connection.

If you attempt to shut down instant messaging by shutting off ports normally associated with AOL, MSN, etc., the AOL/MSN/etc. client will attempt to bypass that port and conduct the IM conversation over another port, such as the HTTP port (port 80).

If you attempt to shut down instant messaging by prohibit access to the URL associated with the servers that process AOL, MSN, etc., there are many well-known tricks to get around referencing that URL.

IMbrella Detector

Using IMbrella Detector

To start using IMbrella Detector, first make sure that IMbrella is monitoring the conversations of the PCs that you have selected.

Verify that IMbrella is monitoring by clicking on the **LIVE MESSAGES** button:

You will see messages that just occurred. You can refresh this by clicking on the **REFRESH** button.

Here's a quick guide to each of the items you can detect:

Users / Inhouse Users	**Who are my in-house users?**
Users / External Contacts	**Who are the contacts my in-house users communicate with?**
Users / Aliases	**Which users have more than one Instant Message address (screen name)?**
Users / Watch List	**Which users are causing violations such as Excessive Usage or Inappropriate Content?**
Stats / Overall Usage Chart	**How much overall time is being spent instant messaging?**

Stats / Top User Chart	**Who are the most active in-house users, who are the most active contacts?**
Stats / Usage Per User	**How much time is each user spending?**
Stats / Hourly Usage	**Which times of day are instant messaging occurring most?**
Stats / Totals	**How much total activity (including file transfers and violations) is occurring?**
Stats / Master Summary Report	**Send an email showing: total activity, top users and hourly usage for a date range.**
Stats / Usage Report	**Send an email showing time spent by users for a date range.**
Stats / Excessive Usage	**Send an email showing excessive usage by users for a date range.**
Violations / Show Violations	**Whose instant messages contained inappropriate content, or spent excessive time instant messaging?**
Violations / Edit Blacklist Words	**Edit the list of words that are considered inappropriate. Each time one of these words occur in an instant message it adds the violation to the above report, and adds the user to the watch list.**
Violations / Usage Computation	**Sets the threshold for excessive usage.**

IMbrella Spotlight

Using IMbrella Spotlight

Once you start IMbrella Spotlight, it will begin capturing the screen names of all users who send and receive instant messages. Verify that IMbrella is monitoring messages by clicking on the Spotlight icon.

You will see the screen names (instant message addresses) of all of the users who are sending and receiving instant messages. If you do not see the screen name (or IP address or computer name) or the user you want to watch, it means that user has not yet sent or received a message.

Spotlight has the following major features:
What is the "spotlighted" user saying?
How much time is spent instant messaging?
To whom is the user talking?
Are they transferring files over instant messaging?

Selecting the user to spotlight

Click the Spotlight icon, and you will see a list of screen names. Select the user's screen name and click **Add to Spotlight**, then click **Save**.

IMbrella will begin saving all of that user's messages in the archive. You can see that user's recent messages by clicking on the Live View of Messages icon:

What is the "spotlighted" user saying?

Here's a quick guide to messages & conversations:

Conversations / Search Conversations	**Let me search all conversations based on in-house user, contact, date range and keyword. Then I will pick to either: -All messages that match the search criteria -A list of conversations between two people. Then I will select one of those conversations and view the messages within the conversation.**
Conversations / Live Messages	**I want to view the most recent 500 messages that have occurred.**
Conversations / Live Conversations	**I want to view the most recent conversations that have occurred. Then I will select one of the conversations to see the messages within the conversation.**
Conversations / Drill-down	**I want to see a list of in-house users and their contacts, and the dates of their conversations. Then I will select a date and see the messages in the conversation.**

How much time is spent instant messaging?

Here's a quick guide to determining usage:

Stats / Usage Per User	**How much time is each user spending?**
Stats / Hourly Usage	**Which time of day is instant messaging occurring most?**
Stats / Totals	**How much total activity (including file transfers and violations) is occurring?**
Stats / Usage Report	**Send an email showing time spent by users for a date range.**

To whom is the user talking?

Here's a quick guide to discovering whom the user is talking to:

Conversations	**All of the conversation screens show both participant names**
Users / External Contacts	**Who are the contacts my in-house users communicate with?**
Users / Aliases	**Which users have more than one Instant Message address (screen name)?**

Are they transferring any files over instant messaging?

Here's a quick guide to watching file transfers:

Stats / File Transfer Chart	**Shows each file transfer that occurred. To ensure that file transfers are being logged, click Block / File Transfer / Log.**

IMbrella Secure Enterprise Pro

Using IMbrella Secure Enterprise Pro

To start using IMbrella Secure Enterprise Pro, first make sure that IMbrella is monitoring the conversations of the PCs that you have selected.

Verify that IMbrella is monitoring by clicking on the **LIVE MESSAGES** button:

You will see messages that just occurred. You can refresh the list of messages by clicking the **REFRESH** button.

Secure Enterprise Pro has the following major features:
Detecting Usage
Watching and Searching messages & conversations
Restricting Instant Messaging

Detecting Usage

Here's a quick guide to each of the items you can detect:

Users / Inhouse Users	**Who are my in-house users?**

Users / External Contacts	**Who are the contacts my in-house users communicate with?**
Users / Aliases	**Which users have more than one Instant Message address (screen name)?**
Users / Watch List	**Which users are causing violations such as Excessive Usage or Inappropriate Content?**
Stats / Overall Usage Chart	**How much overall time is being spent instant messaging?**
Stats / Top User Chart	**Who are the most active in-house users, who are the most active contacts?**
Stats / Usage Per User	**How much time is each user spending?**
Stats / Hourly Usage	**Which times of day are instant messaging occurring most?**
Stats / Totals	**How much total activity (including file transfers and violations) is occurring?**
Stats / Master Summary Report	**Send an email showing: total activity, top users and hourly usage for a date range.**
Stats / Usage Report	**Send an email showing time spent by users for a date range.**
Stats / Excessive Usage	**Send an email showing excessive usage by users for a date range.**
Violations / Show Violations	**Whose instant messages contained inappropriate content, or spent excessive time instant messaging?**
Violations / Edit Blacklist Words	**Edit the list of words that are considered inappropriate. Each time one of these words occur in an instant message it adds the violation to the above report, and adds the user to the watch list.**
Violations / Usage Computation	**Sets the threshold for excessive usage.**

Watching and Searching Messages & Conversations

Here's a quick guide to messages & conversations:

Conversations / Search Conversations	**Let me search all conversations based on inhouse user, contact, date range and keyword. Then I will pick to either:** **-All messages that match the search criteria** **-A list of conversations between two people** **Then I will select one of those conversations and view the messages within the conversation.**
Conversations / Live Messages	**I want to view the most recent 500 messages that have occurred.**
Conversations / Live Conversations	**I want to view the most recent conversations that have occurred. Then I will select one of the conversations to see the messages within the conversation.**

Conversations / Drill-down	**I want to see a list of inhouse users and their contacts, and the dates of their conversations. Then I will select a date and see the messages in the conversation.**
Violations / Scan for blacklisted words	**I want to see how often blacklisted words have been used in the conversations that were already recorded.**

Restricting Instant Messaging

Here's a quick guide to restricting instant messaging:

Restrict Instant Messaging by Instant Message address (screen name)	**Select Block / GateKeeper. You will be prompted with a screen to Enable Gatekeeper - Control who can use Instant Messaging. Check the item Enable Gatekeeper. Then select the users that you want to ALLOW or BLOCK, and click Save.** **The PCs that are managed by IMbrella will no longer be allowed to do instant messaging unless that user's screen name is listed as ALLOW.**
Restrict Instant Messaging by day of week or time of day	**Follow above instructions, and then select Block / Schedule IM Usage. Select the days and hours you want to allow Instant Messaging.** **The PCs that are managed by IMbrella will no longer be allowed to do instant messaging unless the user (based on Instant Message screen name) was set to ALLOW, or the time is during one of the time periods you permit.**
Restrict Web-based Instant Messaging	**Select Block / Block web-based IM. Click the Download from IMbrella button to get a list of URLs commonly associated with web browser IM. You can add more URLs. Click Save.**
Restrict File Transfers	**Select Block / Block File Transfer Click Block all file transfers. Click Save.**

Using the Remote Console

1. Ensure that you are using the IMbrella with the SQL database, not the default database.
2. Install a copy of the Remote IMbrella software on the compliance officer's (or HR manager's) desktop.
3. Specify the SQL Server, username and password to allow access to view conversations, violations and usage statistics.

IMbrella Secure Enterprise / Compliance

Using IMbrella Compliance Enterprise

To start using IMbrella Compliance Enterprise, first make sure that IMbrella is monitoring the conversations of the PCs that you have selected.

Verify that IMbrella is monitoring by clicking on the **LIVE MESSAGES** button:

You will see messages that just occurred. You can refresh the list of messages by clicking the **REFRESH** button.

Compliance Enterprise has the following major features:
Detecting Usage
Watching and Searching messages & conversations
Restricting Instant Messaging
Archiving the database and accessing old archives
Using the Remote Console

Detecting Usage

Here's a quick guide to each of the items you can detect:

Users / Inhouse Users	**Who are my in-house users?**
Users / External Contacts	**Who are the contacts my in-house users communicate with?**
Users / Aliases	**Which users have more than one Instant Message address (screen name)?**
Users / Watch List	**Which users are causing violations such as Excessive Usage or Inappropriate Content?**
Stats / Overall Usage Chart	**How much overall time is being spent instant messaging?**
Stats / Top User Chart	**Who are the most active in-house users, who are the most active contacts?**
Stats / Usage Per User	**How much time is each user spending?**
Stats / Hourly Usage	**Which times of day are instant messaging occurring most?**
Stats / Totals	**How much total activity (including file transfers and violations) is occurring?**
Stats / Master Summary Report	**Send an email showing: total activity, top users and hourly usage for a date range.**
Stats / Usage Report	**Send an email showing time spent by users for a date range.**

Stats / Excessive Usage	**Send an email showing excessive usage by users for a date range.**
Violations / Show Violations	**Whose instant messages contained inappropriate content, or spent excessive time instant messaging?**
Violations / Edit Blacklist Words	**Edit the list of words that are considered inappropriate. Each time one of these words occur in an instant message it adds the violation to the above report, and adds the user to the watch list.**
Violations / Usage Computation	**Sets the threshold for excessive usage.**

Watching and Searching Messages & Conversations

Here's a quick guide to messages & conversations:

Conversations / Search Conversations	**Let me search all conversations based on inhouse user, contact, date range and keyword. Then I will pick to either:** **-All messages that match the search criteria** **-A list of conversations between two people** **Then I will select one of those conversations and view the messages within the conversation.**
Conversations / Live Messages	**I want to view the most recent 500 messages that have occurred.**
Conversations / Live Conversations	**I want to view the most recent conversations that have occurred. Then I will select one of the conversations to see the messages within the conversation.**
Conversations / Drill-down	**I want to see a list of inhouse users and their contacts, and the dates of their conversations. Then I will select a date and see the messages in the conversation.**
Violations / Scan for blacklisted words	**I want to see how often blacklisted words have been used in the conversations that were already recorded.**

Restricting Instant Messaging

Here's a quick guide to restricting instant messaging:

Restrict Instant Messaging by Instant Message address (screen name)	**Select Block / GateKeeper. You will be prompted with a screen to Enable Gatekeeper - Control who can use Instant Messaging. Check the item Enable Gatekeeper. Then select the users that you want to ALLOW or BLOCK, and click Save.** **The PCs that are managed by IMbrella will no longer be allowed to do instant messaging unless that user's screen name is listed as ALLOW.**
Restrict Instant	**Follow above instructions, and then select Block /**

Messaging by day of week or time of day	**Schedule IM Usage. Select the days and hours you want to allow Instant Messaging.** **The PCs that are managed by IMbrella will no longer be allowed to do instant messaging unless the user (based on Instant Message screen name) was set to ALLOW, or the time is during one of the time periods you permit.**
Restrict Web-based Instant Messaging	**Select Block / Block web-based IM. Click the Download from IMbrella button to get a list of URLs commonly associated with web browser IM. You can add more URLs. Click Save.**
Restrict File Transfers	**Select Block / Block File Transfer Click Block all file transfers. Click Save.**

Using the Remote Console

Ensure that you are using the IMbrella with the SQL database, not the default database.

Install a copy of the Remote IMbrella software on the compliance officer's (or HR manager's) desktop.

Specify the SQL Server, username and password to allow access to view conversations, violations and usage statistics.

Archiving the database and accessing old archives

Here's a quick guide to using archives:

Creating a backup CD	**Select Compliance / Archive to CD. Enter the path of the writable CD/DVD to store the archive and click Save. Then click either Archive All or Archive New. This process can be automated to occur every night.**
Exporting conversations to a 3rd party archiving system	**Select Compliance / Archive to Vault. Enter the template file that describes how the information will be properly formatted for the 3rd party archiving system, and the path where to deposit the resultant files (one conversation per file). Click Save, then either Archive All or Archive New. This process can be automated to occur every night.**
Purging the database	**Select Settings / Database Maintenance / Purge. Specify the age of the messages you wish to purge and click Purge. Old messages will be removed from the SQL database and written to a Microsoft Access database that can be imported at a later date, or accessed with the Archive Reader.**
Reading a previously created archive	**Select Settings / Database Maintenance / Open Archive. Specify the name of the previously created archive and**

	click Open. This will not affect IMbrella's recording of new messages - they will be stored in the active database, not the previously created archive.