Ethical Wall Guide

AVAILABLE IN 8.4 AND ABOVE

Overview

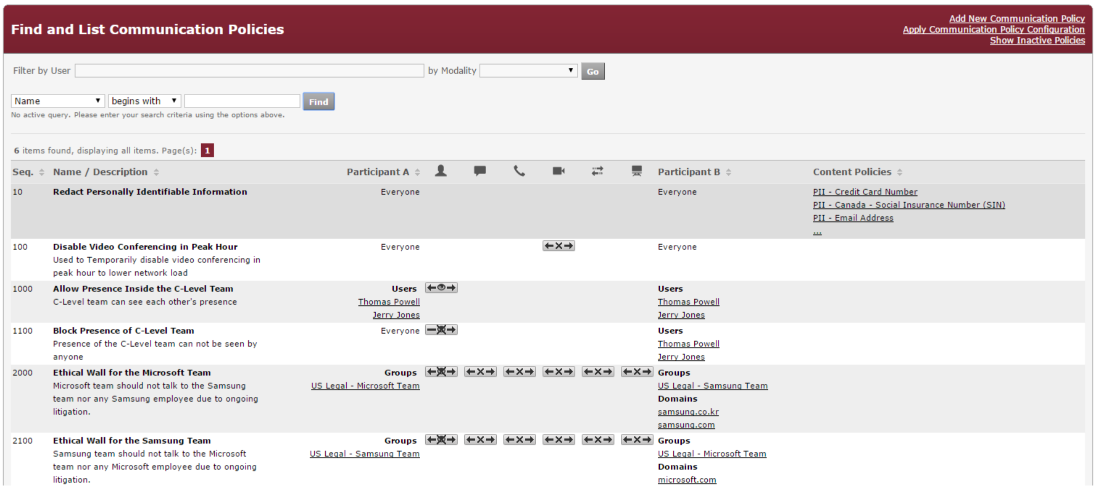
The guide explains the Verba Ethical Wall solution. It describes the design, configuration and administration of the solution.

The Verba Ethical Wall solution provides various control mechanisms for Unified Communications platforms.

Control mechanisms include:

- presence blocking - decide who can see whose presence information
- disclaimers - attach disclaimer messages to communications
- session blocking - block or warn different communication modes between various users /groups
- content filtering - filter messaging content based on your business requirements

You can configure all of the above as part of Communication Policies.



Find and List Communication Policies

Add New Communication Policy
Apply Communication Policy Configuration
Show Inactive Policies

Filter by User ______ by Modality ______ Go

Name ▼ begins with ▼ ______ Find

No active query. Please enter your search criteria using the options above.

6 items found, displaying all items. Page(s): 1

Seq.	Name / Description	Participant A	👤	💬	📞	📹	⇄	🖥	Participant B	Content Policies
10	**Redact Personally Identifiable Information**	Everyone							Everyone	PII - Credit Card Number PII - Canada - Social Insurance Number (SIN) PII - Email Address ...
100	**Disable Video Conferencing in Peak Hour** Used to Temporarily disable video conferencing in peak hour to lower network load	Everyone				←×→			Everyone	
1000	**Allow Presence Inside the C-Level Team** C-Level team can see each other's presence	**Users** Thomas Powell Jerry Jones	←👁→						**Users** Thomas Powell Jerry Jones	
1100	**Block Presence of C-Level Team** Presence of the C-Level team can not be seen by anyone	Everyone	–×→						**Users** Thomas Powell Jerry Jones	
2000	**Ethical Wall for the Microsoft Team** Microsoft team should not talk to the Samsung team nor any Samsung employee due to ongoing litigation.	**Groups** US Legal - Microsoft Team	←×→	←×→	←×→	←×→	←×→	←×→	**Groups** US Legal - Samsung Team **Domains** samsung.co.kr samsung.com	
2100	**Ethical Wall for the Samsung Team** Samsung team should not talk to the Microsoft team nor any Microsoft employee due to ongoing litigation.	**Groups** US Legal - Samsung Team	←×→	←×→	←×→	←×→	←×→	←×→	**Groups** US Legal - Microsoft Team **Domains** microsoft.com	

Supported Unified Communications Platforms

The solution supports all communication modes of both **Cisco Collaboration** products and **Skype for Business** (Lync).

Verba Support will assist you with further information about deployment and configuration details.

Who needs Ethical Walls?

Various industries require Ethical Walls. We have collected a set of use cases and examples.

Licensing the Verba Ethical Wall functionality

Verba Ethical Wall is an integral part of the Verba Recording System solution, and can be **licensed separately or combined with recording**. When combined with recording, your solution becomes **a complete legal compliance solution for Unified Communications**.

Please contact your Verba partner or Verba sales to obtain the necessary licenses or to request a pilot.

Ethical Wall usage examples

Where are Ethical Walls used?

You can use Communication Policies for various purposes. Using Ethical Walls helps you fulfill requirements of:

- Legal compliance
- Avoiding conflict of interests
- Data leakage protection
- Workplace policies and procedures

Various industries use Ethical walls for multiple business scenarios.

Industry/Scenario	Use cases
Investment Banking	• Separating advisory and brokering departments • Protect the firm from insider trading liabilities • Title V of the Sarbanes-Oxley Act strengthens Ethical Wall requirements
Corporate Finance/Financial Services/Accountancies	• Separating client teams of competitors
Law firms	• Separating legal teams of potentially adverse parties
Journalism	• Separate Editorial and Advertising arms
IT/Security	• Avoiding copyright infringements / clean room designs • Avoiding information leakage
Enterprise Procurement	• Separate internal teams from vendors
Union Regulations	• Presence blocking requirements

and more…

Here we are listing a couple of usage examples.

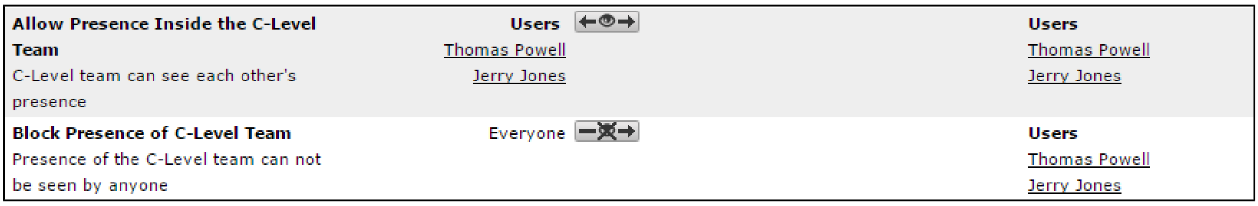
Blocking Presence of the C-Level Team

In case your management team would like to block their presence, you can create two policies:

- a higher priority (lower sequence number) policy that explicitly allows presence withing the C-Level team
- a lower priority (higher sequence number) policy that blocks their presence to the rest of the world

In this case, you can define the C-Level team either by naming the individual users (as below) or by creating a Group and referring to that Group.

See how this is presented in the Communication Policy list:



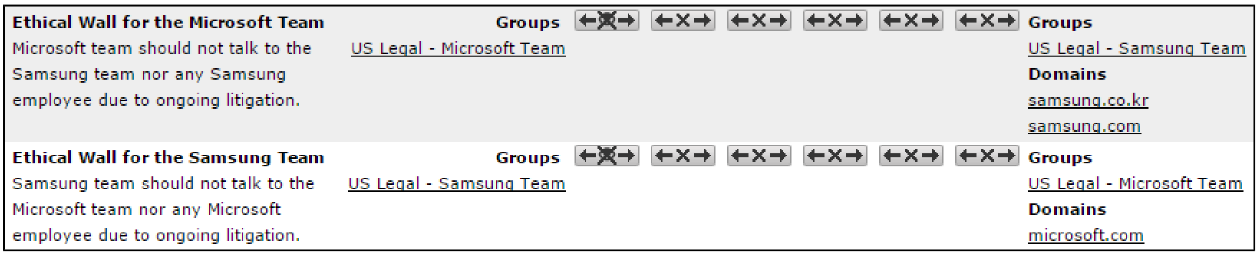
Allow Presence Inside the C-Level Team C-Level team can see each other's presence	**Users** Thomas Powell Jerry Jones	←👁→	**Users** Thomas Powell Jerry Jones
Block Presence of C-Level Team Presence of the C-Level team can not be seen by anyone	Everyone	←✕→	**Users** Thomas Powell Jerry Jones

Ethical Wall to avoid conflict of interest

In case you have two teams inside the company that should not communicate with each other, you can create block policies.

In the example below two policies are created, but you might also create this with a single policy.

See how this is presented in the Communication Policy list:

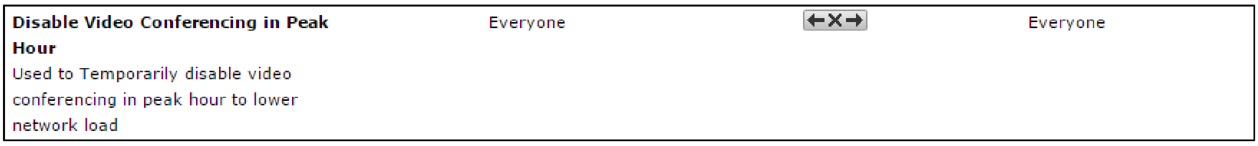


Ethical Wall for the Microsoft Team Microsoft team should not talk to the Samsung team nor any Samsung employee due to ongoing litigation.	**Groups** US Legal - Microsoft Team	←✕→ ←✕→ ←✕→ ←✕→ ←✕→ ←✕→	**Groups** US Legal - Samsung Team **Domains** samsung.co.kr samsung.com
Ethical Wall for the Samsung Team Samsung team should not talk to the Microsoft team nor any Microsoft employee due to ongoing litigation.	**Groups** US Legal - Samsung Team	←✕→ ←✕→ ←✕→ ←✕→ ←✕→ ←✕→	**Groups** US Legal - Microsoft Team **Domains** microsoft.com

Blocking video conferencing to avoid bandwidth problems

If you would like to stop your users from video conferencing (thus using a lot of bandwidth) during peak hour in your network, you can create a policy, which blocks video conversations. Such blocking might be useful in case of e.g. extreme weather when a majority of your users stay at home and might overload your VPN solution.

See how this is presented in the Communication Policy list:



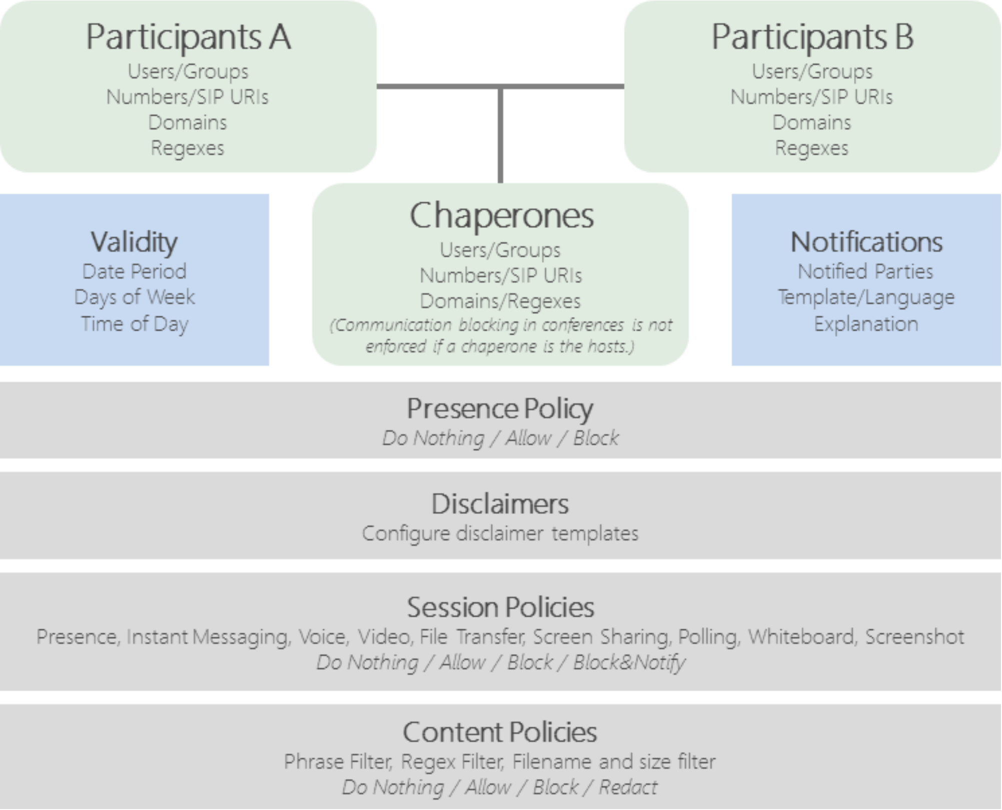
Disable Video Conferencing in Peak Hour Used to Temporarily disable video conferencing in peak hour to lower network load	Everyone	←✕→	Everyone

Communication Policies

Overview

Communication Policies are the foundation of your Ethical wall. Communication Policies define **if and how** Users and Groups can communicate with each other.

The following diagram summarizes parts of a Communication Policy:


Participants A
Users/Groups
Numbers/SIP URIs
Domains
Regexes
Participants B
Users/Groups
Numbers/SIP URIs
Domains
Regexes
Validity
Date Period
Days of Week
Time of Day
Chaperones
Users/Groups
Numbers/SIP URIs
Domains/Regexes
(Communication blocking in conferences is not enforced if a chaperone is the hosts.)
Notifications
Notified Parties
Template/Language
Explanation
Presence Policy
Do Nothing / Allow / Block
Disclaimers
Configure disclaimer templates
Session Policies
Presence, Instant Messaging, Voice, Video, File Transfer, Screen Sharing, Polling, Whiteboard, Screenshot
Do Nothing / Allow / Block / Block&Notify
Content Policies
Phrase Filter, Regex Filter, Filename and size filter
Do Nothing / Allow / Block / Redact

✓ The Chaperones feature is available from **Verba release 8.9**

For more details see Manage Communication Policies.

For information about different parts of a Communication Policy, see

- Presence Policy
- Disclaimers
- Session Policies
- Content Policies

Participants

Policies are defined between **Participant A** and **Participant B** groups. These are defined by combinations of

- **Extensions** - Phone numbers and SIP URIs
- **Users** - Individually with one or more extensions
- **Groups** - Groups of one or more users
- **Addresses** - Phone numbers, SIP URIs
- **Domains** - SIP domains
- **Regular Expressions** - number and SIP URI patterns

All **Users/Groups/Extensions** can be synchronized from Active Directory.

ⓘ Extension, User and Group selection for Session and Content Policies is not available with Starter User licenses, only with full Ethical Wall User licenses.
With Starter licenses the Session and Content Policies can only be defined for all employees.

Communication Modalities

It is possible to monitor and block multiple **modalities**:

- **Presence**
- **Instant Messaging**
- **Voice**
- **Video**
- **File Transfer**
- **Screen Sharing**
- **Data Share in Conference (Lync/SfB only)**

ⓘ The following Lync/SfB actions are viewed as Data Share: Power Point share, Whiteboard, Polling, Q&A, OneNote share, Program share

You can set the policies so that only Participant A can contact Participant B, and not the other way around, or you can block the communication both ways.

List Communication Policies

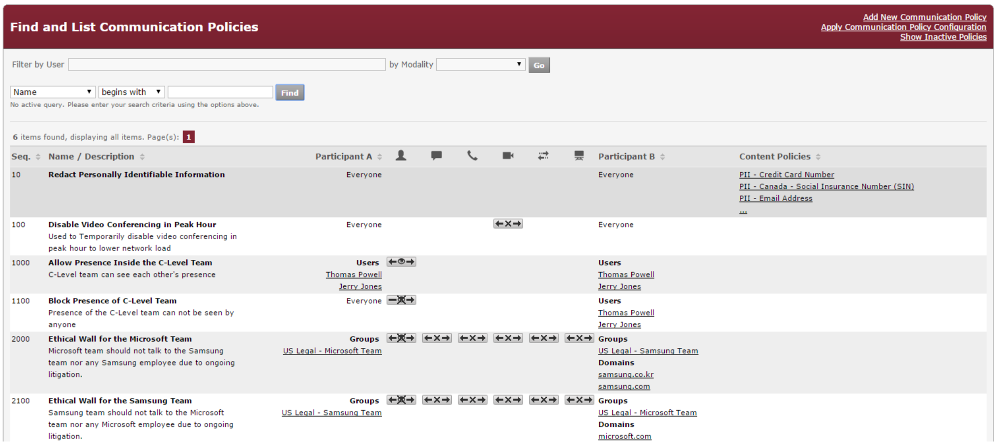
Search or List Communication Policies

To view the configured communication policies, navigate to the Communication Policies in the Verba web interface **Policies > Communication Policies**.

The list displays the following information about each search phrase

- **Sequence -** The policies will be evaluated one by one based on the sequence number assigned to them. The evaluation starts with the lowest sequence number and goes in ascending order. If there is a block or an explicit allow action defined for the certain action in a policy, then the engine stops, no other policies will be evaluated.
- **Name/Description -** Description of the policy, it is used by the administrators to search the database.
- **Participant A/B -** Party A and Party B between whom the given policy will be enforced.
- **Content Policies -** Content policies assigned to the given communication policy. For more information see Content Policies.
- **Channels -** Shows if a certain policy enforces this type of communication
  👤
  Presence - Shows if the presence of party A/B is visible to the other party
  💬
  IM - Shows if Party A and B can send instant messages to each other
  📞
  Voice - Shows if Party A and B can communicate with each other via voice channels
  📹
  Video - Shows if Party A and B can use video calling to contact each other
  ⇄
  File Transfer - Shows if Party A and B can send files to each other
  🖥
  Screen sharing - Shows if Party A and B can use screen sharing
  ↪
  Data share (Conference) - For Skype for Business (Lync) there is the option to restrict the use of Polls, Whiteboards, Power Point presentations, OneNote note sharing and File attachments in conferences

> ⓘ When the policies are evaluated in the order of the sequence numbers, the decision about the given connection will be made by the first policy that matches the criteria of that connection.
> For example if you have two rules:
> *#1 John Doe can send instant messages to Jane Small (Sequence number 10)*
> *#2 John Doe can NOT send instant messages to anyone (Sequence number 20)*
> In this case, John Doe will be able to send messages to Jane Small, because the decision is made when the first policy is evaluated, which is to let the message through.



Find and List Communication Policies

Add New Communication Policy
Apply Communication Policy Configuration
Show Inactive Policies

Filter by User by Modality Go

Name ▾ begins with ▾ Find

No active query. Please enter your search criteria using the options above.

6 items found, displaying all items. Page(s): 1

Seq.	Name / Description	Participant A	👤	💬	☎	🎥	⇄	🖥	Participant B	Content Policies
10	**Redact Personally Identifiable Information**	Everyone							Everyone	PII - Credit Card Number PII - Canada - Social Insurance Number (SIN) PII - Email Address ...
100	**Disable Video Conferencing in Peak Hour** Used to Temporarily disable video conferencing in peak hour to lower network load	Everyone				←×→			Everyone	
1000	**Allow Presence Inside the C-Level Team** C-Level team can see each other's presence	**Users** Thomas Powell Jerry Jones	←👁→						**Users** Thomas Powell Jerry Jones	
1100	**Block Presence of C-Level Team** Presence of the C-Level team can not be seen by anyone	Everyone	—×→						**Users** Thomas Powell Jerry Jones	
2000	**Ethical Wall for the Microsoft Team** Microsoft team should not talk to the Samsung team nor any Samsung employee due to ongoing litigation.	**Groups** US Legal - Microsoft Team	←×→	←×→	←×→	←×→	←×→	←×→	**Groups** US Legal - Samsung Team **Domains** samsung.co.kr samsung.com	
2100	**Ethical Wall for the Samsung Team** Samsung team should not talk to the Microsoft team nor any Microsoft employee due to ongoing litigation.	**Groups** US Legal - Samsung Team	←×→	←×→	←×→	←×→	←×→	←×→	**Groups** US Legal - Microsoft Team **Domains** microsoft.com	

Adding New Communication Policies

For more information refer to Manage Communication Policies

Show Inactive Policies

It is possible to activate or de-activate a certain policy. You can do this via a checkbox on the page where you define a certain policy. To see how to do this, go to the Manage Communication Policies page.

Deactivating a policy means that you invalidate the policy, it will not be deleted, you can restore it anytime you want. Inactive policies do not show up by default when you list all policies.

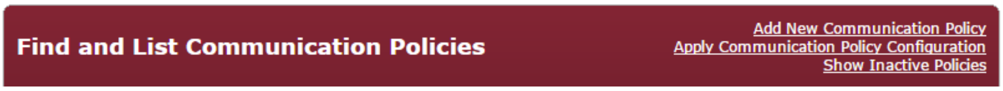
Clicking on the *Show Inactive Policies* button at the top right corner of the page, you can see all the records, including the inactive ones. After this the button changes to *Hide Inactive Policies*, and until you switch back to the default mode, you will be able to see the inactive ones.

Manage Communication Policies

Adding a new Communication policy

To add new communication policies navigate to the Communication Policies in the Verba web interface **Policies > Communication Policies.**

On the top right corner of the page click on *Add New Communication Policy* as shown on the image below:



Find and List Communication Policies

Add New Communication Policy
Apply Communication Policy Configuration
Show Inactive Policies

Defining a Communication Policy

The Communication Policy screen consists of multiple panels:

- Communication Policy
- Validity
- Participants
- Chaperones
- Presence Policies
- Presence blocking
- Contact List blocking
- Session Policies
- Content Policies
- Notifications
- Disclaimers

Communication Policy

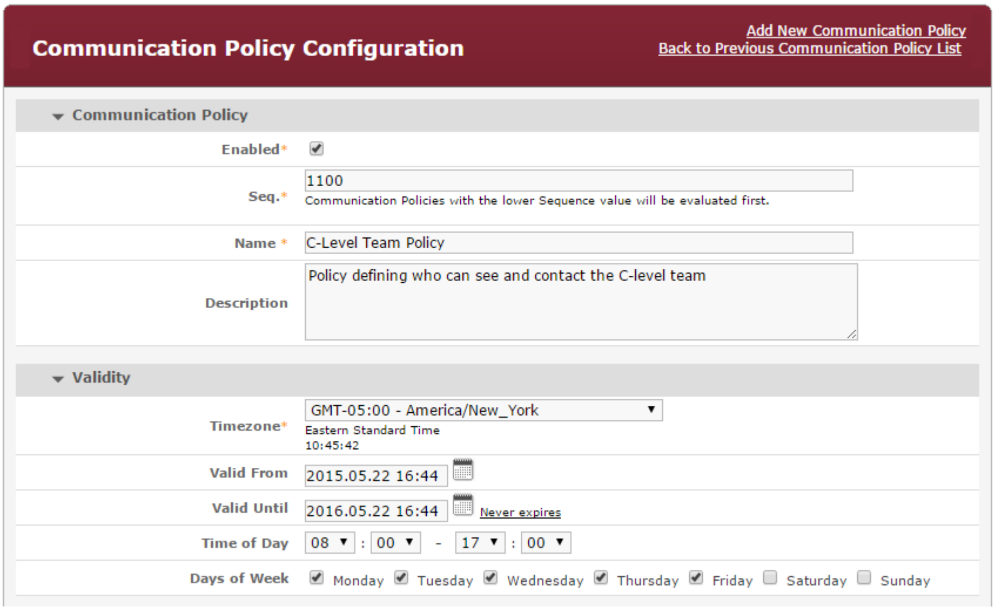
- **Enabled** - If set, then the policy is active, it will be evaluated by the engine
- **Sequence** - The policies will be evaluated one by one based on the sequence number assigned to them. The evaluation starts with the lowest sequence number and goes in ascending order.
- **Name** - You can set any name, only visible for policy administrators
- **Description** - Short description for the administrators to know what the policy does

Validity

You can specify when the policy should be evaluated and when it is not.
You can leave this block empty - and all days of the week checked - in that case, the policy will always be evaluated by the engine. (This is the default setting)

- **Time Zone** - Your time zone (Needs to be set, because the Verba servers may reside in another time zone, based on your system topology)
- **Valid From-Until** - You can set the exact dates, or you can click on *Never expires*
- **Time of Day** - You can set when it should be active every day
- **Days of Week** - The policy will be active on these days every week

In the example shown below, this policy will only be evaluated from 2015.05.22 to 2016.05.22,
every workday from 8:00 to 17:00. (Outside of this period the engine will skip this policy)



Communication Policy Configuration

Add New Communication Policy
Back to Previous Communication Policy List

▾ Communication Policy

Enabled*	☑
Seq.*	1100 Communication Policies with the lower Sequence value will be evaluated first.
Name *	C-Level Team Policy
Description	Policy defining who can see and contact the C-level team

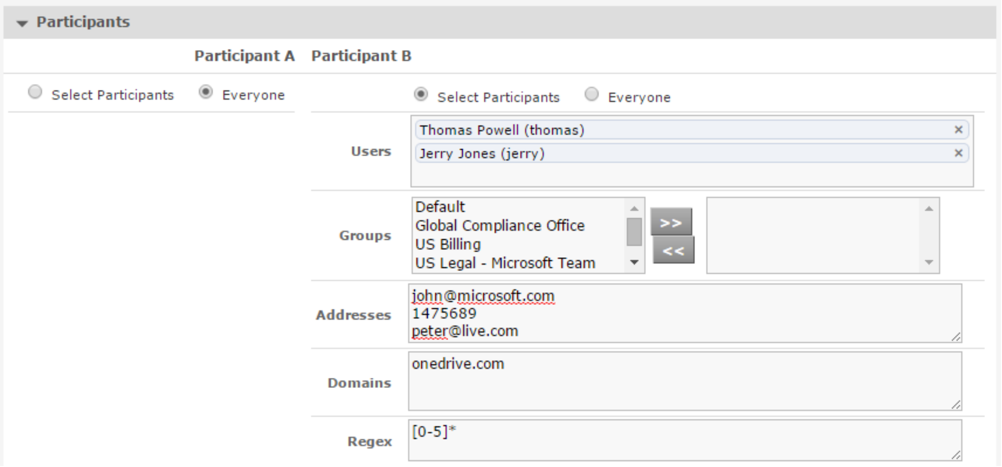
▾ Validity

Timezone*	GMT-05:00 - America/New_York ▾ Eastern Standard Time 10:45:42
Valid From	2015.05.22 16:44
Valid Until	2016.05.22 16:44 Never expires
Time of Day	08 ▾ : 00 ▾ - 17 ▾ : 00 ▾
Days of Week	☑ Monday ☑ Tuesday ☑ Wednesday ☑ Thursday ☑ Friday □ Saturday □ Sunday

Participants

You can define **Participant A** and **B** here.

- **Users** - To select **Users** start typing their name, and a drop-down list will appear with the available options.
- **Groups** - To include **Groups**, move them from the left pane (all groups in the system) to the right pane (selected groups) with the **>>** button. To delete the selection, use the **<<** button.
- **Addresses** - You can define any **Phone number** or **SIP URI** here, even if it is not present in the Verba system (Outside phone numbers, calls coming from the PSTN network, for instance)
- **Domains** - Ability to set a **specific domain** (For example in the case of federated calls you want to block calls to the microsoft.com domain)
- **Regex** - Standard Regular Expressions



▾ Participants

Participant A: ○ Select Participants ● Everyone

Participant B: ● Select Participants ○ Everyone

Users	Thomas Powell (thomas) × Jerry Jones (jerry) ×
Groups	Default Global Compliance Office US Billing US Legal - Microsoft Team >> <<
Addresses	john@microsoft.com 1475689 peter@live.com
Domains	onedrive.com
Regex	[0-5]*

ⓘ Extension, User and Group selection for Session and Content Policies is not available with Starter User licenses, only with full Ethical Wall User licenses.
With Starter licenses the Session and Content Policies can only be defined for all employees.

Chaperones

Under Chaperones, you can define **Users** and **Groups** whose **presence in conferences enables all communication,** even those that would otherwise be blocked by this policy.
You can select Users and Groups the same way as in the case of Participants.

✓ The Chaperones feature is available from **Verba release 8.9**

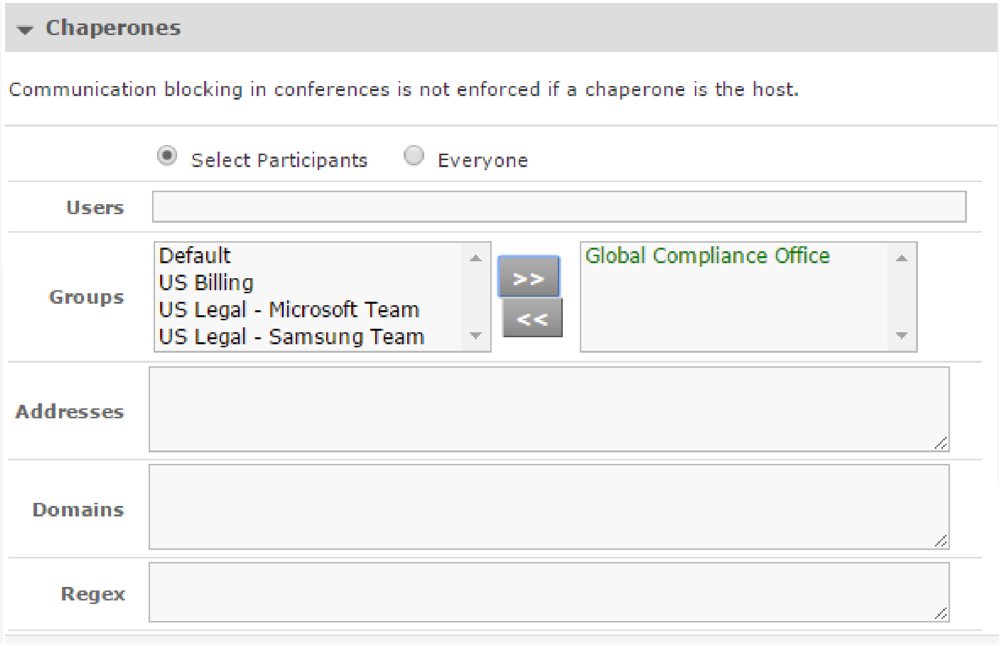
In the table below, the different modalities are shown per communication system and what modality can the chaperones feature be utilized with.

Cisco	Action allowed if Chaperone is present	Session terminated if Chaperone leaves
voice	No	No
video	No	No
IM	Yes	Yes
file transfer*	Not Applicable	Not Applicable
screen share	Yes	No

*The file transfer operation is not available in Cisco Jabber conferences.

SfB/Lync	Action allowed if Chaperone is present	Session terminated if Chaperone leaves
voice	Yes	Yes
video	Yes	Yes
IM	Yes	Yes
file transfer	No	No
screen share	Yes	Yes
content share	Yes	Yes

ⓘ In the example below, if Global Compliance Office is the host, then there is no restriction in communications between Participant A and B. (If this policy is evaluated)



Chaperones

Communication blocking in conferences is not enforced if a chaperone is the host.

● Select Participants ○ Everyone

Users:

Groups: Default, US Billing, US Legal - Microsoft Team, US Legal - Samsung Team → Global Compliance Office

Addresses:

Domains:

Regex:

Presence Policies

In the Verba Ethical Wall solution, Communication Policies include Presence Blocking and Contact List Blocking functionality.

Presence blocking

The presence status of users In Cisco Jabber and Lync/SfB clients can be hidden from other people. This means that users will always show up as offline for other users if their presence should not be shown.

Contact List blocking

When using the Contact List blocking functionality, users are not able to see specific blocked users in their SfB client when running searches for contacts. This means that the existence of certain users can be hidden from others.
Contact List blocking prevents adding blocked contacts to the contact list by default. Turning off the prevention will result that the user will able to add the remote user in possession of the remote user's full SIP URI.

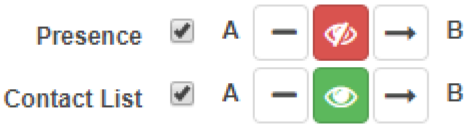
> ⓘ The Contact List blocking functionality is only available for Lync/SfB deployments. If the Contact List search goes through the Lync/SfB IIS contact list service.

You can set the presence or contact list blocking mode:

- **Block**
- **Allow** - used to explicitly allow presence even if lower priority rules would block presence between two users

You can also set the direction of the rule:

- Bidirectional between A and B
- A to B
- B to A



Presence ☑ A — → B

Contact List ☑ A — → B

Read more in the Presence Policies article.

Session Policies

In the Verba Ethical Wall solution, Communication Policies include Session Policy functionality.

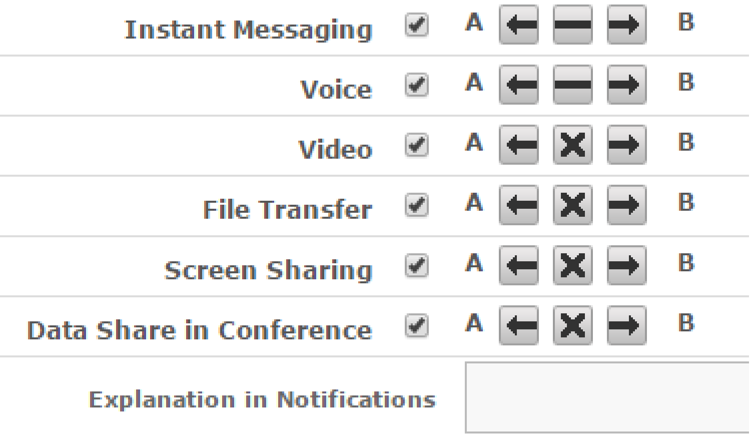
You can set session policy mode

- ✖ **Block**
- ❗ **Warn** - session will be allowed, but a notification will be sent
- ✖❗ **Block and Warn** - session will be blocked, and a notification will be sent
- — **Allow** - used to explicitly allow presence even if lower priority rules would block presence between two users

You can also set the direction of the rule:

- Bidirectional between A and B
- A to B
- B to A

The following example allows IM and voice calls, but blocks all other modalities between the Participant A and B groups:



Instant Messaging ☑ A ← — → B

Voice ☑ A ← — → B

Video ☑ A ← ✖ → B

File Transfer ☑ A ← ✖ → B

Screen Sharing ☑ A ← ✖ → B

Data Share in Conference ☑ A ← ✖ → B

Explanation in Notifications

> ⓘ Please note, that for conferences the direction of the session policies works in a different way. If they are set to bidirectional, then all communication will be blocked, even in conferences. If they are set in one direction, then that rule will not be evaluated for conferences.

Read more in the Session Policies article.

Content Policies

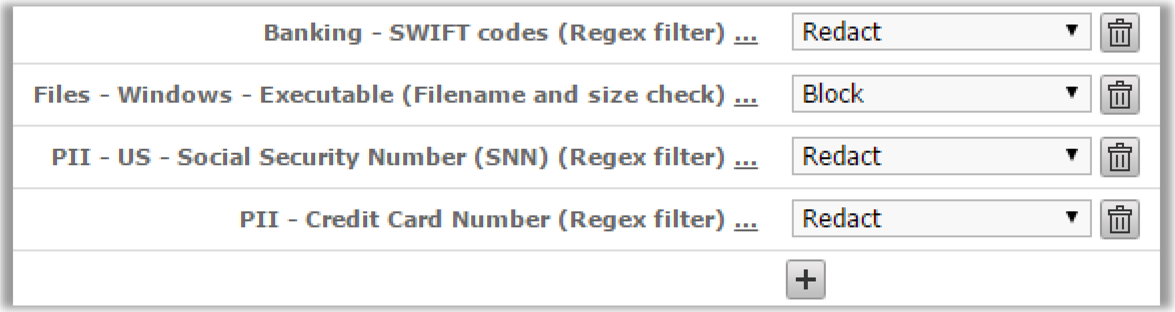
In the Verba Ethical Wall solution, Communication Policies include Content Policy functionality.

You can add **multiple Content Policies** to a Communication Policy.

Content policy actions include

- **Block**
- **Notify** - message will be allowed, but a notification will be sent
- **Redact** - allow the communication, but redact/edit the message to mask the matching information

An example list of Content Policies set on a Communication Policy:



Banking - SWIFT codes (Regex filter) ...	Redact
Files - Windows - Executable (Filename and size check) ...	Block
PII - US - Social Security Number (SNN) (Regex filter) ...	Redact
PII - Credit Card Number (Regex filter) ...	Redact

In the case of content policies, you can also set the direction in which you want the policies to take effect between Participant A and B (unidirectional or bidirectional).

To see how to manage and configure your Content Policies, read the List Content Policies and Manage Content Policies articles.

For the Content Policies to take effect, the IM session policy needs to be set (any setting)

Read more in the Content Policies article.

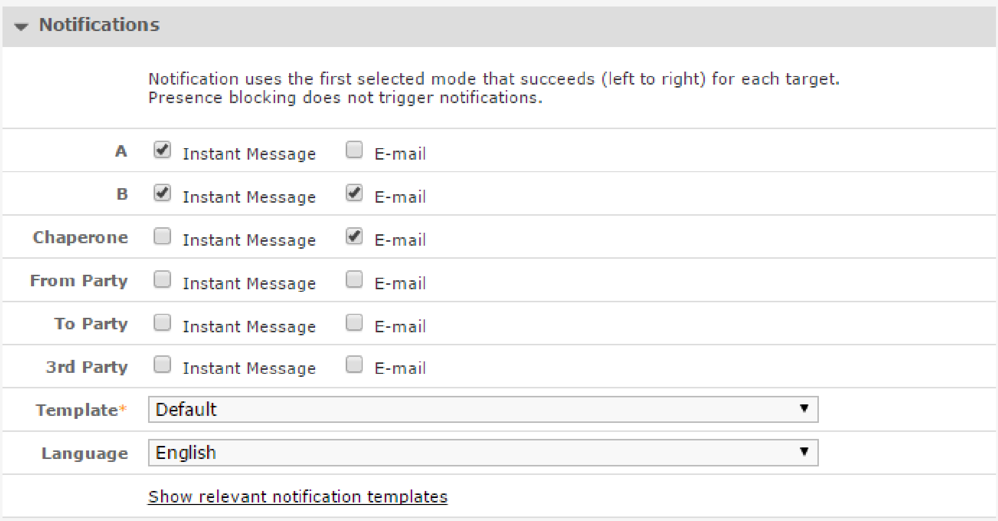
Notifications

As you can see in the *Session Policies* section, you can define for each modality if you want to send notifications when the given communication takes place.
Under the *Notifications* tab, you can set in what way notifications should be sent and to whom. If both IM and email notification are selected, then the email modality will only be used if an IM cannot be sent.

Possibilities include

- **A** - Participant A
- **B** - Participant B
- **Chaperone** - The Chaperone of this policy
- **From Party** - The party that started the call/initiated the action
- **To Party** - The Party that received the call/was the target of the action
- **3rd Party** - If you select this checkbox, you can set any email address or IM address to where the notifications should be sent

These settings only apply when this policy is evaluated and triggered by a conversation.
For example, you have two policies that apply to the same modalities and are
#1 Participant A is John Doe, under notifications only the instant message for Participant A is set (Sequence number 10)
#2 Participant A is John Doe, under notifications only the email message for Participant B is set (Sequence number 20)
In this case above an instant message will be sent to Participant A (John Doe), but no email will be sent to Participant B, as the first policy is evaluated only.



Notifications

Notification uses the first selected mode that succeeds (left to right) for each target.
Presence blocking does not trigger notifications.

A	☑ Instant Message	□ E-mail
B	☑ Instant Message	☑ E-mail
Chaperone	□ Instant Message	☑ E-mail
From Party	□ Instant Message	□ E-mail
To Party	□ Instant Message	□ E-mail
3rd Party	□ Instant Message	□ E-mail
Template*	Default ▼	
Language	English ▼	
	Show relevant notification templates	

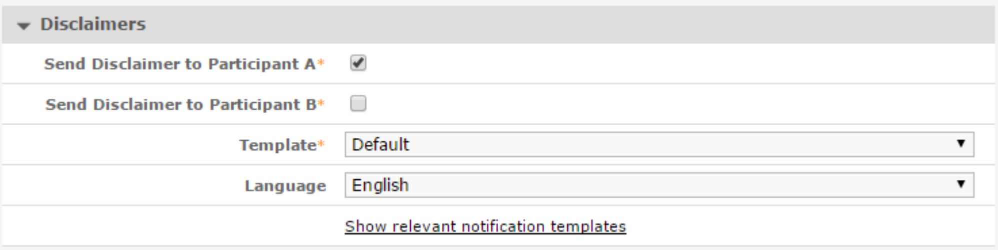
Select the Notification Template that you want to assign to this communication policy.

ⓘ The language of the notification will mainly be the **language of the user** that the notification is being sent to. This can be set for each user at the **user properties page.**
The language selection that you see here **defines a default language**, which applies when the notification template does not have messages defined in the language of the user.
In this case, the default language will be used.

Disclaimers

In the Verba Ethical Wall solution, Communication Policies include Disclaimer functionality.

You can set Disclaimer Templates to be attached to all Instant Message communications of various parties.



Disclaimers

Send Disclaimer to Participant A*	☑
Send Disclaimer to Participant B*	□
Template*	Default ▼
Language	English ▼
	Show relevant notification templates

Select the Disclaimer Template that you want to assign to this communication policy.

Presence Policies

Overview

In the Verba Ethical Wall solution, [Communication Policies](#) include Presence Blocking and Contact List Blocking functionality.

Presence blocking

The presence status of users In Cisco Jabber and Lync/SfB clients can be hidden from other people. This means that users will always show up as offline for other users if their presence should not be shown.

Contact List blocking

When using the Contact List blocking functionality, users are not able to see specific blocked users in their SfB client when running searches for contacts. This means that the existence of certain users can be hidden from others.
Contact List blocking prevents adding blocked contacts to the contact list by default. Turning off the prevention will result that the user will able to add the remote user in possession of the remote user's full SIP URI.

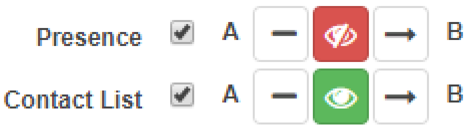
> ⓘ The Contact List blocking functionality is only available for Lync/SfB deployments. If the Contact List search goes through the Lync/SfB IIS contact list service.

You can set the presence or contact list blocking mode:

- **Block**
- **Allow** - used to explicitly allow presence even if lower priority rules would block presence between two users

You can also set the direction of the rule:

- Bidirectional between A and B
- A to B
- B to A



Presence ☑ A — → B

Contact List ☑ A — → B

Creating a Presence or Contact List Blocking Policy

In order to create a presence blocking policy:

Step 1 - Create a new [Communication Policy](#)

Step 2 - Configure the **Participant A** and **Participant B** groups

Step 3 - Configure the **Presence Blocking** category

Step 4 - Press **Save**

You can mix Presence Blocking with Disclaimers, Session Policies and Content Polices on the same Communication Policy.

Session Policies

Overview

In the Verba Ethical Wall solution, Communication Policies include Session Policy functionality.

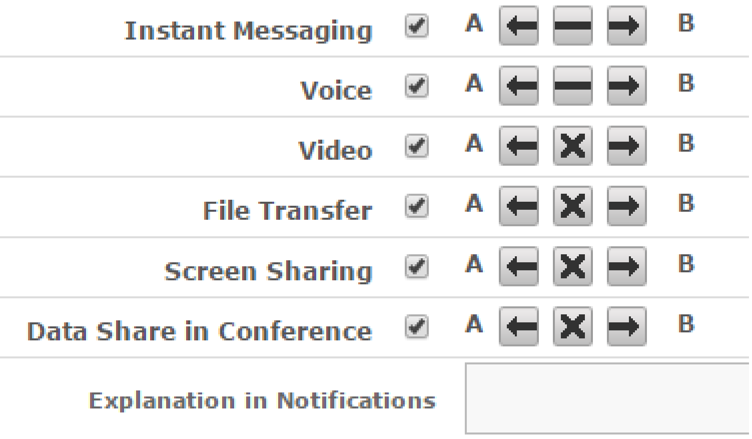
You can set session policy mode

- ✖ **Block**
- ! **Warn** - session will be allowed, but a notification will be sent
- ✖! **Block and Warn** - session will be blocked, and a notification will be sent
- ▬ **Allow** - used to explicitly allow presence even if lower priority rules would block presence between two users

You can also set the direction of the rule:

- Bidirectional between A and B
- A to B
- B to A

The following example allows IM and voice calls, but blocks all other modalities between the Participant A and B groups:



Instant Messaging	☑	A	←	▬	→	B
Voice	☑	A	←	▬	→	B
Video	☑	A	←	✖	→	B
File Transfer	☑	A	←	✖	→	B
Screen Sharing	☑	A	←	✖	→	B
Data Share in Conference	☑	A	←	✖	→	B

Explanation in Notifications

> ⓘ Please note, that for conferences the direction of the session policies works in a different way. If they are set to bidirectional, then all communication will be blocked, even in conferences. If they are set in one direction, then that rule will not be evaluated for conferences.

Creating a Session Policy

In order to create a session blocking policy:

Step 1 - Create a new Communication Policy

Step 2 - Configure the **Participants A** and **Participant B** groups

Step 3 - Configure the **Session Policy** category

Step 4 - Press **Save**

You can mix Session Policy with Presence Policies, Disclaimers and Content Polices on the same Communication Policy.

Platform and conference specific behaviour

Skype for Business (Lync)

File transfer refers to peer-to-peer file transfers.
In conferences Data Share applies to file and other application/content sharing.

ⓘ Please note, that if your Lync clients are set to automatically change the User's presence to Do Not Disturb when a Screen or Data Sharing session is established, then the Verba components will not be able to send out the Notifications to that party.

Cisco

In Cisco environments the Voice and Video modalities cannot be controlled separately, both of them define policies for the combined Voice&Video session.
Data Share is a Skype for Business/Lync specific modality, it is not used in Cisco deployments.
In conferences only the IM session policies take effect.

Disclaimers

Overview

In the Verba Ethical Wall solution, Communication Policies include Disclaimer functionality.

You can set Disclaimer Templates to be attached to all Instant Message communications of various parties.

Creating a Disclaimer

In order to create a presence blocking policy:

Step 1 - Create a new Communication Policy

Step 2 - Configure the **Participants A** and **Participant B** groups

Step 3 - Configure the **Disclaimers** category

Step 4 - Press **Save**

You can mix Presence Blocking with Presence Policies, Session Policies and Content Polices on the same Communication Policy.

Content Policies

Overview

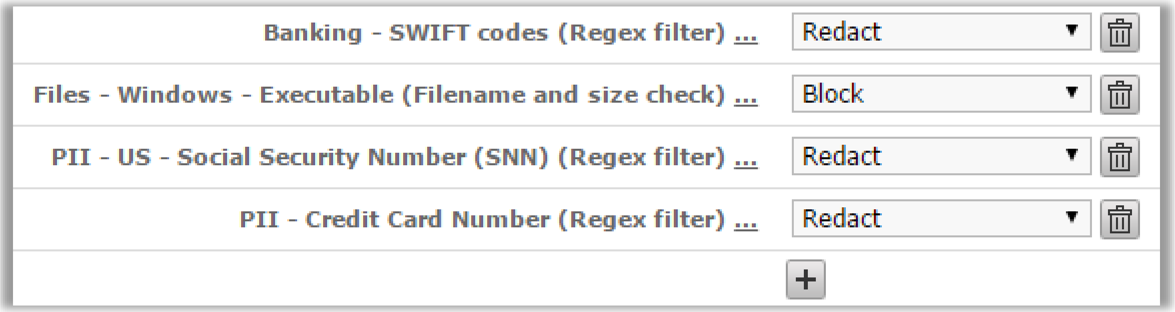
In the Verba Ethical Wall solution, Communication Policies include Content Policy functionality.

You can add **multiple Content Policies** to a Communication Policy.

Content policy actions include

- **Block**
- **Notify** - message will be allowed, but a notification will be sent
- **Redact** - allow the communication, but redact/edit the message to mask the matching information

An example list of Content Policies set on a Communication Policy:



Banking - SWIFT codes (Regex filter) ...	Redact ▼
Files - Windows - Executable (Filename and size check) ...	Block ▼
PII - US - Social Security Number (SNN) (Regex filter) ...	Redact ▼
PII - Credit Card Number (Regex filter) ...	Redact ▼

In the case of content policies, you can also set the direction in which you want the policies to take effect between Participant A and B (unidirectional or bidirectional).

To see how to manage and configure your Content Policies, read the List Content Policies and Manage Content Policies articles.

Assigning a Content Policy to a Communication Policy

In order to assign a Content Policy to a Communication Policy:

Step 1 - Create a new Communication Policy

Step 2 - Configure the **Participant A** and **Participant B** groups

Step 3 - Click on the button with the + (plus) sign

Step 4 - **Assign Content Policies** to your Communication Policy

Step 5 - Press **Save**

You can mix Content Policies with Presence Policies, Disclaimers and Session Policies on the same Communication Policy.

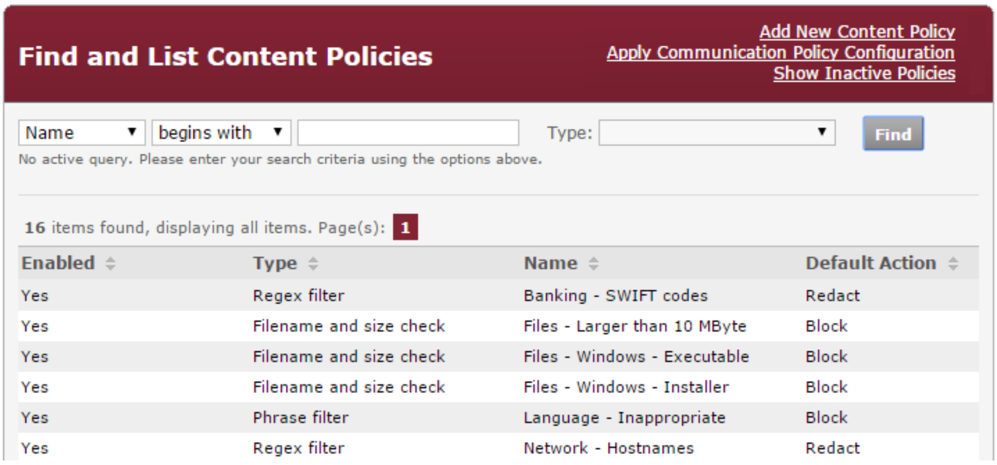
List Content Policies

Search of List Content Policies

To view the configured content policies, navigate to the Content Policies in the Verba web interface **Policies > Content Policies**.

The list displays the following information about each search phrase

- **Enabled** - Scroll down to the ***Show Inactive Policies*** **section** for more information
- **Type** - The three types are **Regex filter**, **Filename and size check** and **Phrase filter**
- **Name** - Information for the administrators, you can pick any name that you like.
- **Default Action** - If the policy activates, there are two available actions, **block the whole message**, or send the message but **redact the words** that are in violation of the policy.



Find and List Content Policies

No active query. Please enter your search criteria using the options above.

16 items found, displaying all items. Page(s): 1

Enabled	Type	Name	Default Action
Yes	Regex filter	Banking - SWIFT codes	Redact
Yes	Filename and size check	Files - Larger than 10 MByte	Block
Yes	Filename and size check	Files - Windows - Executable	Block
Yes	Filename and size check	Files - Windows - Installer	Block
Yes	Phrase filter	Language - Inappropriate	Block
Yes	Regex filter	Network - Hostnames	Redact

Adding New Content Policies

For more information refer to Manage Content Policies.

Show Inactive Policies

It is possible to activate or de-activate a certain policy. You can do this via a checkbox on the page where you define a certain policy. To see how to do this, go to the Manage Content Policies page.

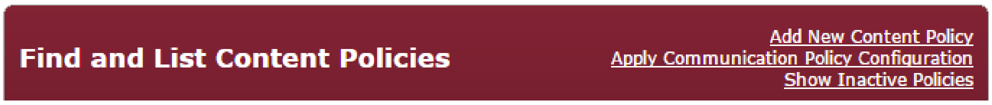
Deactivating a policy means that you invalidate the policy, it will not be deleted, you can restore it anytime you want.
Inactive policies do not show up by default when you list all policies.

Clicking on the *Show Inactive Policies* button at the top right corner of the page, you can see all the records, including the inactive ones. After this the button changes to *Hide Inactive Policies*, and until you switch back to the default mode, you will be able to see the inactive ones.

Manage Content Policies

Adding a new Content Policy

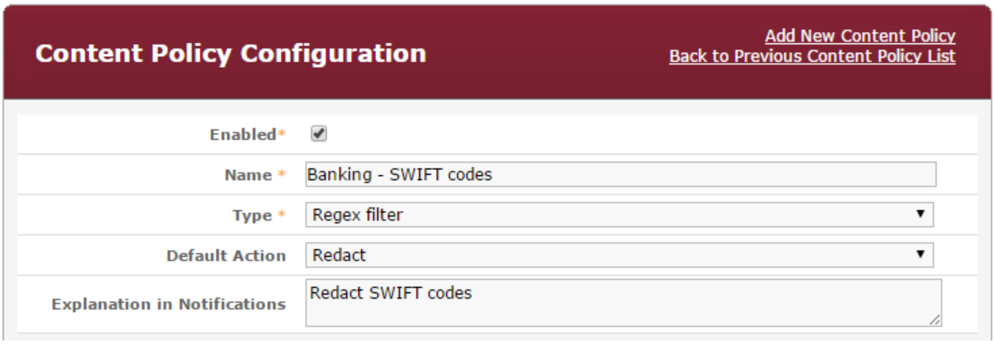
To add new content policies navigate to the Content Policies in the Verba web interface **Policies > Content Policies.**
On the top right corner of the page click on *Add New Content Policy* as shown on the image below


Find and List Content Policies
Add New Content Policy
Apply Communication Policy Configuration
Show Inactive Policies

Defining a Content Policy

Basic settings

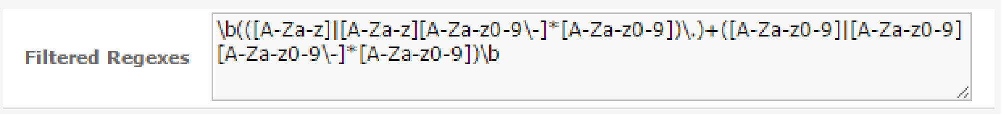
- **Enabled** - If set, then the policy is active, it will be evaluated by the engine
- **Type** - You can see the configuration of the **Regex filter**, **Filename and size check** and **Phrase filter**, at their respective sections down below
- **Default Action** - If the policy activates, there are two available actions, **block the whole message**, or send the message but **redact the words** that are in violation of the policy.
- **Explanation in Notifications** - To append this message to the notification message, use the *[rule-explanation]* tag in the Notification Templates.


Content Policy Configuration
Add New Content Policy
Back to Previous Content Policy List

Enabled*	☑
Name *	Banking - SWIFT codes
Type *	Regex filter ▼
Default Action	Redact ▼
Explanation in Notifications	Redact SWIFT codes

Regex Filter

Standard regular expressions to look for a pattern in the messages.

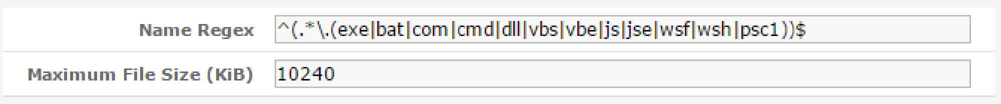


Filtered Regexes	\b(([A-Za-z]|[A-Za-z][A-Za-z0-9\-]*[A-Za-z0-9])\.)+([A-Za-z0-9]|[A-Za-z0-9][A-Za-z0-9\-]*[A-Za-z0-9])\b

To make sure that your Regular Expression matches the strings that you want it to, check it with a regexp tester first. You can find an online tool for this here: https://regex101.com/

Filename and size check

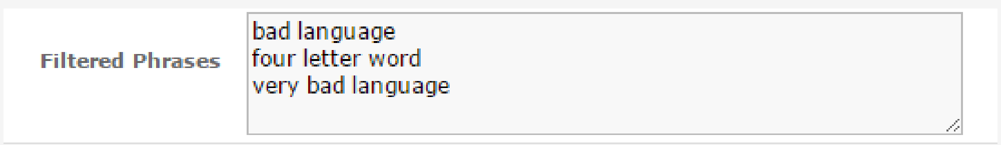
You can use regex for the name of the file, and you can define a maximum file size.
If the file is larger than the value defined here, the policy will trigger.



Name Regex	^(.*\.(exe|bat|com|cmd|dll|vbs|vbe|js|jse|wsf|wsh|psc1))$
Maximum File Size (KiB)	10240

Phrase Filter

Without the complexity of regular expressions, you can filter words and phrases.



Filtered Phrases

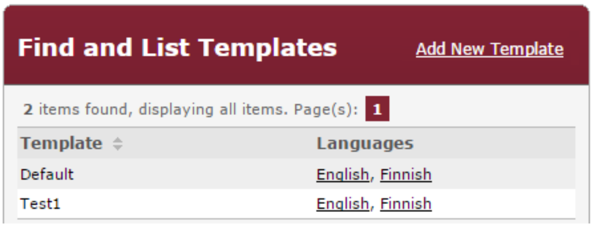
```
bad language
four letter word
very bad language
```

Notification Templates

Overview

The Verba Ethical wall solution can send notifications to the selected parties when a given communication channel is opened.
To see how you can define **when notifications are sent**, refer to the Session Policies article.

With Notification Templates, you can **define what messages** should be sent as notifications.
The see and manage Notification Templates, in the Verba web interface, navigate to **Policies > Notification Templates.**



Find and List Templates

Add New Template

2 items found, displaying all items. Page(s): 1

Template	Languages
Default	English, Finnish
Test1	English, Finnish

The steps to **define notification messages** for a certain Communication Policy are as follows

Step 1 - In the Verba web interface navigate to **Policies > Notification Templates**

Step 2 - Click on **Add New Template** at the top right corner of the page

Step 3 - Define the initial parameters for the template as shown in the ***Add New Template* section** below

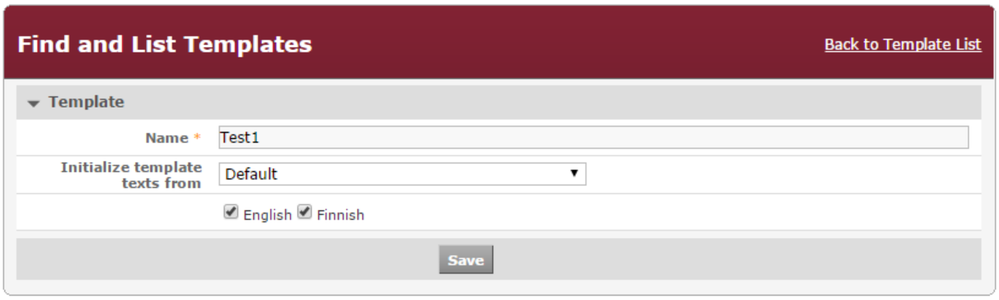
Step 4 - Define your policy as shown in the ***Define Your Template* section** below

Step 5 - **Assign** the Notification Template and the desired language to a Communication Policy as shown in Manage Communication Policies

Add New Template

To Add a New Notification Template, navigate to **Policies > Notification Templates** in the Verba web interface, then in the top right corner click on **Add New Template**.

- **Name** - The name is for administration purposes only, choose any that you like.
- **Initialize template texts** - To save time and effort, you can **import templates** that are already defined in your system. Using this, you only need to change the messages that are different.
- **Language** - Choose the languages that you want to use in this template. Here, the ones that are already defined in the system are shown. In the *Define your Template* section, you can see how you can add new languages.



Find and List Templates

Back to Template List

Template

Name * Test1

Initialize template texts from: Default

☑ English ☑ Finnish

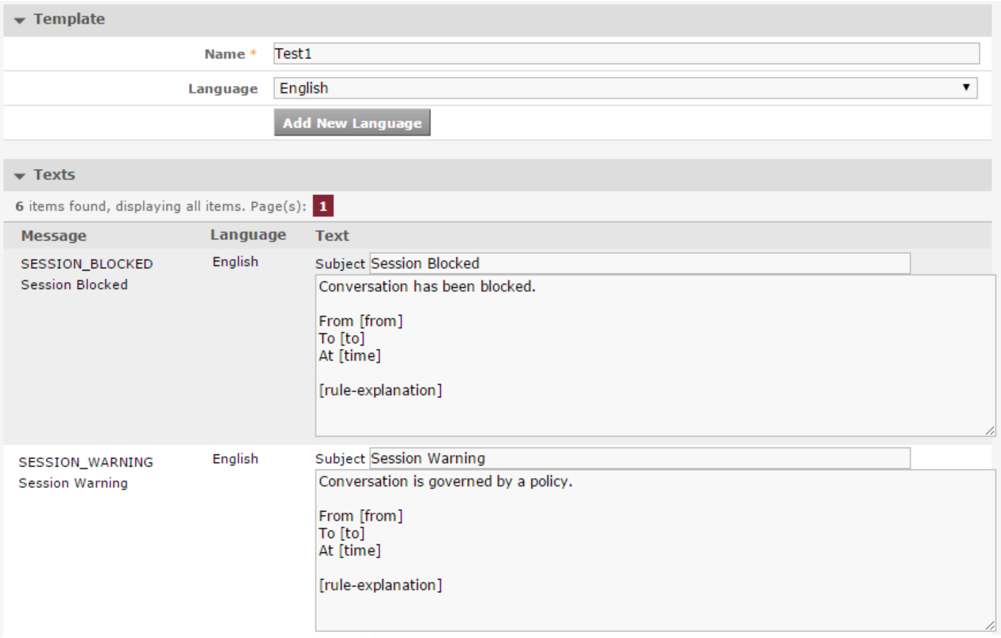
Save

Click on **Save**, and then continue with the *Define Your Template* section.

Define Your Template

To Add a New Language that is not assigned to your template yet, click on the **Add New Language** button > **Select** the language > Click on **Add**

Under the **Texts** tab, the possible notification types are listed, such as SESSION_BLOCKED, which is sent when a session is blocked by the policy, or SESSION_WARNING for sessions that are not blocked but monitored.
You can define the text of these messages in every language that you assigned to the given template.



Name * Test1

Language English

6 items found, displaying all items. Page(s): 1

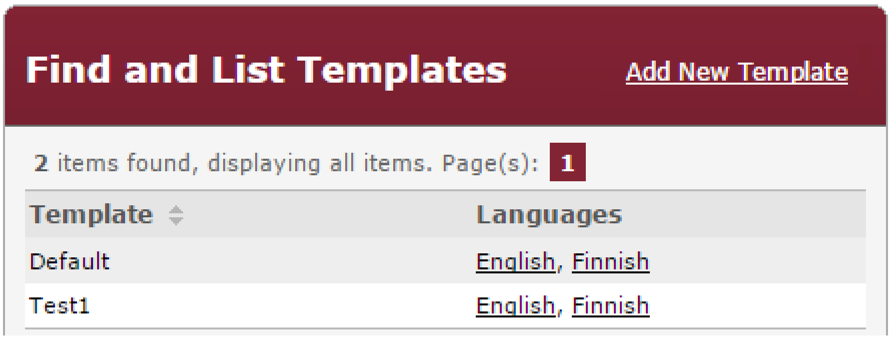
Message	Language	Text
SESSION_BLOCKED Session Blocked	English	Subject Session Blocked Conversation has been blocked. From [from] To [to] At [time] [rule-explanation]
SESSION_WARNING Session Warning	English	Subject Session Warning Conversation is governed by a policy. From [from] To [to] At [time] [rule-explanation]

Disclaimer Templates

Overview

The Verba Ethical wall solution can send Disclaimers to the participants of a communication session.

The users can **define the messages** to be sent out as disclaimers with the aid of Disclaimer Templates.
The see and manage Disclaimer Templates, in the Verba web interface navigate to **Policies > Disclaimer Templates.**



2 items found, displaying all items. Page(s): 1

Template	Languages
Default	English, Finnish
Test1	English, Finnish

The steps to **define disclaimer messages** for a certain Communication Policy are as follows

Step 1 - In the Verba web interface navigate to **Policies > Disclaimer Templates**

Step 2 - Click on **Add New Template** at the top right corner of the page

Step 3 - Define the initial parameters for the template as shown in the ***Add New Template* section** below

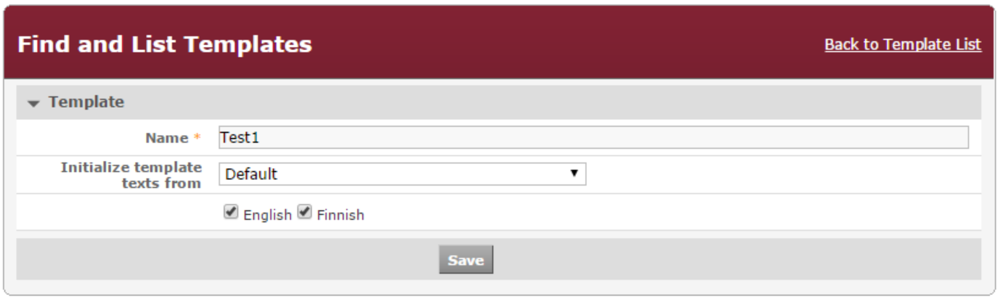
Step 4 - Define your policy as shown in the ***Define Your Template* section** below

Step 5 - **Assign** the Disclaimer Template and the desired language to a Communication Policy as shown in Manage Communication Policies

Add New Template

To Add a New Disclaimer Template, navigate to **Policies > Disclaimer Templates** in the Verba web interface, and then in the top right corner click on **Add New Template**.

- **Name** - The name is for administration purposes only, choose any that you like.
- **Initialize template texts** - To save time and effort, **templates** that are already defined in the system can be **imported**. When this option is used, only messages that are different need to be changed.
- **Language** - Choose the languages to be used in this template. The ones that are already defined in the system are shown. See the *Define a Template* section on adding new languages.



Name * Test1

Initialize template texts from: Default

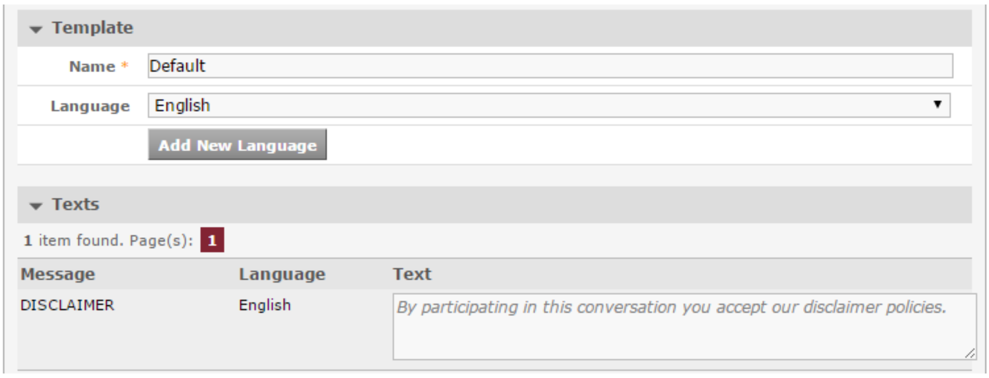
☑ English ☑ Finnish

Click on **Save**, and then continue with the *Define a Template* section.

Define a Template

To Add a New Language that is not yet assigned to a template, click on the **Add New Language** button > **Select** the language and finally click on **Add**

The disclaimer text can be set under the **Texts** tab. This message will be sent to the participants as a disclaimer.



Name * Default

Language English

1 item found. Page(s): 1

Message	Language	Text
DISCLAIMER	English	By participating in this conversation you accept our disclaimer policies.

The text of this message can be defined in every language assigned to the given template.

Disclaimer Examples

Here you find examples for Instant Message disclaimer templates.

Note
Verba does not provide legal advice. The examples below are shown for illustrative purposes only.

English

NOTICE TO RECIPIENTS: The information contained in and accompanying this communication may be confidential, subject to legal privilege, or otherwise protected from disclosure, and is intended solely for the use of the intended recipient(s). If you are not the intended recipient of this communication, please delete and destroy all copies in your possession, notify the sender that you have received this communication in error, and note that any review or dissemination of, or the taking of any action in reliance on, this communication is expressly prohibited.

: . .

Deutsch

MITTEILUNG AN DEN EMPFAENGER: Die Informationen, welche in dieser Nachricht enthalten oder dieser beigefuegt sind, koennen vertraulich sein und sind ausschliesslich fuer den Gebrauch durch den oder die Adressaten bestimmt. Wenn Sie nicht der Adressat dieser Nachricht sind, bitten wir Sie, saemtliche Kopien dieser Nachricht zu vernichten und den Sender darueber zu benachrichtigen, dass Sie diese Nachricht irrtuemlich erhalten haben. Wenn Sie nicht der Adressat dieser Nachricht sind, weisen wir Sie ausserdem darauf hin, dass es ausdruecklich untersagt ist, diese Nachricht zu lesen, weiterzuleiten oder in sonstiger Frorm zu verwenden.

Español

AVISO A LOS RECEPTORES: La información que figura en la presente comunicación y que la acompaña puede ser de naturaleza confidencial o bien estar sujeta a normas de confidencialidad legal o a protecciones relativas a su divulgación. Tiene por único objeto su utilización por parte del receptor a quien está destinada. Si usted no es el destinatario de la presente comunicación, rogamos eliminar y destruir todos los ejemplares de ésta que se encuentren en su poder, avisándole al remitente que la recibió por error. Queda expresamente prohibido examinar o difundir la presente comunicación o ejecutar actos en base a la misma.

Français

Ce message et toutes les pièces jointes peuvent être confidentiels et, de plus, peuvent être couverts par un privilège ou une protection légale. Il est établi à l'intention exclusive de ses destinataires. Si vous n'êtes pas le destinataire de ce message, merci de détruire toute copie en votre possession et d'en informer l'émetteur. Dans ce cas, toute diffusion ou toute publication, totale ou partielle, de ce message est formellement interdite, ainsi que toute action prise sur la foi dudit message.

Italiano

INFORMAZIONE PER IL RICEVENTE: Le informazioni che sono contenute o che accompagnano questa comunicazione potrebbero essere riservate, coperte da segreto professionale, o altrimenti protette da altre restrizioni alla loro divulgazione, e sono destinate esclusivamente alle persone alle quali questa comunicazione é indirizzata. Se questa comunicazione non é indirizzata a Voi, siete pregati di distruggerne tutte le copie in Vostro possesso, di notificarci che avete ricevuto questa comunicazione per errore, e di considerare che sono espressamente vietate la lettura, la diffusione o la distribuzione totale o parziale di questa comunicazione, nonché l'agire sulla base di (informazioni contenute in) questa comunicazione.

: , , , () . , , , .

Português

INFORMAÇÕES AOS RECEBEDORES: As informações contidas e as anexadas a esta comunicação podem ser confidenciais, legalmente privilegiadas, ou ter de outra forma protegida a sua divulgação, sendo exclusivamente para o uso do(s) seu(s) destinatário(s). Se você não for o destinatário previsto desta comunicação, queira por gentileza excluir e destruir todas as cópias em seu poder, notifique o remetente que você recebeu esta comunicação por engano e esteja ciente de que a leitura ou a divulgação bem como a adoção de qualquer ação baseada nesta comunicação estão expressamente proibidas.

Русский

К сведению получателей: Данное сообщение или приложения к нему могут содержать информацию, конфиденциальность которой защищена законом, либо не подлежащую разглашению информацию. Указанная информация предназначена исключительно для прочтения определённым адресатом или определёнными адресатами. В случае, если Вы получили это сообщение, не являясь предназначенным получателем, пожалуйста, удалите его и уничтожьте все имеющиеся в Вашем распоряжении копии, а также уведомите отправителя о том, что Вы получили данное сообщение по ошибке. Учтите, что любое ознакомление с информацией, содержащейся в сообщении, а также её распространение или использование в личных целях запрещено.

Communication Policy Validator

Overview

The **Communication Policy Validator** tool is used to make sure that the Communication Policy rules that are configured really enforce the correct policies.

The administrators can define users and see what policies are being enforced between them, thus checking if they set up the engine correctly.

The Validator can be accessed by navigating to Policies -> Validator in the Verba menu.

Testing P2P sessions

To test your policies on peer-to-peer sessions (two participants):

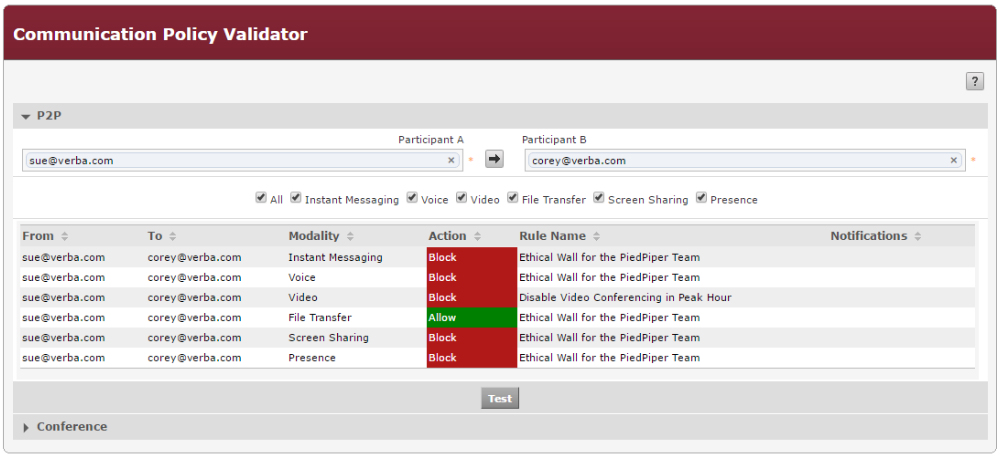
Step 1 - Specify two participants

Step 2 - Specify a direction (the icon in the middle)

Step 3 - Specify which modalities to test (click All to select all modalities)

Step 4 - Click Test

The result will show the matching Communication Policies for each direction and modality.



Participant A: sue@verba.com

Participant B: corey@verba.com

☑ All ☑ Instant Messaging ☑ Voice ☑ Video ☑ File Transfer ☑ Screen Sharing ☑ Presence

From	To	Modality	Action	Rule Name	Notifications
sue@verba.com	corey@verba.com	Instant Messaging	Block	Ethical Wall for the PiedPiper Team	
sue@verba.com	corey@verba.com	Voice	Block	Ethical Wall for the PiedPiper Team	
sue@verba.com	corey@verba.com	Video	Block	Disable Video Conferencing in Peak Hour	
sue@verba.com	corey@verba.com	File Transfer	Allow	Ethical Wall for the PiedPiper Team	
sue@verba.com	corey@verba.com	Screen Sharing	Block	Ethical Wall for the PiedPiper Team	
sue@verba.com	corey@verba.com	Presence	Block	Ethical Wall for the PiedPiper Team	

Testing Conferences

To test your policies on conference sessions (more than participants):

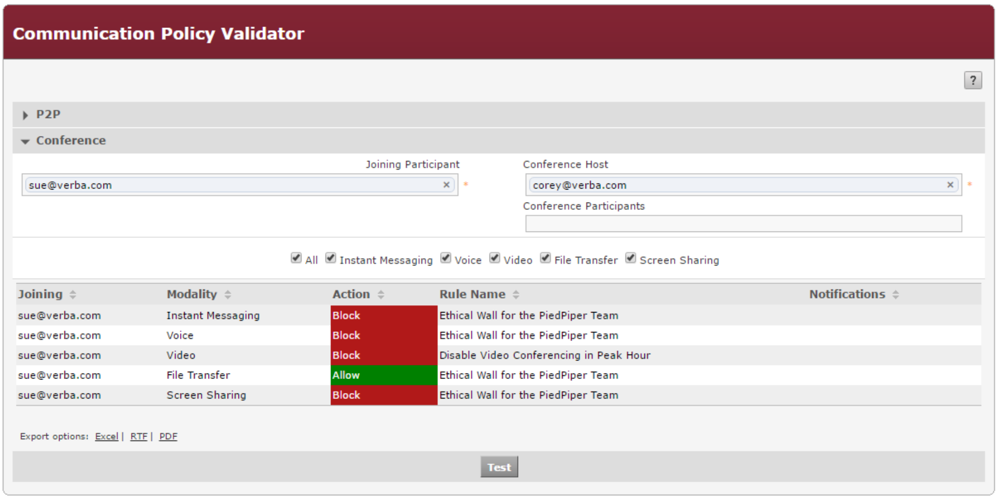
Step 1 - Specify the joining participant, the conference host

Step 2 - *(optionally)* Specify a chaperone - a participant already in the call, whose participation might change the outcome

Step 3 - Specify which modalities to test (click All to select all modalities)

Step 4 - Click Test

The result will show the matching Communication Policies for each direction and modality.



Communication Policy Validator

Joining Participant: sue@verba.com *

Conference Host: corey@verba.com *

Conference Participants:

☑ All ☑ Instant Messaging ☑ Voice ☑ Video ☑ File Transfer ☑ Screen Sharing

Joining	Modality	Action	Rule Name	Notifications
sue@verba.com	Instant Messaging	Block	Ethical Wall for the PiedPiper Team	
sue@verba.com	Voice	Block	Ethical Wall for the PiedPiper Team	
sue@verba.com	Video	Block	Disable Video Conferencing in Peak Hour	
sue@verba.com	File Transfer	Allow	Ethical Wall for the PiedPiper Team	
sue@verba.com	Screen Sharing	Block	Ethical Wall for the PiedPiper Team	

Export options: Excel | RTF | PDF

Configuring the Ethical Wall for Cisco Collaboration

Overview

The Verba Ethical Wall for Cisco Collaboration solution uses the following connections to the Cisco platform:

- **Cisco EventBroker API** - Jabber IM blocking, filtering and disclaimers
- **Cisco CURRI API** - Session blocking for Voice and Video

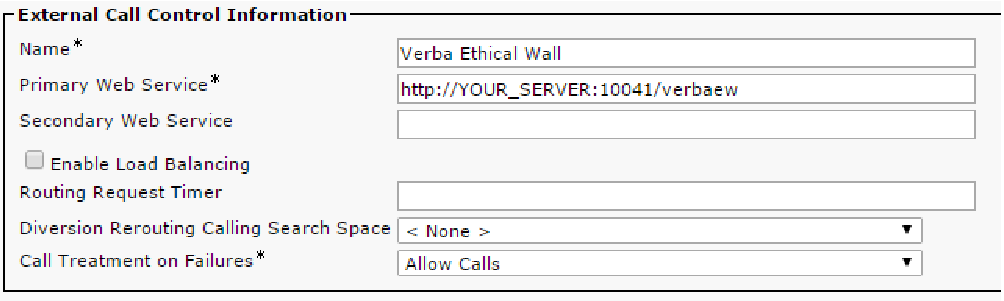
Configuring Cisco components

To use the Verba solution for Voice and Video overwatch, you need to set the service as a compliance server in Cisco Unified Communication Manager.
For IM, Presence, Screen Share and File Transfer you need to configure the Cisco IM & Presence Server.

Compliance for Voice and Video

Step 1 - In the CUCM menu navigate to **Call Routing > External Call Control Profile**

Step 2 - Click on the **Add New** button



External Call Control Information

Name*	Verba Ethical Wall
Primary Web Service*	http://YOUR_SERVER:10041/verbaew
Secondary Web Service	
□ Enable Load Balancing	
Routing Request Timer	
Diversion Rerouting Calling Search Space	< None >
Call Treatment on Failures*	Allow Calls

Step 3 - Set configuration

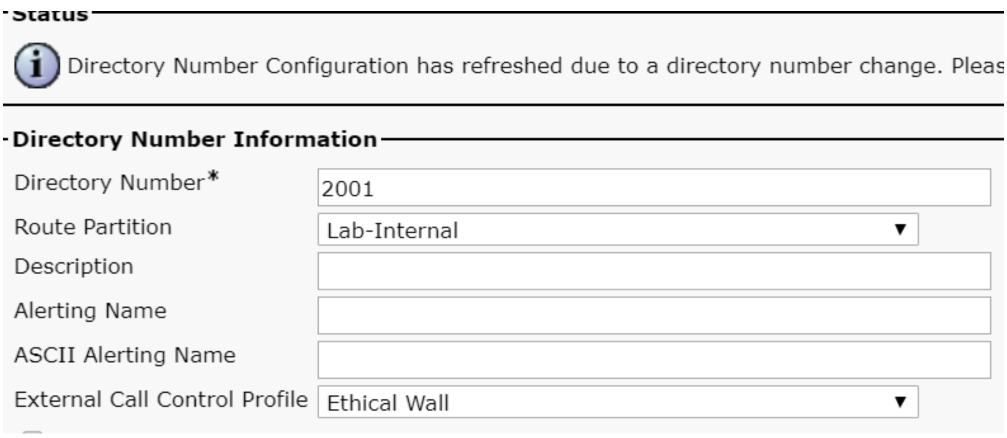
Set the URL that you want the service to use for communication with the Verba compliance server.
Under the *Configuring Verba components* section, you will see how to adjust Verba to listen on this address.
With the *Call Treatment on Failures* option, you can define what the call manager should do if it cannot reach the compliance server. (Network failure for example)

Step 4 - Click **Save**

Step 5 - In the CUCM menu navigate to **Device > Phone**

Step 6 - Select the device, then select the line.

Step 7 - Select the External Call Control Profile created previously.



Status

Directory Number Configuration has refreshed due to a directory number change. Pleas

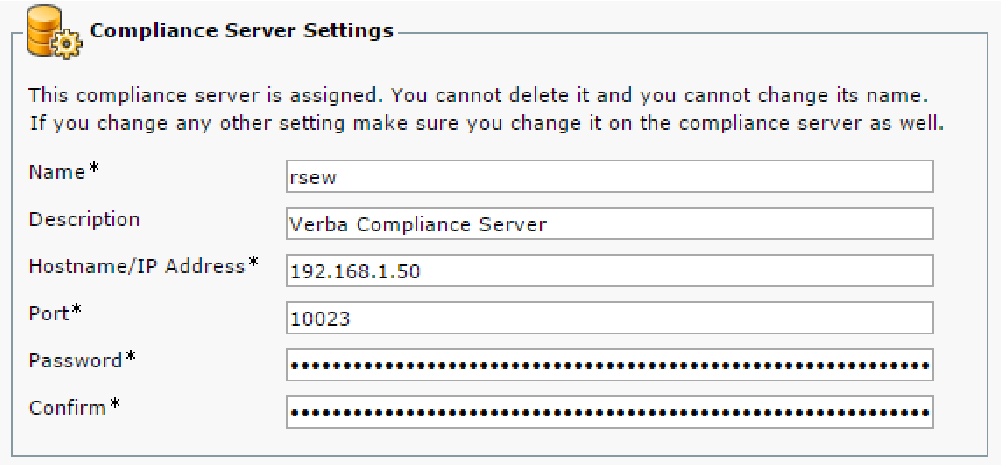
Directory Number Information

Directory Number*	2001
Route Partition	Lab-Internal
Description	
Alerting Name	
ASCII Alerting Name	
External Call Control Profile	Ethical Wall

Compliance for IM, Presence, Screen Share and File Transfer

Step 1 - In the Cisco IM & Presence Server menu navigate to **Messaging > External Server Setup > Third-Party Compliance Servers**

Step 2 - Click on the **Add New** button



Compliance Server Settings

This compliance server is assigned. You cannot delete it and you cannot change its name. If you change any other setting make sure you change it on the compliance server as well.

Name*	rsew
Description	Verba Compliance Server
Hostname/IP Address*	192.168.1.50
Port*	10023
Password*	••
Confirm*	••

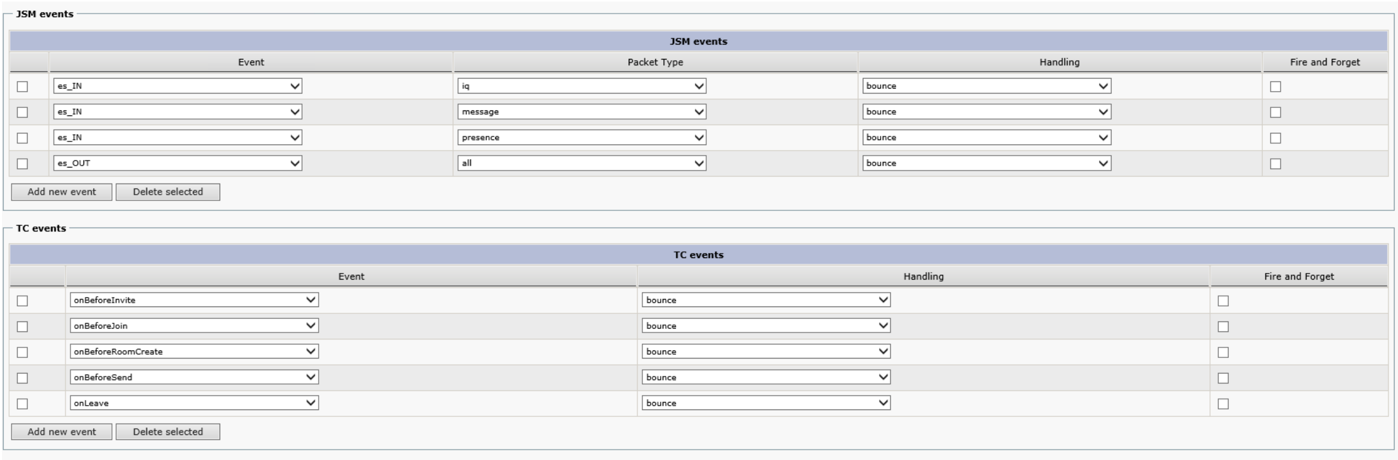
Step 3 - Set your Verba Compliance Server's parameters here

This is the **Name** you will be referring to your compliance server in the Cisco IM & Presence Server
Set the **Hostname**, **Port** and choose a **Password**

> ⓘ Steps 4 to 7 apply only to **Cisco IM&P 10.x and above**. For Cisco IM&P 9.x and below, these profiles need to be set in the Verba Web Application as shown in section **Configuring Verba Components > Step 5**

Step 4 - In the Cisco IM & Presence Server menu navigate to **Messaging > Compliance > Compliance Profiles**

Step 5 - Click on the **Add New** button



JSM events

JSM events				
	Event	Packet Type	Handling	Fire and Forget
□	es_IN	iq	bounce	□
□	es_IN	message	bounce	□
□	es_IN	presence	bounce	□
□	es_OUT	all	bounce	□

TC events

TC events			
	Event	Handling	Fire and Forget
□	onBeforeInvite	bounce	□
□	onBeforeJoin	bounce	□
□	onBeforeRoomCreate	bounce	□
□	onBeforeSend	bounce	□
□	onLeave	bounce	□

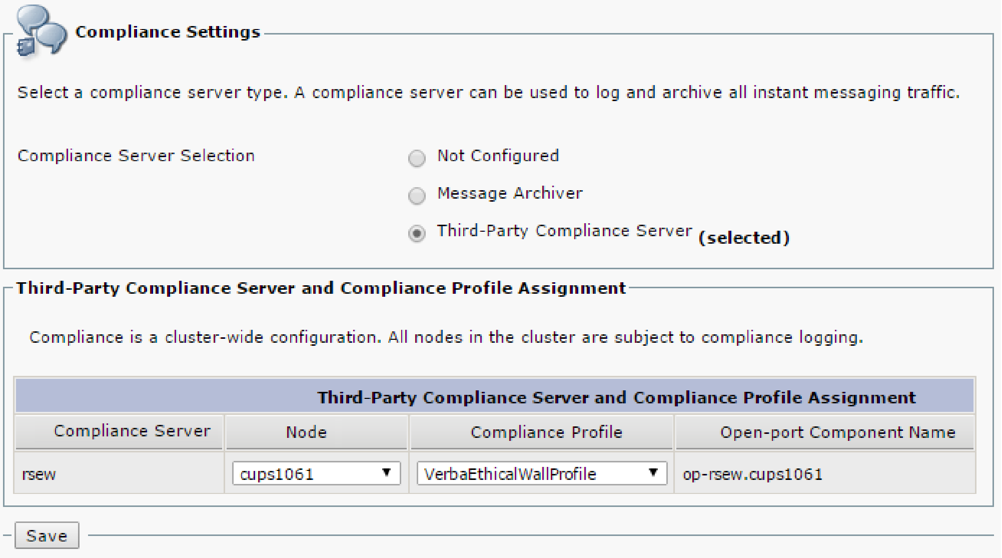
Step 6 - Set configuration

You can configure the events for which you want the IM & Presence server to call the Verba compliance service. If you want your Communication Policies to apply to all communication on your network, then the recommended configuration is as shown above.

ⓘ Also, this profile configuration should be used in systems where the Ethical Wall and IM Recording are both deployed.

Step 7 - Click **Save**

Step 8 - In the Cisco IM & Presence Server menu navigate to **Messaging > Compliance > Compliance Settings**



Compliance Settings

Select a compliance server type. A compliance server can be used to log and archive all instant messaging traffic.

Compliance Server Selection
○ Not Configured
○ Message Archiver
● Third-Party Compliance Server **(selected)**

Third-Party Compliance Server and Compliance Profile Assignment

Compliance is a cluster-wide configuration. All nodes in the cluster are subject to compliance logging.

Third-Party Compliance Server and Compliance Profile Assignment			
Compliance Server	Node	Compliance Profile	Open-port Component Name
rsew	cups1061	VerbaEthicalWallProfile	op-rsew.cups1061

Step 9 - Under Compliance Server Selection, select **Third-Party Compliance Server**

Step 10 - **Assign** the Compliance Profiles to your Compliance server

Compliance Server is the server that your Verba compliance service runs on.
Select the **Cisco Node** and the **Profile** that you set up in Step 3.

Step 11 - Click **Save**

Restarting the XCP Router Service

For the Compliance server settings to take effect, the **XCP Router Service** has to be restarted. To do that, follow the steps below:

Step 1 From the list in the top right corner of the CUPS management interface select **Cisco Unified IM and Presence Serviceability** and click Go.

Step 2 From the top menu select **Tools > Control Center > Network Services**

Step 3 From the server list select **CUCM IM and Presence** and click Go.

Step 4 Select the **Cisco XCP Router** service and click **Restart**. The process can take several minutes to complete.

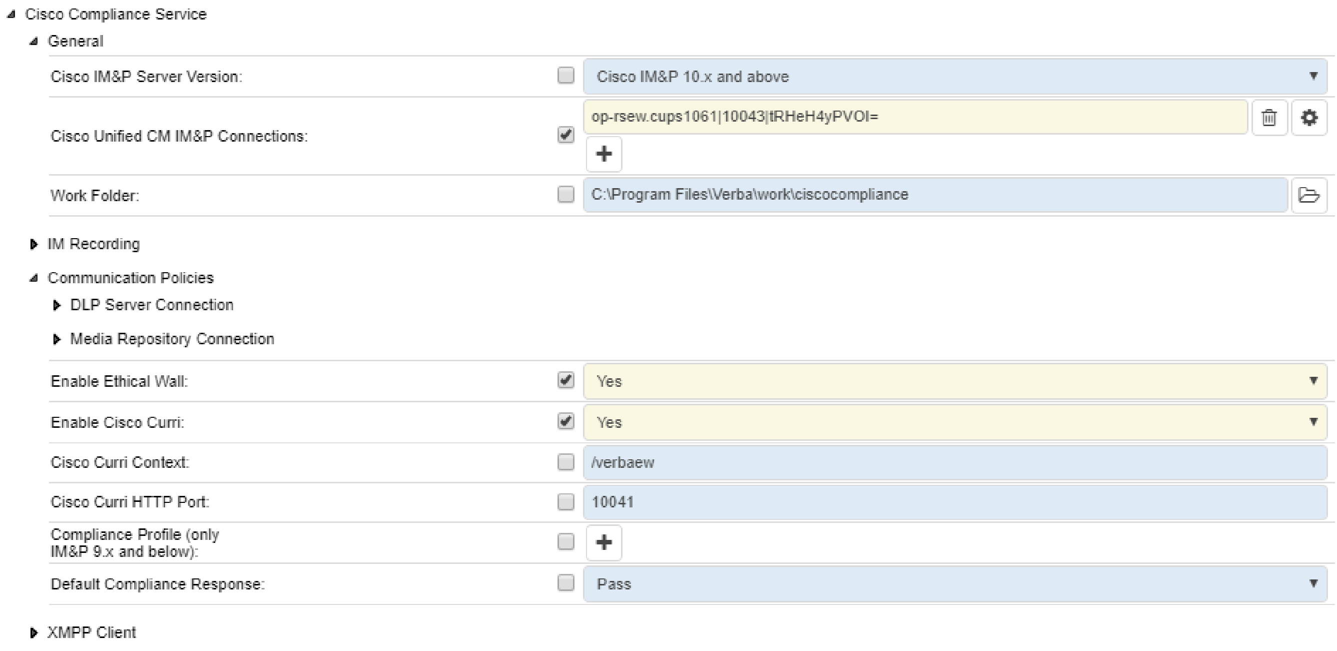
Configuring Verba components

Step 1 - In the Verba Web Application menu navigate to **Administration > Verba Servers**

Step 2 - Click on the server that the Verba compliance service will run on

Step 3 - Click on the **Service Activation tab**, and **activate** the Verba Cisco Compliance Service, using the ⚙ button at the end of the line

Step 4 - Click on the **Change Configuration tab**, and look for the Cisco Compliance Service section



- Cisco Compliance Service
  - General

Cisco IM&P Server Version:	☐	Cisco IM&P 10.x and above ▾
Cisco Unified CM IM&P Connections:	☑	op-rsew.cups1061|10043|tRHeH4yPVOI= +
Work Folder:	☐	C:\Program Files\Verba\work\ciscocompliance

  - IM Recording
  - Communication Policies
    - DLP Server Connection
    - Media Repository Connection

Enable Ethical Wall:	☑	Yes ▾
Enable Cisco Curri:	☑	Yes ▾
Cisco Curri Context:	☐	/verbaew
Cisco Curri HTTP Port:	☐	10041
Compliance Profile (only IM&P 9.x and below):	☐	+
Default Compliance Response:	☐	Pass ▾

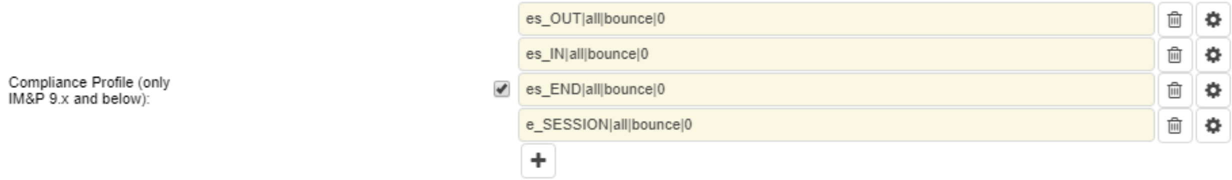
  - XMPP Client

Step 5 - Set configuration

- **Cisco IM&P Server Version** - Set the Cisco IM&P Server Version. The *General* section does not need to be configured if the Ethical Wall is only used for voice and video traffic.
- **Cisco Unified CM IM&P Connections** - To configure a connection, in the next line click on the + icon. At the right panel, set the **Component Name** setting. The component name will be the **Open-port Component Name** that is shown in the IM&P servers under **Messaging \ Compliance \ Compliance Settings** menu. The **Port** and **Password** should be the same as what previously set in the Compliance Profile that is assigned to this node in the IM&P servers.
- **Enable Ethical Wall** - Set to Yes to turn the function on

- **Cisco CURRI Context** - You set this parameter in the previous section (Configuring Cisco Components > Compliance for Voice and Video > Step 3) This only needs to be configured if the Ethical Wall is used for voice and video traffic
- **Cisco CURRI HTTP Port** - You set this parameter in the previous section (Configuring Cisco Components > Compliance for Voice and Video > Step 3)

- **Compliance Profile (only IM&P 9.x and below)** - If you have Cisco IM & Presence server 9.x or earlier, then you cannot set Compliance Profiles on the IM&P server. You have to define which messages the IM&P server should send to the Verba Compliance Service for processing.
  For standard cases set all 4 types of events (**es_OUT**, **es_IN**, **es_END**, **e_SESSION**), with **all** packet types (**IM**, **Presence**, **File Transfer**, **Screen Share**).
  Fire and Forget - Leave the checkbox unchecked if the IM and Presence Service node must wait for a response from the compliance server before it continues to process the event. Check the checkbox if the IM and Presence Service node does not require a response from the compliance server before it continues to process the event further. (For the Verba Ethical Wall to fully function, leave this unchecked)
  Handling - Select **bounce** if errors returned from the compliance server should be bounced back to the originating party or component, select **pass** if they should be discarded. The **Handling** setting is ignored if **Fire and Forget** is not chosen.
  To configure these settings, click on the
  ✚
  button, then click on the
  ⚙
  button at the end of the line. The right-hand panel changes, set the message types one by one here, as shown above. Click on the **Save** button at the bottom of the panel.



Compliance Profile (only IM&P 9.x and below): ☑

es_OUT|all|bounce|0

es_IN|all|bounce|0

es_END|all|bounce|0

e_SESSION|all|bounce|0

Step 6 - Save the Configuration

At the top-right corner of the panel click on **Save**, to save the whole configuration.

A yellow strip appears with the message: "*There are tasks to be executed regarding the configuration of this Verba Server. If you would like to execute these tasks now, please click here*"
Click on the link and **execute the tasks** that you see in the list.

Configuring the Ethical Wall for Skype for Business

Overview

The Verba Ethical Wall for Skype for Business (Lync) uses the following connections to the Skype for Business (Lync) platform:

- **Trusted application on the Front End Servers** - a filter is processing signaling for presence blocking, session blocking, and disclaimers
- **UCMA application** - used for notifications

Prerequisites

- The **Verba Ethical Wall** and the **Verba Ethical Wall init** have to be registered in the Skype for Business (Lync) environment as trusted applications. The required commands can be found under the "**Verba SfB/Lync Communication Policy Service**" section in the Installing the Verba Skype for Business - Lync Filter article.
- If the **notifications** are required then the **Verba Announcement service** needs to be installed and configured. For instructions, please refer to the Installing and configuring the Verba SfB - Lync Announcement service page.
- At least an empty policy (allowing all communications) has to be created. For instructions, see Manage Communication Policies.

Configuring Verba components

Front End Servers

The actions described below need to be completed for each Front End Server.

Step 1 - In the Verba Web Application navigate to **System \ Servers**

Step 2 - Select a Front End Server

Step 3 - Click on the **Service Activation** tab

Step 4 - Activate the **Verba SfB/Lync Communication Policy Service**, using the ⚙ icon at the end of the line

Step 5 - Click on the **Change Configuration Settings** tab

Step 6 - Under the **Skype for Business/Lync Ethical Wall -> General** section set the required settings:

Setting	Description	Example
Server Version	The version of the Skype for Business/Lync environment	Lync Server 2013
Verba Announcement services	The announcement services, one in each line. Required if **notifications** or **Session termination if Chaperone leaves** is configured in the Communication policy panels. The format is: announcement_server_hostname:10211|computer_gruu	testucma1:10211|sip:testucma1.verbatest.local@verbatest.local;gruu;opaque=srvr:trainingannouncementapp:LOqq58liLV2IFR7QVbfv4QAA
Block Additions to Contact List	Blocks the addition of the queried users to the contact list. The possession of the remote user's full SIP URI allows the user to add the remote user to the contact list. This setting prevents this functionality. Default Value: **On**	

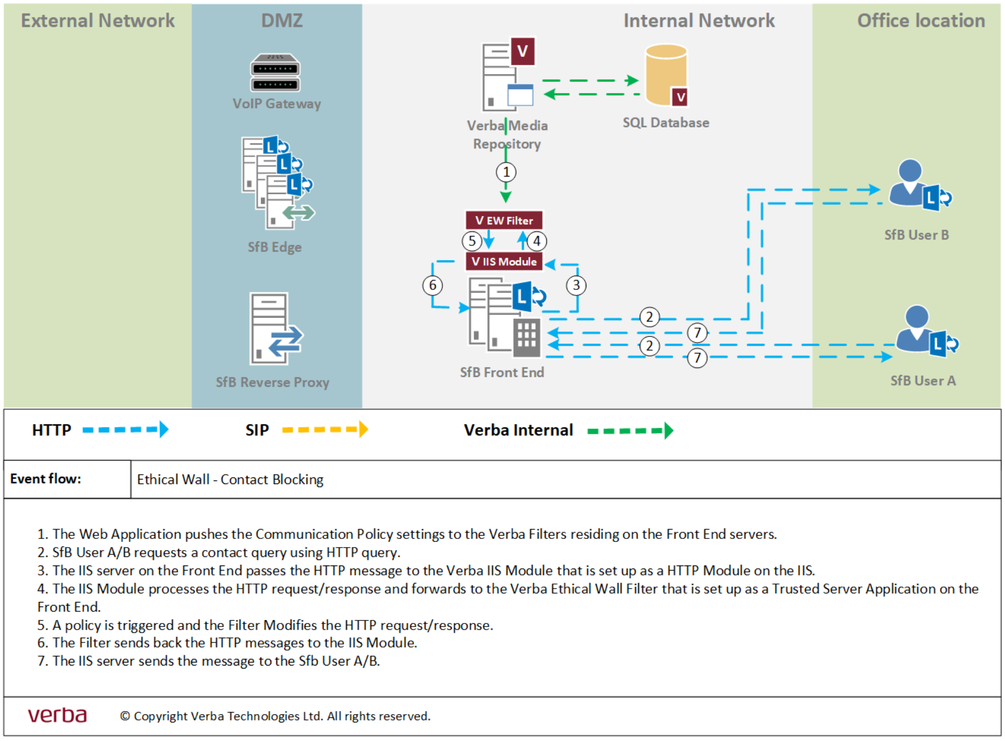
Step 7 - **Save** and **apply** configuration

Installing and configuring Skype for Business contact request blocking

Overview

For the contact blocking functionality, an IIS module needs to be deployed alongside the usual Ethical Wall Lync components. This IIS module intercepts the contact list requests and forwards the message to the Filter for processing and decision making.

The flow below describes which components are involved when the contact list blocking functionality is used.



Event flow:	Ethical Wall - Contact Blocking

1. The Web Application pushes the Communication Policy settings to the Verba Filters residing on the Front End servers.
2. SfB User A/B requests a contact query using HTTP query.
3. The IIS server on the Front End passes the HTTP message to the Verba IIS Module that is set up as a HTTP Module on the IIS.
4. The IIS Module processes the HTTP request/response and forwards to the Verba Ethical Wall Filter that is set up as a Trusted Server Application on the Front End.
5. A policy is triggered and the Filter Modifies the HTTP request/response.
6. The Filter sends back the HTTP messages to the IIS Module.
7. The IIS server sends the message to the Sfb User A/B.

ⓘ To see how to enable this functionality, refer to the Presence Blocking article.

Installation

1. **Force Address Book Web Query**
    a. Open Skype for Business Management Shell on the Front End server
    b. Execute the following command to apply the contact request blocking for entire organization: Set-CsClientPolicy -Identity Global -AddressBookAvailability WebSearchOnly
    c. Alternatively, create a Client Policy and apply for a group of users:

```
New-CsClientPolicy -Identity GroupClientPolicy  -AddressBookAvailability WebSearchOnly
Grant-CsClientPolicy -Identity User1 -PolicyName GroupClientPolicy
```

2. **Install Verba Contact Request Proxy into the GAC (Global Assembly Cache) on the Front End servers (later the install will do it)**

   a. Open a cmd with Administrator privileges
   b. Navigate to the "C:\Program Files\Microsoft SDKs\Windows\v7.0\Bin\" folder
   c. Type the following command:

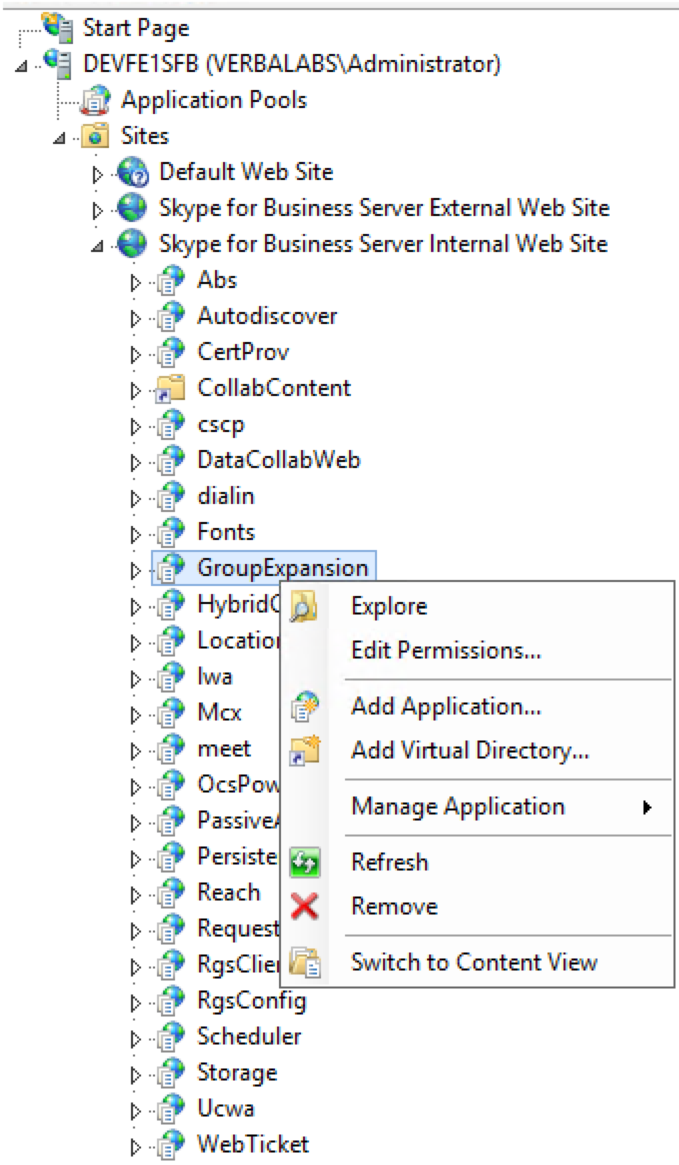
   ```
   gacutil -i "C:\Program Files (x86)\Verba\Verba.Lync.WebProxy.dll"
   ```

3. **Configure Verba Contact Request Proxy in IIS**

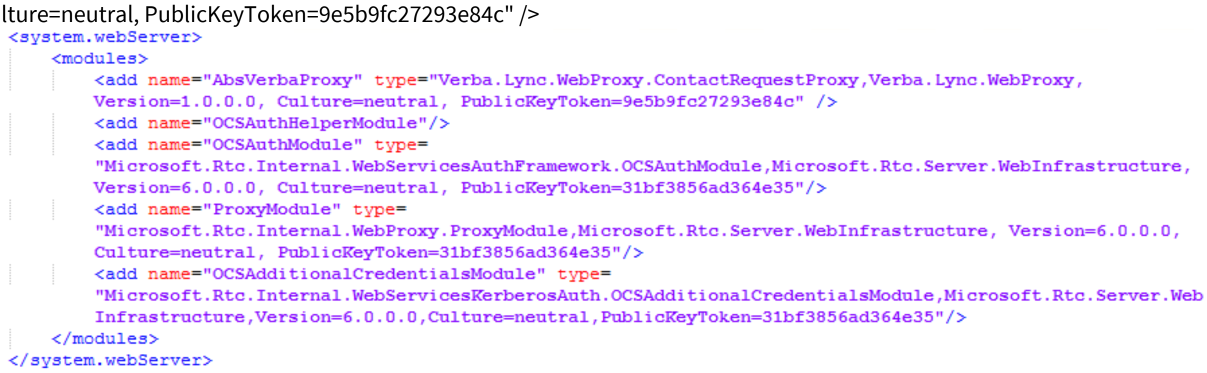
   a. Open the IIS Manager
   b. Expand the tree list until you get the Skype for Business Server Internal Web Site\GroupExpansion
   c. Right click on the

   the Skype

   for Business Server Internal Web Site\GroupExpansion and select the Explore option



d. In the File Explorer open the web.config file and insert the following line to the xml module tag <add name=" AbsVerbaProxy" type="Verba.Lync.WebProxy.ContactRequestProxy,Verba.Lync.WebProxy, Version=1.0.0.0, Culture=neutral, PublicKeyToken=9e5b9fc27293e84c" />



```
<system.webServer>
    <modules>
        <add name="AbsVerbaProxy" type="Verba.Lync.WebProxy.ContactRequestProxy,Verba.Lync.WebProxy,
        Version=1.0.0.0, Culture=neutral, PublicKeyToken=9e5b9fc27293e84c" />
        <add name="OCSAuthHelperModule"/>
        <add name="OCSAuthModule" type=
        "Microsoft.Rtc.Internal.WebServicesAuthFramework.OCSAuthModule,Microsoft.Rtc.Server.WebInfrastructure,
        Version=6.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35"/>
        <add name="ProxyModule" type=
        "Microsoft.Rtc.Internal.WebProxy.ProxyModule,Microsoft.Rtc.Server.WebInfrastructure, Version=6.0.0.0,
        Culture=neutral, PublicKeyToken=31bf3856ad364e35"/>
        <add name="OCSAdditionalCredentialsModule" type=
        "Microsoft.Rtc.Internal.WebServicesKerberosAuth.OCSAdditionalCredentialsModule,Microsoft.Rtc.Server.Web
        Infrastructure,Version=6.0.0.0,Culture=neutral,PublicKeyToken=31bf3856ad364e35"/>
    </modules>
</system.webServer>
```

e. Save the web.config file

f. Restart the IIS Server from the manager application. Right click on name of the server and press stop. When it is stopped click to the start option.

4. **Activate the Verba Ethical Wall Service in Verba and set rules for contact list blocking**

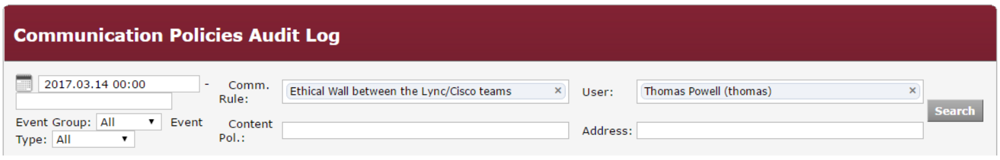
Troubleshooting

Communication Policy Audit Log

The Audit log shows all events in the Ethical Wall when rules needed to be enforced.

Ethical Wall administrators can see when disclaimers were sent, when session and content blocking rules were used, notifications sent, etc.

On the first page, results can be refined, so that only events are shown that are in relation to a certain Communication Policy, Content Policy or a specific User.



Communication Policies Audit Log

2017.03.14 00:00 -

Comm. Rule: Ethical Wall between the Lync/Cisco teams ×

User: Thomas Powell (thomas) ×

Event Group: All ▾

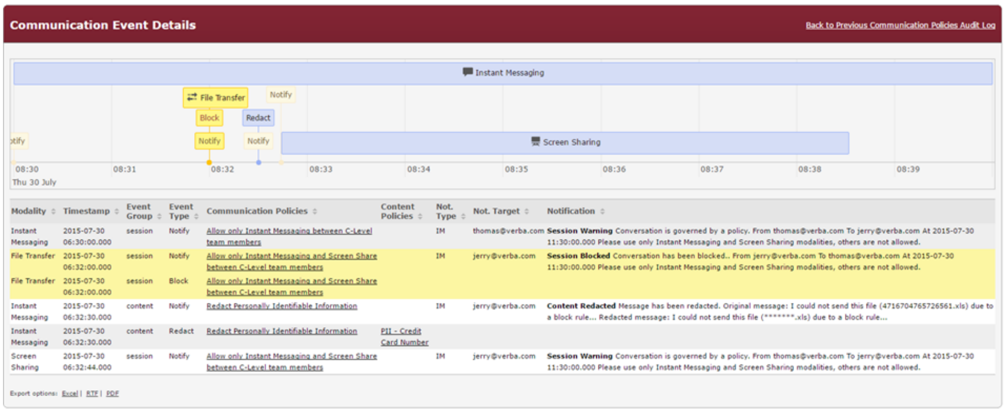
Event Type: All ▾

Content Pol.:

Address:

After clicking on one of the sessions, all events related to this session are shown in a timeline. It is also visible which communication policy triggered the action, what happened exactly.

The target of the notification message and the text are also visible.



Communication Event Details

Back to Previous Communication Policies Audit Log

Modality	Timestamp	Event Group	Event Type	Communication Policies	Content Policies	Not. Type	Not. Target	Notification
Instant Messaging	2015-07-30 06:30:00.000	session	Notify	Allow only Instant Messaging between C-Level team members		IM	thomas@verba.com	**Session Warning** Conversation is governed by a policy. From thomas@verba.com To jerry@verba.com At 2015-07-30 11:30:00.000 Please use only Instant Messaging and Screen Sharing modalities, others are not allowed.
File Transfer	2015-07-30 06:32:00.000	session	Notify	Allow only Instant Messaging and Screen Share between C-Level team members		IM	jerry@verba.com	**Session Blocked** Conversation has been blocked.. From jerry@verba.com To thomas@verba.com At 2015-07-30 11:30:00.000 Please use only Instant Messaging and Screen Sharing modalities, others are not allowed.
File Transfer	2015-07-30 06:32:00.000	session	Block	Allow only Instant Messaging and Screen Share between C-Level team members				
Instant Messaging	2015-07-30 06:32:30.000	content	Notify	Redact Personally Identifiable Information		IM	jerry@verba.com	**Content Redacted** Message has been redacted. Original message: I could not send this file (4716704765726561.xls) due to a block rule... Redacted message: I could not send this file (*******.xls) due to a block rule...
Instant Messaging	2015-07-30 06:32:30.000	content	Redact	Redact Personally Identifiable Information	PII - Credit Card Number			
Screen Sharing	2015-07-30 06:32:44.000	session	Notify	Allow only Instant Messaging and Screen Share between C-Level team members		IM	jerry@verba.com	**Session Warning** Conversation is governed by a policy. From thomas@verba.com To jerry@verba.com At 2015-07-30 11:30:00.000 Please use only Instant Messaging and Screen Sharing modalities, others are not allowed.

Export options: Excel | RTF | PDF

ICAP integration for Data Loss Prevention

Data Loss Prevention (DLP) overview

The Verint Verba Ethical Wall solution has the ability to run real-time checks on file transfers using an external DLP server.

Supports standard ICAP (Internet Content Adaptation Protocol) servers and is verified and tested with Symantec Protection Engine.

New Content Policy option

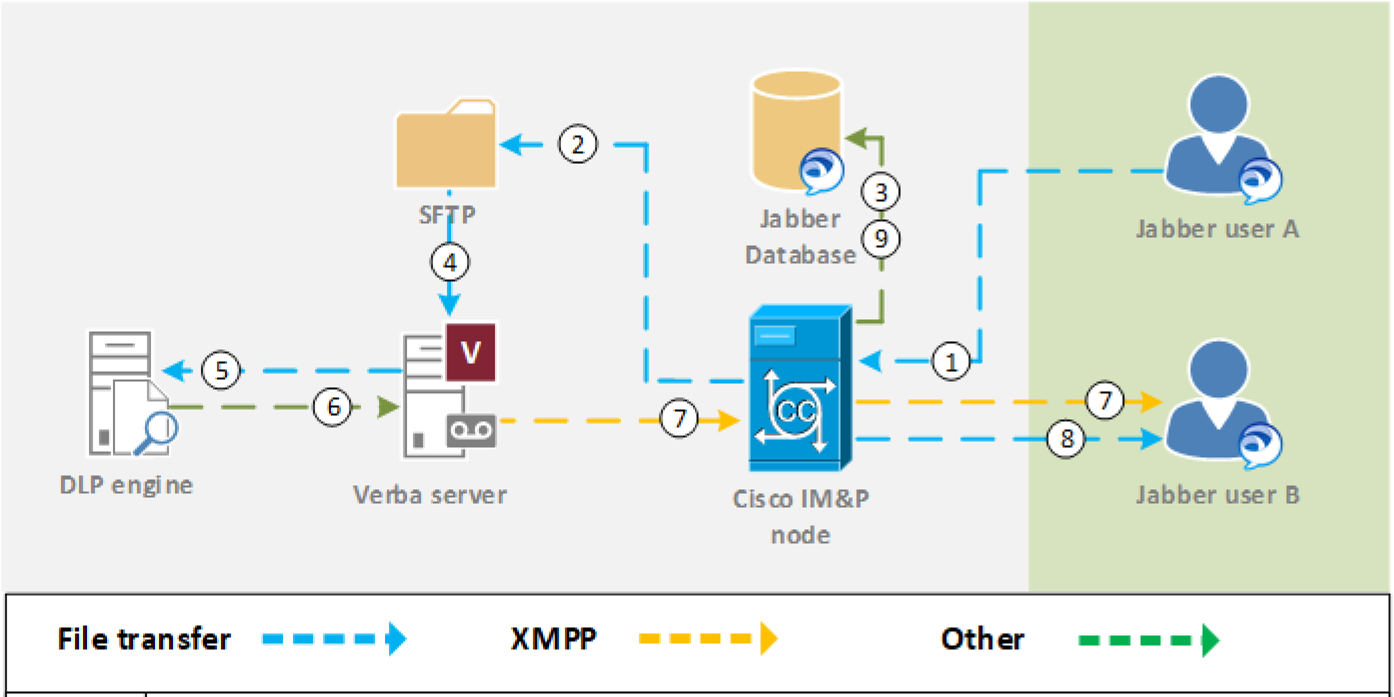
DLP can be configured by using the Content Policy option called **File DLP Check.**

This policy option allows **Block / Block & Notify / Notify** policy actions, **Redact** action is not available.

How DLP works

The ICAP integration for DLP is implemented in the **Verba Communication Policy Service**.

As an example in a Cisco environment, the DLP check flow is the following:



Flow:	File scanning with a DLP engine using Managed File Transfer

1. User A initiates a File Transfer to User B.
2. The IM&P node uploads the file to the defined SFTP storage.
3. An audit log entry of the file upload event is created in the database.
4. The Verba server downloads the file from SFTP.
5. The Verba server sends the file to the specified DLP engine.
6. The DLP engine scans the file and returns the results of the scan to the Verba server.
7. Upon receiving a “clean” indication from the DLP engine, the Verba server sends a URL pointing to the file on storage to User B.
8. User B clicks on the URL in the message and downloads the file.
9. An audit log entry of the file download event is created in the database.