



an
NTT Communications
Company

arkadin[®]anywhere



Security Features

01/01/2014



an
NTT Communications
Company

Introduction

ArkadinAnywhere is Arkadin's easy-to-use web collaboration service that helps improve internal and external communication processes, thereby enabling employees to work more efficiently through the ability to collaborate remotely.

Designed for a quick deployment and adoption by all users, Arkadin Anywhere has a simple, user friendly and intuitive interface requiring minimum user training. Online meetings can start instantly and there is no need to download software.

Arkadin Anywhere offers easy visual sharing from a computer:

- Share documents and applications online (web conference participants can see everything that is on the presenter's screen: a spread sheet, a web site, or any job specific program placed on the desktop)
- Present slide presentations
- Demonstrate new products in a visual format
- Annotate and utilize the white board in real-time
- Remotely control another desktop

This document describes the security features built into Arkadin Anywhere. It also includes the web based audio console for managing Arkadin audio conferences.

Anywhere meeting experience

Meeting roles

Three key roles are defined in ArkadinAnywhere conference: **Moderator**, **Presenter** and **Participant**.

Moderator: has the most control in a session and the ability to grant and revoke various privileges for the other participants. He/she joins the conference with a specific Moderator PIN.

- Start/end the conference, and lock the conference to avoid uninvited participant to join in
- See the complete list of Attendees and manage their roles (e.g. Participant to Presenter promotion)
- Manage the conference settings to allow or disallow certain functions for participants, for example:
- Chat, save presented document, transfer file, waits for moderator etc.
- Moderators are able to use their personal Content Bank to upload and store content for future presentation in a web conference.



an
NTT Communications
Company

Presenter: has the sharing ability to present documents, specific applications, or the entire desktop and control the annotation tools. He/she joins the conference with the Participant PIN and gets promoted to Presenter by the Moderator.

Whenever the Moderator or a Presenter is sharing an application or his/her entire desktop, a “Participant view” panel is displayed as a reminder that desktop sharing is active, so that desktop screens are never shared accidentally.

Participant: has minimal responsibilities and typically only views session content. He/she joins the conference with the Participant PIN.

Attendee list and content list confidentiality

By default the list of conference attendees will appear on the screen. The Moderator can disable access to the attendee list at any time during the conference for confidentiality. The list can also be disabled ahead of time or permanently.

The same options are also available for the list of content being shared during a meeting so the Moderator can stop the content list being shared.

Application or Desktop sharing

The application or desktop sharing feature can be disabled centrally for all your users by Arkadin during provisioning or at a later date. The remote control or the ability for participants to be made presenters in order to share their applications or desktop can also be disabled.

Audio Conference Management via Web Console

The web based audio console is unique to Arkadin and provides security and control for conference calls. This is an incredibly powerful, yet simple and user-friendly tool that allows moderators to view and control audio conference calls in real time via an Internet browser.

At a glance the moderator can see the list of all attendees on the call together with their telephone numbers. The moderator can monitor and control the conference by using the features that include: features including muting, conference locking and disconnecting one or several participants. It is therefore easy to see if there are any unexpected callers attending the call and they can be disconnected if appropriate, so ensuring meeting confidentiality.



an
NTT Communications
Company

One-Time PIN Conference Access

In addition to the permanent conference PINs, one-time use conferences can be scheduled via the ArkadinLounge portal for a specific date, time and duration. One-time PIN codes are only valid for the duration of the scheduled conference for greater security.

Meet-Me Secure

This feature provides the most secure profile. Instead of a shared Participant PIN, Participants are provided with individual PIN codes or User IDs, which authenticate and automatically name them in the Participant list. The system checks the Participant's PIN code against a pre-established white list before granting access to the conference. Non matching PIN users are automatically re-directed to an operator.

Security level	Ease for Moderator	Anywhere or Audio Console	One-Time PINS	Secured PINS
Good	One-click	X		
Strong	Booking	X	X	
Strongest	PIN list management	X		X

Security

Transport layer security

On top of the application security, access to the ArkadinAnywhere platform is secured at the transport layer level using a high level of encryption thanks to the https protocol and TLS encryption over TCP port 443.

All non-secured communications over port 80 are automatically forced and redirected to a secure mode.

The anywhereconference.com web site identity has been verified by VeriSign which provides the https certificate. The certificate provides a 128 bits encryption using an RC4 cyphered connection with SHA1 for authentication and RSA for key exchanges.

Servers do not accept connections using a version under the SSL V3.0 protocol. TLS 1.0 is the default mode.



an
NTT Communications
Company

Server to server communications is on private MPLS networks between regions and on private LANs when on the same site. Application servers securely communicate between each other through AES 256 bits encrypted streams with RSA for key exchanges.

Firewall compatibility

Arkadin Anywhere uses HTTPS (port 443) to establish a reliable and secure connection between the anywhereconference.com domain and the servers. If IT administrators have to allow traffic to the anywhereconference.com servers using TCP port 443 with https protocol, Arkadin Administrators can provide the exact list of server IP addresses.

Caution: Arkadin is often adding servers to the infrastructure so the list is frequently updated. There is no direct communication between users' terminals. All communications go through the server to provide end-to-end high level security.

Content security

Data exchanged during meetings is secured thanks to the 128 bits encryption. It covers slides, application or desktop sharing data, chat messages, files and everything being exchanged during the meeting.

Content exchanged during an ArkadinAnywhere web conference is securely stored in folders that are not accessible from the Internet. This security is regularly tested to ensure confidentiality is maintained (see Third Party Audit.) Only application servers have access to the content and are able to forward it to authenticated users. All content shared during a web conference is deleted from servers when the moderator ends the conference.*

Arkadin has security measures in place to ensure that data exchanged during a given web conference is solely restricted to that specific meeting. It is not possible to access shared data from another web conference.

Strong role based authentication checks are also in place to ensure that users rights are maintained for data sharing so the level of documentation sharing rights are done to make sure data are reachable only depending on the user role: Moderator, Presenter or Participant.



an
NTT Communications
Company

Arkadin Anywhere application sharing module

An optional module is required on users' machines for application and desktop sharing. The module is digitally signed by Arkadin. It is an ActiveX for Internet Explorer, a Firefox module on Windows and a DMG package on MacOS for Safari, Firefox and Chrome browsers.

Arkadin Anywhere Content Bank

The Arkadin Content Bank* provides Cloud storage to Moderators so they are able to easily retrieve their content, especially if it is frequently used, during their meetings. Content is stored in secured databases that cannot be accessed via the public Internet (only authenticated users can access the information.) Only application servers have access to the database.

*Arkadin will not modify documents stored in the Content Bank. It is the moderator's storage space and as such they are responsible for the content of documents stored and the uploading and deletion of these documents. The Content Bank should not be used for data back-up or archiving.

There are content banks in the US, in France and in Hong-Kong. Arkadin administrators can determine which one of these content banks is used for your company.

By default the Content Bank will be enabled. However, it can be deactivated during provisioning by Arkadin administrators, if requested. It can also be deactivated at any time by contacting Arkadin Client Care.

Documents in the Content Bank will be automatically archived after 6 months for a period of 3 months before being deleted. When a customer account is deleted, all documents in the associated Content Bank will be removed.

Third party audit

Verizon Cybertrust Security performs security audits on the ArkadinAnywhere application.

Verizon Cybertrust Security has more than 350 security consultants in 18 countries with robust methodologies based on standards and certifications (OSSTMM, OWASP, CREST and CHECK). Their consultants have the following certifications:

- CESSG CHECK
- GIAC Certified Penetration Tester
- Certified Information Systems Security Professional CISSP
- ISACA Certified Information System Auditor (CISA)
- Payment Card Industry Qualified Security Assessor PCI QSA.



an
NTT Communications
Company

Verizon Cybertrust Security audits are manual penetration tests performed by their security consultants. Their security reports are referring to the OWASP methodology. Please refer to www.owasp.org for more details.

Arkadin commits to fixing any major security issue that might be discovered by Verizon Cybertrust Security.

Data Centers

Arkadin has deployed global audio and web conferencing platforms all around the world. These platforms are housed in world-class Tier 1 secured data centers located in major cities such as London, Paris, New York, Frankfurt, Hong Kong, Tokyo, Guangzhou, ChongQing, New Delhi, Gyeonggi, Sydney, Brazil, Singapore etc...

People allowed to access to any facility must be registered on the access list managed globally by the Arkadin security team.

