

Seven Key Considerations for a Successful Unified Communications Deployment



Contents

Seven key considerations for deploying unified communications successfully	01
Technologies covered	01
Organisational culture and change management	01
Environmental consideration	01
Architecture	02
Security	02
Ongoing support	02
Enterprise integration	03
Project management	03
Conclusion	03

Seven key considerations for deploying unified communications successfully

It's no secret that organisations are always on the lookout to maximise the use of their investment in technology, while at the same time delivering more flexible and effective ways for their employees to communicate and collaborate. Integrating all forms of communication – from telephony to e-mail, web conferencing to instant messaging (IM) – helps to deliver a richer communications environment and ultimately paves the way to cost savings and productivity increases.

Technologies covered

Although many vendors offer collaboration technologies, this document focuses on those from the Cisco and Microsoft stables as examples.

These include:

- **Telephony (IP PBX or TDM PBX)** – Cisco Unified CallManager
- **E-mail and scheduling** – Microsoft® Exchange Server
- **Unified messaging** – Cisco Unity or Microsoft® Exchange Server
- **Instant messaging (IM)** – Microsoft® Lync™ Server
- **Presence** – Cisco Unified Presence Server or Microsoft® Lync™ Server
- **Video, audio and web conferencing** – Cisco MeetingPlace, Microsoft® Office LiveMeeting
- **Corporate directories** – Microsoft Active Directory® (AD)
- **Collaboration servers** – Microsoft® Office SharePoint® Server
- **Desktop applications** – Microsoft® Office, Microsoft® Lync™ Server, Cisco Unified Personal Communicator (CUPC)

There are very few, if any, vendors today that offer a complete suite of collaboration technologies. There are even fewer organisations that have standardised on a single vendor for all of their communication needs. This presents a need to integrate multiple vendor technologies across multiple platforms and architectures. Before you embark on such a journey, be mindful that there are a number of elements that require careful consideration.

Organisational culture and change management

Before setting off down the unified communications or integrated collaboration paths, it is critical that your organisation's culture is receptive to the adoption of such technologies. You need to embrace the concepts of central document storage, multi-modal communications and the benefits that presence brings. If presence is viewed as 'big brother' or a privacy intrusion, if communication is purely e-mail based, if all collaboration is held in-person, in real-time, a unified communications project will be doomed to failure without proper training and change management.

Similarly, the IT team managing this environment needs to be well integrated and share responsibility for the success of projects. Unified communications touches everything from the PBX, to the server environment to the user desktop, and security is a critical component throughout.

In some instances unified communications technologies may not offer the value and gains anticipated. It is best suited to knowledge-based workers, workers who form ad-hoc or virtual teams, or who are geographically dispersed. Consulting teams, remote/home office workers and mobile workforces are ideal candidates to benefit.

Target the key employees who will benefit the most, align the delivery team and ensure the corporate culture is suited to interactive collaboration. Combine this with a well-planned and articulated change management process and the stage is set for a successful deployment.

Environmental considerations

After issues of corporate culture and IT responsibility have been addressed, the next phase is to assess and prepare the environment for the deployment of technology. Unified communications solutions rely heavily on accurate and consistent contact information. This information is usually stored in one (often more than one) directory. You need to select and maintain a single authoritative directory as a source of contact details. This should include:

- Full name
- Email address
- Telephone numbers
 - Work
 - Fax
 - Mobile
 - Home
- SIP/Presence/IM address
- Location

- a) **Prepare the directory:** Prepare the directory, e.g. Microsoft Active Directory®, for scheme extensions to support corporate IM and ensure the directory is synchronised correctly. Ensure numbers are normalised into a standard format (E.164 is frequently used) and that users understand how to enter numbers in this format to their own personal contacts.
- b) **Prepare the PBX:** The PBX may need configuration to accept the new numbering scheme and interpret it correctly. Additionally, some form of computer telephony integration (CTI) interface is required to enable telephony presence and call control. This may be a software license, a piece of hardware or may even require a platform upgrade, depending on the PBX. With Cisco CallManager, the CTI license is provided and only a presence (CUPS) license is required.

- c) **Prepare desktops:** Client software (Microsoft® Lync™ Server/CUPC) will need to be deployed to desktops. Desktops will need to meet the minimum hardware and software requirements for these applications. Soundcards and headsets may be necessary depending on the solution selected.
- d) **Prepare identities:** With all of these technologies coming together, a single user identity is important for accurate interaction between systems. For example, your email identity may be joe.soap@company.com, your IM address jsoap@hotmail.com, your AD user name jsoap, and your telephony identity your extension: 5222. In order to ease integration and identification, these identities need to be rationalised or synchronised in some manner so that the disparate systems know they all refer to the same individual.

Ultimately, of course, we will have a single identity used for all communications (likely joe.soap@company.com) and a selection will be made (by Joe, the caller, or even the network) as to the best medium to use for communication. Planning a suitable and flexible identity is critical, as this is the detail that will be shared extensively and will be hard to change or alter at a later stage. Think of the effort involved in changing your mobile number or postal address for instance.

Architecture

Now it is time to select a suitable architecture for your organisation. Will you decide on a distributed or centralised architecture? There are a large number of influencing factors affecting this decision, including:

- **Support** – are you equipped to support a distributed architecture from a staffing and systems perspective?
- **Security** – Which offers the most appropriate security and compliance architecture to meet policy requirements?
- **Underlying network infrastructure** – Will the underlying IP network support the bandwidth requirements for your choice of architecture?

Assessing the impact on the underlying infrastructure is key to a successful deployment. Many collaboration technologies rely on real-time protocols that put demands on IP networks to minimise latency and jitter. Therefore, quality-of-service policies must be in place and adequate bandwidth provisioned for.

Determine upfront what path communications will follow, assess the current network and predict impact and network changes necessary to accommodate these new applications.

Some vendors' applications may impose design constraints, so vendor selection also plays an important role when making architectural decisions. An implementation partner with experience in similar projects and thus some of the undocumented pitfalls associated with multiple vendor integration, will help ensure a sound architecture.

Security

Integrating multiple communication systems, many of which are mission critical to business operations, brings about many security considerations. After all, who can survive today without a telephone or e-mail system?

To secure unified communications, you should take advantage of capabilities that exist within network equipment (routers and switches) and encryption designed into the unified communications devices themselves. Security for these systems should be viewed as a natural extension of your existing security technologies like firewalls and intrusion detection. Keep in mind that security for unified communications should involve the infrastructure, call management, endpoints and application levels.

One of the main motivators for the deployment of enterprise IM systems is the additional security they offer through better control, conformity to corporate policy and archiving capabilities. In order to take advantage of these security and compliance features, consider the following:

- **Archiving** – Will communication sessions, especially IM, be archived and stored? Will this occur centrally or at distributed locations? What impact will this have on data storage systems such as network attached storage? Microsoft® Lync™ Server archives IM sessions in a SQL database. Ensure this database is secured and that adequate capacity has been provided for future growth of this archive – why intercept IM traffic when it can be stolen from an unsecured SQL database?
- **Federation** – Many organisations will wish to federate their Lync™ Server environments system with other organisations or public IM servers. This requires careful planning of certificates, server names and internet DNS entries. Plan what external connectivity will be required at the architectural stage and design accordingly.
- **Policies** – The implementation of suitable policies will determine the features enabled (file transfer, call control, etc.).
- **System security** – By implementing integrated collaboration tools, many systems throughout the organisation will be exposed to one another. PBXs will be exposed to the IP network via CTI interfaces, messaging and Presence systems will be exposed to the public Internet to enable remote connectivity and federation. Close attention needs to be paid to securing these previously isolated systems.

Ongoing support

Ultimately, the success of your deployment will depend on your ability to retain support staff who have the depth of skill to focus on all of the disciplines required (networking, voice, presence, messaging), can operate and conduct administration and troubleshooting of an integrated environment, and who can maintain the stability of the environment on a daily basis. An increasingly popular option is to outsource the maintenance and monitoring of the environment to a partner in order to reduce or eliminate the need for in-house support skills and administration personnel, and to reduce the risk of downtime that may result in revenue loss.

Enterprise integration

Once a solution has been deployed and users have become familiar with its use and features, there are opportunities to extend the system to deliver deeper integration and increased value.

- **Application integration** – Consider integrating presence and call-control into line-of-business applications such as ERP or CRM systems, allowing the applications to initiate calls, and show the presence status of users directly within the application.
- **Conferencing** – Integrate the call control and presence tools into collaboration systems such as Cisco MeetingPlace. This allows users to seamlessly escalate a call to an audio or video conference and share desktop applications such as spreadsheets and presentations.
- **Customisation** – Customise the information displayed in the Lync™ Server client or on the screen of the IP phone to suit your needs. Display order information on the phone when a client calls or a list of shared documents in Lync™ Server when a colleague sends an instant message.

Project management

Enlisting a partner with a sound project methodology coupled with proven experience in deploying small and large scale projects, will give you a better chance of success and satisfaction. It's important that your implementation partner bases its deployment on a structured project management methodology that consists of a set of processes, tools, templates and guidelines based on industry best practices.

A sound project management methodology simplifies and standardises the way that the project will be delivered and also improves manageability through standardisation and tools.

In addition, ensure that your partner of choice documents the deployment. A documentation handover reduces the future risks of disaster and downtime and assists you with change management and training.

Conclusion

Steering for Success

The world of corporate communications is experiencing a revolution. Communication media are going to be tightly integrated with users selecting appropriate communication methods based on context, availability, situation and location. Many existing systems won't need to be completely replaced and can be incorporated today.

A successful deployment comes from selecting appropriate end-users, careful planning and an architecture that takes security and ongoing support into consideration.

Most of all, partner with an integrator that has the skills and experience to integrate multi-vendor technologies, follows a transparent and strict project management discipline and can offer ongoing support and maintenance throughout the solution's lifecycle.



MIDDLE EAST & AFRICA

ALGERIA • ANGOLA
BOTSWANA • CONGO
DEMOCRATIC REPUBLIC OF THE CONGO
GABON • GHANA • KENYA
MADAGASCAR • MALAWI
MAURITIUS • MOROCCO • NAMIBIA
NIGERIA • SAUDI ARABIA • SOUTH
AFRICA • TANZANIA • UGANDA
UNITED ARAB EMIRATES • ZAMBIA

ASIA

CHINA • HONG KONG
INDIA • INDONESIA • JAPAN
KOREA • MALAYSIA
NEW ZEALAND • PHILIPPINES
SINGAPORE • TAIWAN
THAILAND • VIETNAM

AUSTRALIA

AUSTRALIAN CAPITAL TERRITORY
NEW SOUTH WALES • QUEENSLAND
SOUTH AUSTRALIA • VICTORIA
WESTERN AUSTRALIA

EUROPE

BELGIUM • CZECH REPUBLIC
FRANCE • GERMANY
ITALY • LUXEMBOURG
NETHERLANDS • SPAIN
SWITZERLAND • UNITED KINGDOM

AMERICAS

BRAZIL • CANADA • CHILE
MEXICO • UNITED STATES