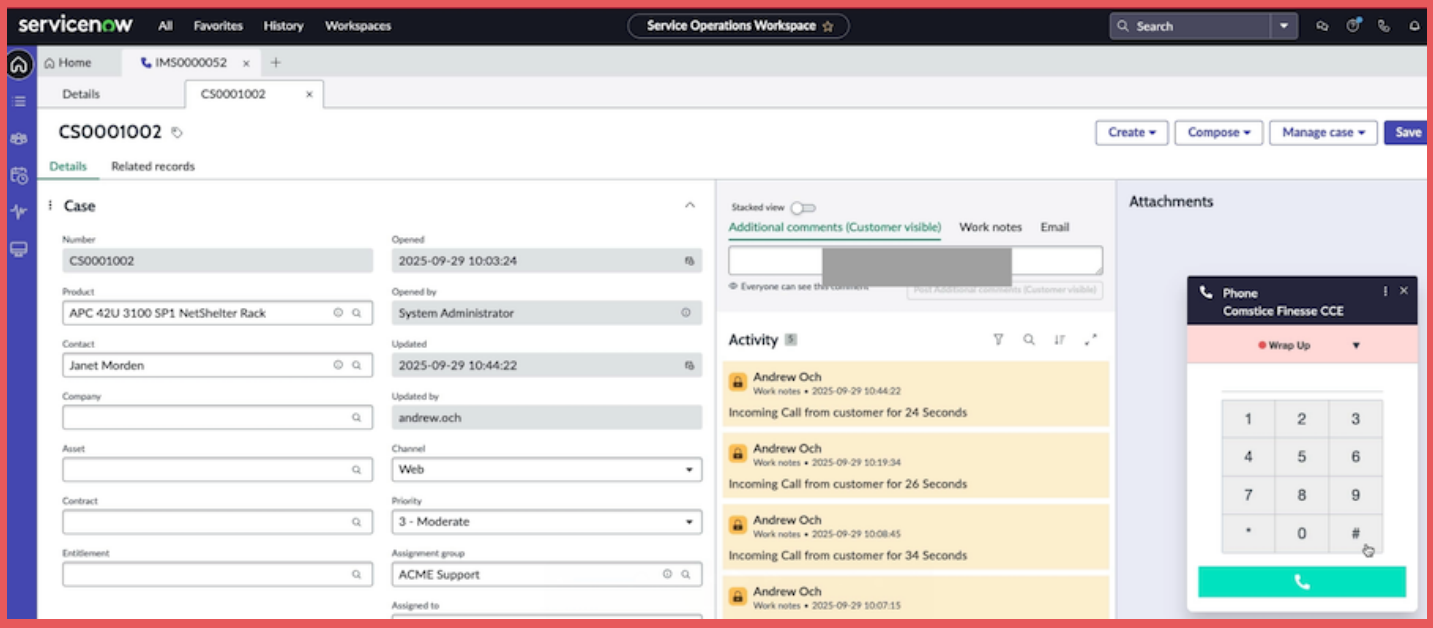
Comstice

Comstice ServiceNow Webphone for Cisco

Cisco Enterprise Users and Finesse Agents



Comstice Webphone for ServiceNow - Cisco

Comstice Webphone is a WebRTC Phone on the browser and it gets coverted to a SIP Phone on the client's network. Comstice WebRTC Gateway helps WebRTC sessions to be converted to SIP and reach out to the company's enterprise telephony and the PSTN without installing anything on the user side. It runs **on-premises** or **in your private cloud**.

No Installation Needed

WebRTC standard helps users to utilise any modern web browser including Microsoft Edge to make and receive voice and video calls as well as screen sharing on the browser with full encryption. It is the same technology used by Microsoft Teams and similar services.

Agent Functionality

Comstice Webphone also includes Cisco Finesse agent login, state changes and call control features. It uses Cisco Finesse RESTFul APIs. Therefore, for Cisco Finesse, it is not any different than

Supports Cisco CUCM

All Comstice Webphone scenarios support Cisco CUCM integrations. For enterprise users, Comstice Webphone can register as a third-party SIP Phone. For the Finesse agents, Comstice Webphone registering to Cisco CUCM as a third-party phone is not supported. Hence, it will register to Comstice SIP Proxy and Cisco CUCM will have a SIP Trunk with Comstice SIP Proxy.

Take aways about ServiceNow Webphone

- No need to go to a shared cloud call center service
- Webphone is not only for call center agents; enterprise users can use as well.
- No installation needed; No Jabber, no VPN client or any installation needed.
- Four times faster to handle calls and run outbound campaigns
- Faster Outsource agency integration and remote agent onboarding

Screen-Pop and Click to Dial

ServiceNow offers a webphone framework called **OpenFrame**. This helps to enable the phone icon on the top right corner of the agent pages. It also helps to do screen-pop and click to dial.

Screen-Pop for the Incoming Call

ServiceNow can be configured to do a screen-pop of the caller's contact details or the incident page if the caller has entered an incident number or the contact is associated with an open incident. (Check out Comstice ServiceNow videos)

If the caller is not associated with any incident or did not enter an incident number in the IVR, then a new incident form can be opened in the screen-pop.

Enterprise user who is not a call center agent can also have screen-pop.

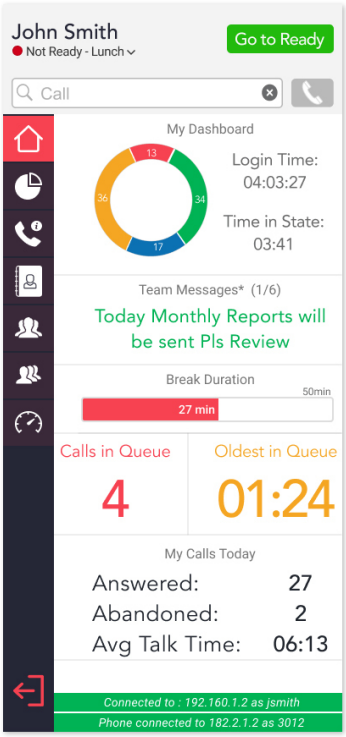
Click to Dial

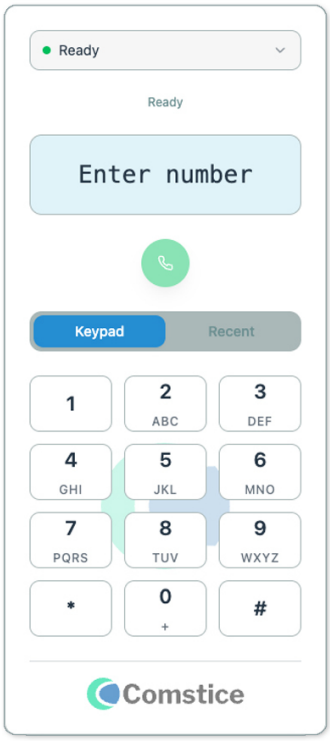
Once ServiceNow webphone is enabled, Phone number fields in the Contact pages will have a phone icon activated. (Check out Comstice ServiceNow videos). If the number manipulation is needed, Comstice Webphone can handle that on its configuration for outbound prefix 9 etc.

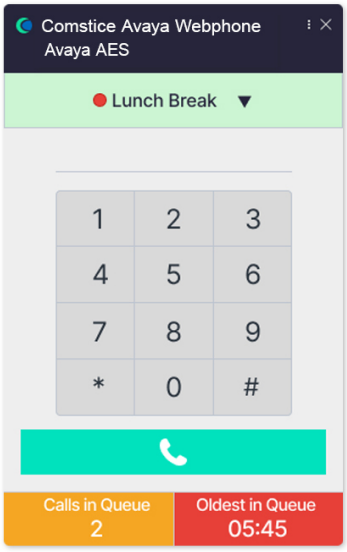
Comstice Wephone Skins

Comstice Webphone has different design options based on your business requirements. It can be as simple as a mini webphone or it can have many built-in features such as call logs, team member states, real-time queue information, agent's daily performance.

Call logs and agent performance information can also be accessible as a separate side menu item, outside the webphone user interface.



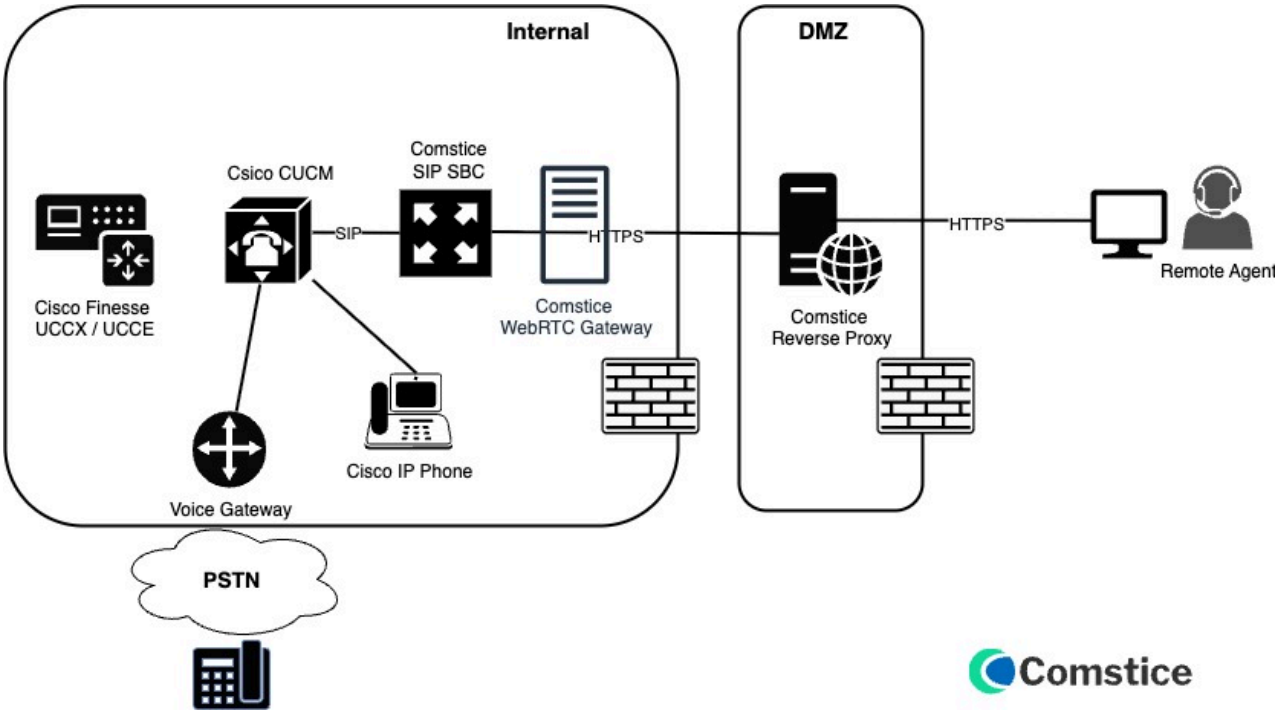




Integration with Cisco

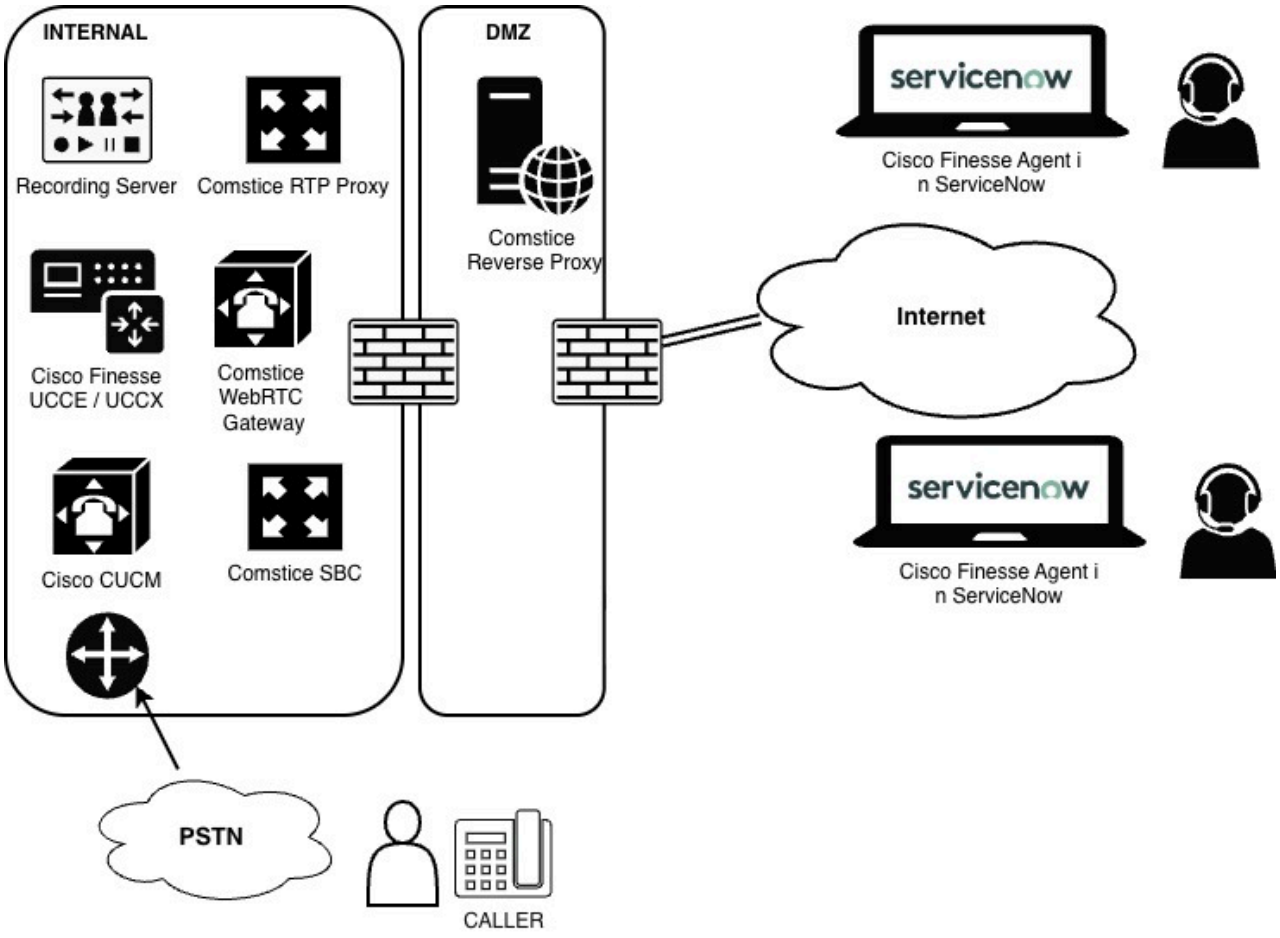
Comstice Webphone can be integrated with Cisco CUCM. WebRTC sessions can register directly to Cisco CUCM or they can be registered to Comstice SIP SBC and then access to Cisco CUCM via SIP trunk.

Webphone also supports Cisco Finesse REST APIs. Using HTTPS APIs, agent can login, change states, control calls via Finesse for the full contact center monitoring and reporting.



Comstice Webphone Finesse Topology

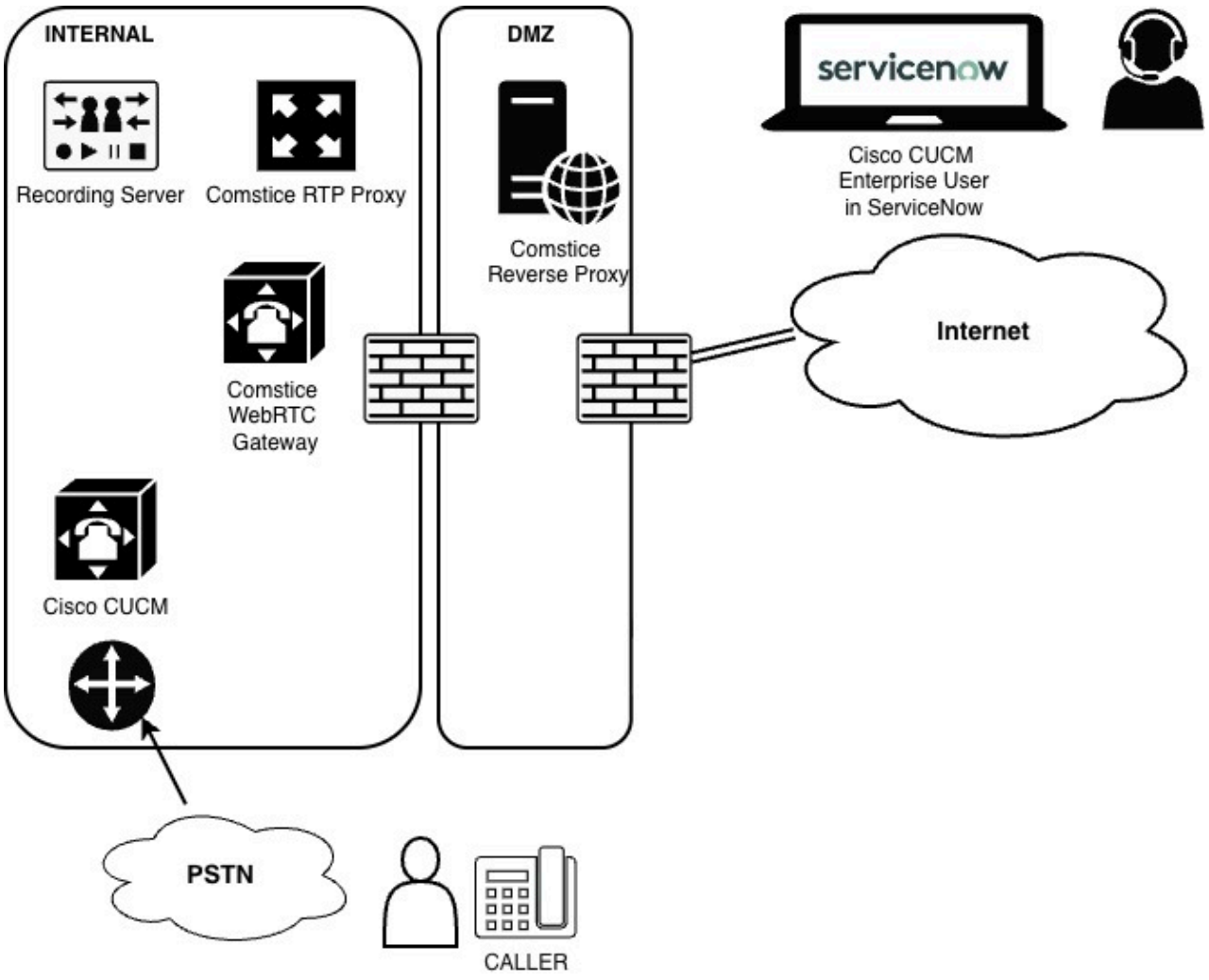
Comstice Webphone solution can have the agent login details built-in and populate agent username, password and extension automatically. Finesse integration is done through Finesse RESTFul APIs.



Comstice Webphone Topology for Cisco CUCM

Comstice Webphone can register as a third-party SIP Phone to Cisco CUCM. There will be two legs of the call;

- From agent web browser to Comstice WebRTC Gateway, it will be WebRTC; signalling will be HTTPS and audio will be secure RTP. Both signaling and audio will be fully encrypted.
- SIP leg of the call will be between Comstice WebRTC Gateway and the other party's phone or voice gateway. Since this leg of the call is purely internal, encryption is often disabled.



Audio Recording - Cisco

Audio recording will be different for web phones; instead of Cisco CUCM built-in bridge, SIPREC protocol will be used. Comstice Webphone integrates with Calabrio, Verint recording and any other platform that support SIPREC. Comstice also offers **audio recording** solution that can be bundled into the solution as well.

Port Utilization - Cisco

The following ports must be opened towards Comstice Reverse Proxy on your DMZ network;

External to DMZ

Port	Protocol	Destination
443,8445	HTTPS	Comstice Reverse Proxy
20000-23000 (Configurable)	UDP	Comstice Reverse Proxy

DMZ to Internal

Source	Port	Protocol	Destination
Comstice Reverse Proxy	8445	HTTPS	Cisco Finesse Servers
Comstice Reverse Proxy	8189 (Configurable)	HTTPS	Comstice WebRTC Gateway
Comstice Reverse Proxy	20000-23000 (Configurable)	UDP	Comstice WebRTC Gateway
Comstice Reverse Proxy	5060 (only internally, there is no SIP on the external call leg)	TCP/SIP	Comstice SIP Proxy

Cybersecurity Questions Answered

Comstice Webphone works securely without any VPN required. You may get questions from your Cybersecurity team such as;

- "If we open a port in our firewall, we will get attacked"
- "Application-level hacks can compromise our customer data"
- "Our internal applications may get affacted"

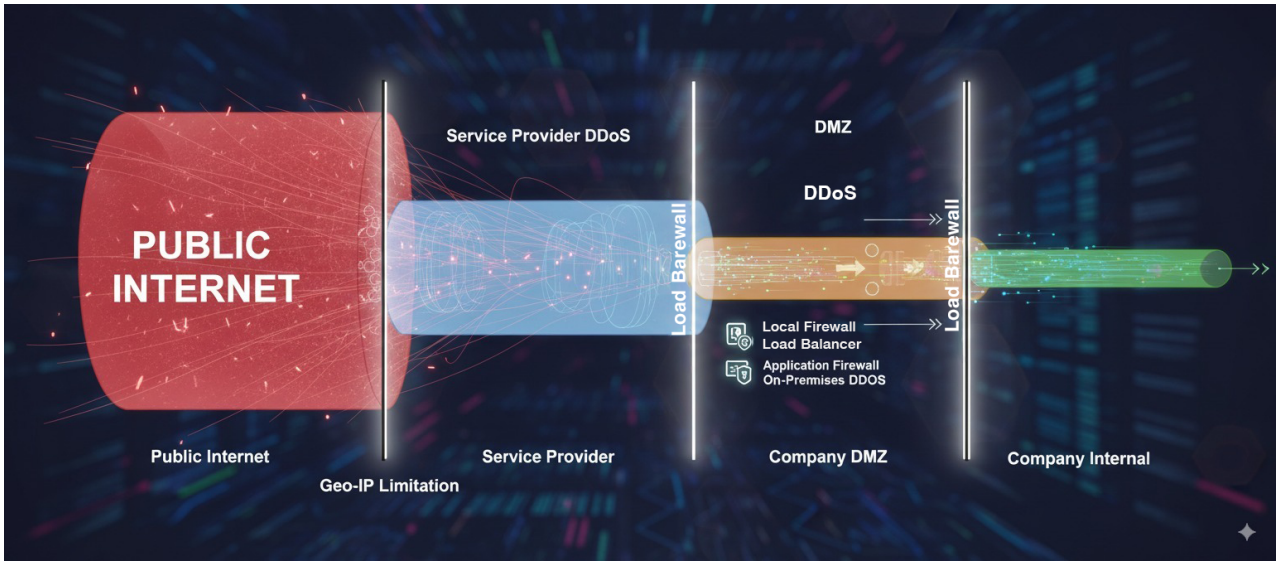
Application-level risks are mitigated by single sign-on with multi-factor authentication and time-limited IP whitelisting for the remote user. But this **"we will get attacked"** threat stops many businesses.

Demystifying DDoS Attacks

Attacks referred are the distributed denial of service attacks; sending extreme amount of connection requests to exhaust your network. Let's see how real they are, what machanisms you already have and how you can test and mitigate risks

1. You can get attacked at anytime

This idea of "If you open a port, they will attack your network" is not reflecting the reality. Today, even AWS and Microsoft Azure can get attacked and get brought down. That's why organizations create a layered mitigation structures and it starts from the service provider level.



Cybersecurity Challenges -

2. Your Standard Firewall has limits

Firewalls have a limit of handling the maximum number of packets per seconds. If it gets data levels beyond that, it will struggle and may go down. That's why many businesses use tiered firewall levels i.e. external and DMZ. Also application firewalls and load balancers are used to distribute the packet analysis load from the standard firewalls to them. Finally, your organisation may have Intrusion Detection / Intrusion Prevention solutions, either on-site or as a service from CloudFlare or similar providers. This helps to apply additional methods such as rate limiting, data blackholing (instead of denying packets, routing them to a null destination)

3. Your Business Should Have DDoS Tests Done Quarterly

You should work with a third-party testing company to review DDoS mitigation points every three months. Attack methods and other DDoS mitigation technologies change very rapidly. Quarterly audits will help to stay up to datr. Comstice recommends SafeDash **(https://safedash.co.uk)** as an independent testing partner.

4. Comstice apps can whitelist user IPs during the shift

Once the user is authenticated in the Comstice applications or CRM platforms, Comstice can whitelist the browser session and the IP address of the remote user for 8-10 hours. This helps to have additional security on top all all the security measures described above.

Roles and Responsibilities - Cisco

Here is a draft project steps and the timelines for rolling out Comstice Webphone for ServiceNow. Configurations will be done remotely using screen-sharing via Webex or Microsoft Teams.

Task	Owner	Duration
Download and Deploy Comstice OVAs (or provide Customer-Licensed Redhat VM)	Client	2 days
Internal and External Firewall configurations	Client	2 days
Cisco CUCM and UCCX, UCCE and PCCE Configurations	Client and Comstice	2 days
Comstice Server Configurations for Client's Cisco Telephony and Network	Comstice	2 days
ServiceNow Configuration and Testing	Client	2 days
UAT	Client and Comstice	2 days
Admin Training	Comstice	1 day
Power User Training	Comstice	1 day

Software Updates and Day 2 Support

Software Updates

Comstice Webphone solution components run as Docker containers. Each service is like a mini virtual server. Comstice provides updates for the software as new Docker image files. It is very quick (within minutes) to update and rollback, thanks to Docker container based environment.

Software updates can be done by the client/partner or by Comstice over the webex.

Break-Fix Support

Comstice also offers break-fix support as an escalation point. On the Admin training, client's IT personnel will have the troubleshooting flows. If the troubleshooting flow points out a Comstice escalation, you can access to Comstice Service Delivery Manager, Comstice Support phone numbers and Comstice support ticket page from https://comstice.com/support