ivanti

FedRAMP

FedRAMP Infrastructure Connections

White Paper

Date: October 28, 2019

Audience: Federal Agencies

Owner: Jennifer Thomas

Classification: Internal only, unless specifically requested by government agency. Share on case-by-case basis**.**

SMEs: Derek Murphy, Douglas Lippi, Brent Taylor, Anthony Eaton

Notice

This document, the *Ivanti Enterprise License Agreement Program Guide*, provides an overview of the Ivanti Enterprise License Agreement and describes how the agreement works and the specific products included. The program guide is subject to change and clarification without notice. In all cases, the version posted on the Ivanti Legal web page is the governing version for contractual purposes.

If you have questions about the program or any of the content in this document, please contact your Ivanti sales representative or send an email to the ELA team.

Contents

Executive Summary

Ivanti delivers world-class and proven IT Service Management (ITSM) capabilities on a true multi-tenant, built-for-purpose platform. Modeled and built specifically for the cloud environment, Ivanti delivers the most comprehensive cloud service management solutions with world-class availability, reliability, and security.

Our highly secure Compute Environments utilize state-of the art electronic surveillance and multi-factor access control systems. These geographically distributed sets of Compute Environments maintain service continuity in the event of a disaster or other incident in a single region. High-speed connections between the Compute Environments help to support swift failover. Management of the Compute Environments is also distributed to provide location-independent, around-the-clock coverage and system administration.

Ivanti ISM FedRAMP Compute Environments have been designed to provide optimum availability for our government agency customers while ensuring complete customer privacy and segregation. This white paper provides details about the infrastructure connections that customers can use to get started quickly.

There are several connections that can be used to integrate Ivanti Cloud with your business. Talk to our Ivanti Technical Staff who can review the options with you. The most common connections are listed in this white paper for your reference.

Core and Common Infrastructure Connections

1. Authentication

Ivanti Cloud supports four main types of Authentication:

1. Active Directory LDAP (or LDAPS) connection allows for your Active Directory user accounts to be synchronized with your ISM tenant database.
2. Local Authentication using Ivanti Cloud-defined username and password stored in your ISM tenant database (no integration with a third-party system).
3. Sign-on using OPENID authentication protocol.
4. Single Sign-On (SSO) using a SAMLv2-based authentication protocol. Ivanti Cloud supports multiple Authentication providers that include Microsoft ADFS, Ping Identity, Okta, Symplified, and many others. This is the most common and recommended method as it will commonly result in Single Sign-On capabilities.

2. Bulk User Import

This will import user data (like email, phone, department, etc.) from your user store i.e., Active Directory, into your ISM tenant database. Commonly this is done by LDAP/LDAPS read-only import and is separate from the authentication method.

3. Ivanti Cloud Sending Emails to Your Users

Commonly called an SMTP gateway connection, the Ivanti Cloud system will enable the user to send emails via your SMTP Mail Services. This means that you leverage your own email systems to reduce cost and have the emails originating from your own domain.

4. Ivanti Cloud Receiving Emails from Your Users

Ivanti Cloud can connect to and monitor mailboxes in your Mail system via IMAP, IMAPS, POP3, or POP3S. This allows the Ivanti Email Listener to pick up emails sent to an address on your domain and create Incidents automatically based on the sender's email address.

5. Advanced Connections

Ivanti Cloud can support several advanced integrations. Depending on your requirements and purchases, the Ivanti implementation team will enable whatever is appropriate for your usage. The more common integrations scenarios are:

SCCM Connector: A connection into your Microsoft® SCCM database to allow your SCCM-discovered assets to be synchronized into your ISM tenant database.

Third-Party Integrations: These connections are possible depending on the requirements; for example, to Salesforce, network monitoring tools, TFS servers, and SharePoint. These connections are handled on a case-by-case basis and often require a VPN connection. (See section 6.0.)

Bulk Data Import/Export: It is possible to import and export data via CSV, XML, or text files commonly transferred via FTP/FTPS or HTTP/HTTPS. These connections are also handled on a case-by-case basis.

6. VPN Connection

Ivanti Cloud supports dedicated IPsec VPN connections for back-end integrations. VPN connections are used when the customer side restricts access for Ivanti Cloud offerings via the internet, due to firewall restrictions and security policies.

Ivanti can provide a redundant VPN tunnel to the main site as well as a DR site at an additional charge per year. It is important to note that VPN is not used for user access, but only for system-to-system communication.

Our devices in the Compute Environment will be able to connect to any enterprise-class router/firewall (such as Cisco router or firewall) using standard IPSec protocols.

IPSec is the industry standard for secure tunneling and 99.9% of VPN tunnels use this, with a selection of encryption levels that can be applied based on exact customer requirements. Please contact your Ivanti implementation team for details regarding a VPN solution.

7. Requirements for Core Connections

For customers that allow traffic over the internet, firewall rules will need to be open to allow connections from the list of Ivanti Cloud IP addresses.

List of Public IPS Used by Compute Environments
Primary Compute Environment
18.233.3.236
DR Compute Environment
34.208.112.206

8. Ports Required

Depending on your configuration, the ports required can be configured. Sections 8.1, 8.2, and 8.3 below discuss the common ports that Ivanti Cloud can be configured to:

8.1. LDAP Import and Authentication

The Lightweight Directory Access Protocol (LDAP) is used to read/write to/from Active Directory. By default, LDAP traffic is transmitted unsecured. You can make LDAP traffic confidential and secure by using Secure Sockets Layer (SSL)/Transport Layer Security (TLS) technology. You can enable LDAP over SSL (LDAPS) by installing a properly formatted certificate from either a Microsoft Certification Authority (CA) or a non-Microsoft CA with due support from Ivanti Cloud's Technical team.

Ivanti Cloud can be configured to use all three protocols—LDAP, LDAPS, and Start-TLS. Both Start-TLS and LDAP use port 389 by default. LDAP is not recommended over the Internet as it is in plain text and considered unsecure. LDAPS uses Port 636 by default. Additionally, a read-only account with permissions to the user directories is required.

You must provide the following details:

Detail	Customer Inputs
IP/Server URL **of LDAP server**	
Base DN:	In the format: Ou=My Org Unit,dc=mydomain,dc=co m
Active Directory Username	In the format: AD\username (with Read Only access)
Password	
Use SSL	Yes/No
Certificate Sent	Yes/No

If using LDAPS for Authentication, you must provide a base64 Public key only (not the private key) and the LDAP certificate file from your LDAP server must be uploaded to your ISM tenant. Send these details to your Solution Manager in charge of your implementation. For more information on this refer to: http://support.microsoft.com/kb/321051

8.2. SMTP Connection

Set up an SMTP connection to allow emails to be sent to your organization from Ivanti Cloud. **You must provide the following details:**

Detail	Customer Inputs
SMTP Server setting	External IP Address
SMTP Port	Set to Port 25 by default
Authentication	Can be None /AuthLogin / Cram MDS / NTLM. If required, please enter username and password.
Use SSL/TLS	Yes/No
Username	
Password	

8.3. Mail Account for Email Listener Connection

This allows incidents to be generated automatically from email.

You must provide the following details:

Listener	Customer Hosted Mail Box
Email Address	
Host Mail Server External IP Address	
Host Server Fully Qualified Domain Name	
Port	110 / 995 (default ports for non-SSL and SSL POP3)
Username	143 / 993 (default ports for non-SSL and SSL IMAP4)
Protocol	POP3/IMAP4
Authentication	Plain / APOP / AuthLogin / CramMD5 / NTLM
Username	
Password	

This document is only meant to give you an idea of the minimum inputs required from your end. Your Ivanti Cloud software implementation team will suggest and implement the most appropriate connection for your needs. For any further information please contact your Ivanti Cloud implementation coordinator.

9. Trusted Internet Connections

Some government agencies will require more secure connections based on their requirements and the sensitivity of the data being processed in the cloud via Ivanti Service Manager. For these customers, we offer the following options:

- Ivanti Cloud may provide routes on all government traffic via VPN back to an agency network if requested.
- Ivanti Cloud may provide routes on all government traffic through an agency-sponsored MTIPS, in which no government traffic is allowed over the public Internet if requested.

These options are considered special implementations and require additional time and increase in overall price to be fully implemented.

10. Revision History

Version	Date of Change	Responsible	Summary of Change
1.0	August 2018	Toby Foss	Doc creation.
1.2	August 27, 2019	Elaine Atkinson	Doc revisions per Douglas Lippi's edits. Previously reviewed by Rebecca Botvinik for accuracy of content.
1.2	August 30, 2019	Elaine Atkinson	Derek's IP NOTE added at bottom of doc.
1.2	October 28, 2019	Jennifer Thomas	Updated List of Public IPS Used by Compute Environments table, minor language changes, removed mention of Rebecca Botvinik