Intel® Cloud Builders Guide
Intel® Xeon® Processor-based Servers
McAfee Cloud Identity Manager

Intel® Cloud Builders Guide to Cloud Design and Deployment on Intel® Platforms

McAfee Cloud Identity Manager

Intel® Xeon® Processor 5500 Series

Intel® Xeon® Processor 5600 Series

McAfee | Cloud Identity Manager

Audience and Purpose

Cloud computing offers a path to greater scalability and lower costs for service providers, infrastructure hosting companies, and large enterprises. Establishing an infrastructure that can provide such capabilities requires experience. Intel has teamed up with leading cloud vendors through the Intel® Cloud Builders program to help any customer design, deploy, and manage a cloud infrastructure.

This reference architecture focuses on securing the access to applications proliferating in the cloud, where the traditional enterprise access control methods and solutions are not sufficient and have to be extended or complemented. Identity and Access Management (IAM) systems are mature and well established in the enterprise IT arena and do a good job of securing applications running within the enterprise network perimeter. But these solutions tend to be large, monolithic implementations that require a lot of effort and cost to extend to support applications in the cloud. This document lays out in detail the McAfee Cloud Identity Manager solution architecture that will help secure access to cloud based applications.

The intended audiences for this document include enterprise architects, security architects, network architects, enterprise IT managers, and business managers who are responsible for implementing and maintaining the appropriate security model for a particular enterprise, and have genuine concern around securing the applications and data that now reside outside the traditional enterprise network perimeter. These include organizations that are on both sides of the cloud ecosystem – enterprises that use cloud services, and providers that host these cloud services.

March 2012

Table of Contents

Executive Summary

Enterprises of all sizes are embracing cloud computing because of the many advantages it provides. These include lower costs, greater business agility, reduced IT administrative overhead, access to best of breed applications, and more. The legacy ERP applications are being replaced by cloud-based applications that address virtually any conceivable business need: sales, marketing, human resources, collaboration and communication, finance, legal, etc.

However, this proliferating profusion of cloud based solutions has created a daunting operational challenge: how to efficiently manage the profusion of identities that users require – one for each cloud application they access. For instance, if you have 1,000 employees, each accessing 10 cloud applications on average, that's 10,000 unique identities to manage. The best way to address these concerns is to deploy strong identity management processes and technologies to ensure that only authorized users have access to cloud applications.

The traditional heavyweight, monolithic enterprise Identity Management solutions do not extend easily to the cloud, and do not address the full spectrum of enterprise class security capabilities required to deploy critical applications to the cloud. These solutions are complex and require a lot of effort to deploy, and once deployed are expensive to maintain and not completely secure.

The Intel® Cloud Builders solution uses the McAfee Cloud Identity Manager Software to design, deploy, and manage an effective and efficient identity and access management solution for software-as-a-service (SaaS) applications. McAfee Cloud Identity Manager can control the entire lifecycle of user access security for enterprises connecting to cloud applications. It delivers a comprehensive 3-in-1 solution combining user account provisioning, cloud federation/single sign on (SSO) and strong multi-factor and context based authentication.

Introduction

Security Challenges for Applications in the Cloud

With the proliferation of applications and infrastructure to the cloud, organizations adopting cloud apps are concerned about overwhelming security complexity and the lack of comprehensive solutions that can effectively project an enterprise-class security model on the cloud. Some of these concerns include:

- Multiple Logins/Weak Security: Users have different credentials in each of the cloud applications, stored natively in those applications. Users tend to create weak passwords when there are too many passwords to remember. This compromises the security of the solution especially when the application is accessible from outside the enterprise network.
- Manual Provisioning: In most cases the user access is not automatically provisioned or de-provisioned with the cloud application; users have access to the application even after they have been terminated or if they are no longer authorized to access the application. This also increases the cost of administering users, due to lack of automated processes.
- Lack of Visibility: With users accessing applications running in the cloud, there is no easy centralized/consolidated view of who has access to what, and who accessed what at any given time. This results in SaaS users lacking oversight or authorization, leading to sensitive data leakage and compliance risks. To minimize this risk, without a centralized cloud Identity and Access Management (IAM) solution in place, the traditional method is to retrieve access logs from each of the cloud apps and have them consolidate and correlated for visibility. This is an expensive and time consuming process, and does not provide timely notifications to immediate action, nor does it prevent unauthorized access.
- When applications are running within the enterprise network, a single factor authentication (uid/pwd) may be sufficient. But when critical apps are put in the cloud, a stronger authentication method is required to have a higher confidence in identity proofing and validating who the user says he/she is.

The McAfee Cloud Identity Manager Solution

So how does the enterprise regain control in an environment where security models change by cloud provider or are left entirely up to the enterprise? McAfee Cloud Identity Manager Software is the first solution suite designed to control the entire lifecycle of identity and access management for cloud security providing Identity Federation based SSO with strong authentication and provisioning. McAfee Cloud Identity Manager Software is the McAfee branded version of Intel® Expressway Cloud Access 360. Note that some diagrams in this reference architecture may reflect the original Intel brand name.

Capabilities:

- **Control**: Manages the identity lifecycle with policy driven automatic account provisioning/de-provisioning to cloud applications. This ensures that only authorized users get provisioned to cloud applications, and as soon as they are terminated or their role changes, their account is automatically de-provisioned. For user access control, it minimizes the risk of unauthorized access to the applications, by

enforcing user identity and context based authorization, applying strong authentication, and eliminating passwords by creating a federation trust between the enterprise and the SaaS provider.

- **Visibility**: Since all access control is managed by McAfee Cloud Identity Manager, there is better visibility of user access, via a centralized management and reporting console. It can monitor user, administrator and API access activity and send alerts against SLAs.
- **Strong Authentication**: Has a built in One Time Password (OTP) solution, that can be used to provide a multi-factor stronger authentication or when the risk based on the context is higher. This is critical in protecting applications that have sensitive data where one needs a higher level of authentication. To ensure only authorized users log on to such applications, you need to go beyond single-factor authentication based on what you know (username and password), and add a second factor based on what you have: a one-time password. In a situation where passwords are compromised, this will prevent unauthorized access to cloud resources, especially when users access the application from networks or locations outside your control.
- **Compliance**: Maintains audit records of identity lifecycle events and correlates user cloud activity with on-premise logs for end-to-end compliance. It also is capable of detecting orphan accounts, and automatically de-provisioning the accounts from the target cloud system.
- **Connectors**: Comes with pre-built Identity and Cloud Connectors. Identity Connectors allow the choice of a range of authentication sources (LDAP, RDBMS, SAML2, Social Network logins like Facebook, Google, Yahoo, Twitter etc., OTP, Certificate, Identity Protection Technology etc.). Cloud Connectors allow federated SSO and provisioning integration with popular IdM systems and cloud providers and supports industry standards (SAML, OAuth, and OpenID).

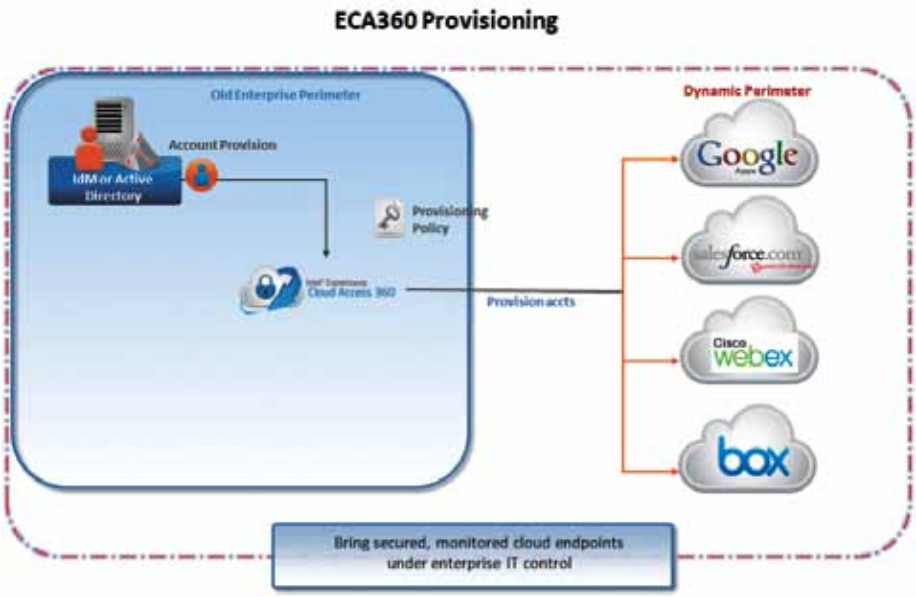


Figure 1: ECA360 Provisioning

Product Overview

McAfee Cloud Identity Manager is a Cloud Identity Management solution that is available in two scenarios:

- Identity to the Cloud: IAM for SaaS applications from an on-premise platform
- Identity in the Cloud: IAM for SaaS applications from an on-demand platform in the cloud

This paper is going to be focused on the on-premise version of the product.

McAfee Cloud Identity Manager is based on proven, standards based technology available as an integrated suite with modules for provisioning, SSO, and One Time Password.

Provisioning

McAfee Cloud Identity Manager Provisioning Module has functions for distribution, synchronization, compilation, and follow-up of identity and attributes information. Two-way provisioning is also supported, which means that connected systems can be both source and receiver of identity and attribute information.

The product is a policy-based service that in a flexible way can leverage the rules and policies decided on within a company regarding the handling of identity and attribute information to a set of automated actions. It can communicate by Web service or directly with all modern databases or LDAP v3 directories.

An image of so-called integrated identity information is constructed in the service. In short, this means that it can work towards one or more data sources in order to compile a configurable image of what an object (user, units, groups, roles, etc) looks like. This image of the object can then be treated in different steps, and be distributed and stored in various data sources.

By exploiting the provisioning features, companies and organizations can ensure good quality of data between systems and processes. This is important especially when planning to carry out extensive migration of information between systems, which often follows a defined workflow.

The powerful reporting features that are included in McAfee Cloud Identity Manager will help to create an increased visibility of the assets that exist within an organization. It can include everything from licensing to system access for employees. It can also provide an overview of how information from different sources is consistent. Both predefined reports and adjustments for custom supported the basic version of the AAM.

The combination of systems and processes supported by the Provisioning Module also follows the thoughts on "best practices" contained in frameworks such as ITIL, MOF, and the like. The Provisioning Module is a powerful feature that uses existing infrastructure and resources so there are no hidden costs or expensive investments.

Some of the key benefits of the Provisioning Module include:

- Connectors to all modern systems including:
  - Web service (SOAP)
  - LDAP v3 directories
  - Databases
  - File Import/Export
- Includes many actions, no developer knowledge required
- Rapid deployment; ery fast and flexible implementation
- Easy to move configuration from test to production environment
- Leverages existing infrastructure and resources

Federation and Single Sign-On to Cloud Apps

McAfee Cloud Identity Manager's SSO module provides standards based federation to cloud based applications for both Identity Provider (IdP aka asserting party) or Service Provider (SP aka relying party) scenarios. The SSO module provides seamless single sign-on for enterprise users to cloud applications. This module also includes a built-in SSO Portal acting as an application launch pad for the users. Connectors to common identity sources (Active Directory, LDAP, databases, Facebook, Google, Yahoo, and Twitter etc.) and to popular SaaS/PaaS (Platform as a Service) platforms are included in the package. A Web-based administrative console makes it easy to create, monitor, and control SSO access. Federated authentication and authorization protocols are based on Security Assertion Markup Language (SAML 2.0), eXtensible Access Control Markup Language (XACML) and emerging OAuth and OpenID identity standards that can connect Internet identity providers (e.g., Facebook) with corporate identities and authorization policy.

Cloud SSO improves end-user convenience and productivity – users log on once to a trusted, secure portal controlled by their enterprise (either on-premise or in the cloud), and access authorized SaaS applications with a single click. Cloud single sign-on requires a high degree of integration between the IAM/SSO system and the target application(s).

The SAML is the standard of choice for authentication and authorization between domains. SAML has several important attributes:

- SAML is a widely adopted standard which is supported by most major SaaS application vendors.
- SAML is based on a proven federated trust model.
- SAML doesn't require a password. A SAML-protected service provider relies on the ability of a trusted identity provider to verify a user's identity.

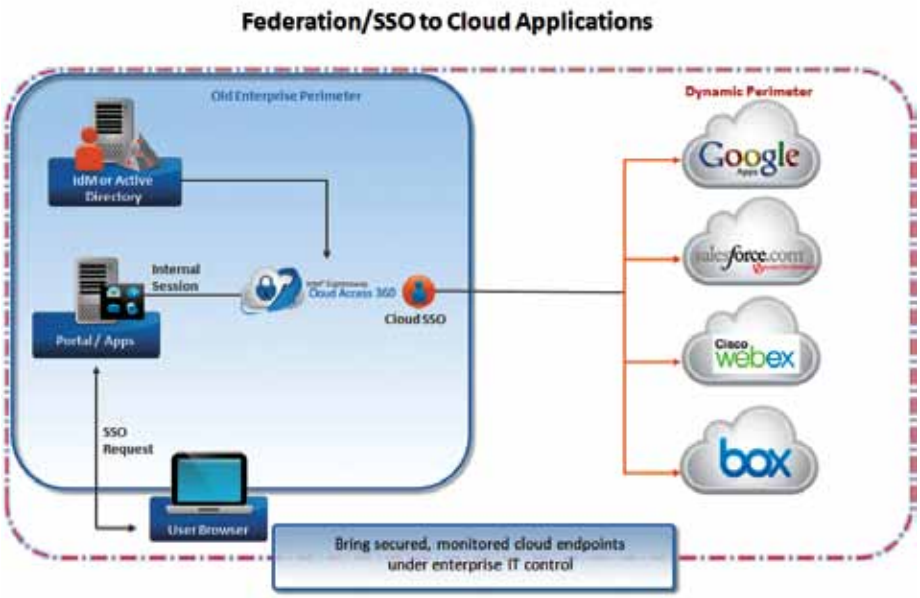


Figure 2: Federation/SSO to Cloud Applications

Identity Connectors: Used in an Identity Provider scenario, Identity Connectors provide the ability to connect to authentication sources to seamlessly authenticate the users. McAfee provides out of the box connectors to authentication sources including LDAP, any JDBC compliant database, Active Directory (including Integrated Windows Authentication), any OpenId provider (like Google, Yahoo etc.), any social network credentials (Facebook, Twitter, LinkedIn etc.), SAML assertion from a trusted IDP, Salesforce, CAS, strong authentication solutions like X509 certificates, OTP (Intel or other third party solution), CAS, and Intel IPT. The Identity Connectors can retrieve any available user information from the identity sources and make it available to the Cloud Identity Manager to use for subsequent SSO actions.

Cloud Connectors: In an Identity Provider scenario, once the user is the authenticated using an Identity Connector, McAfee provides pre-built connectors to enable trusted federation with target SaaS applications. There are over 100 pre-built connectors available to popular SaaS sites, and the list is growing pretty rapidly. There are four types of cloud connectors currently available:

- SAML2-Based Connectors: These connectors use SAML2 as the protocol for federating to the target apps. There is also a generic SAML2 connector available that can be used to connect to SAML enabled SaaS apps.
- Proprietary SaaS connectors: Several SaaS providers do not support SAML2 and have their own method for SSO. McAfee Cloud Identity Manager includes connectors for some of these popular target SaaS apps.
- Token-Based Connector: This connector is specifically built to provide SSO to custom Java or .NET apps. A Web filter on the application server enables SSO using encrypted and digitally signed JSON token containing configurable identity information.
- HTTP Post Connectors: These connectors are used for applications that do support any method of SSO, and these connectors work as a credential vault to post stored credentials to authenticate the users automatically.

In addition to the above available connectors, it also includes an SDK to build to register custom connectors.

SSO Portal: A customizable portal is included with the solution, which provides a landing page for users to view the links to the SaaS applications they are authorized to use. This portal page can be embedded into an existing enterprise portal. The portal can be customized to for branding and adding other content specific to user context. For example, depending on the user type the look and feel of the portal page can be customized for specific user types.

Application Adapters: Application Adapters are used when using McAfee Cloud Identity Manager in a Service Provider mode, where internally hosted Java/.NET apps can be integrated for SSO using the token approach using a pre-built Web filter on the application server.

Cloud Authenticators: Cloud authenticators are similar to Identity Connectors, but are used when running in an SP mode. Multiple cloud authenticators can be mapped to the same application adapter – this provides the end user a choice to pick how they want to authenticate. This feature comes in handy in a multiple-IdPs using the SP scenario, when a user can be prompted to pick the IdP they want to authenticate with when accessing the application.

Administrative Console: The centralized admin console allows an administrator to configure the connectors, and set up federation with cloud applications. It also provides several operational features to ensure that McAfee Cloud Identity Manager is running smoothly. These include audit logging, out-of-the-box operational reporting, operational monitoring and alerting, and certificate management.

One Time Password

Protecting data in the cloud requires user authentication that goes beyond what you know (user ID and password) to what you have: a second factor that enables authoritative verification of the user's identity. Strong authentication with OTP is the single most cost-effective way to protect enterprise cloud applications, particularly when users outside the firewall access the application.

The McAfee Cloud Identity Manager One Time Password module leverages your existing enterprise identity repositories to deliver mobile two-factor strong authentication for enterprise and cloud applications, using devices your users already have: eliminating the expense and inconvenience of purchasing, distributing, and managing single-purpose hardware tokens.

The OTP Server delivers software tokens to desktops and smart phones (iPhone, Android, Blackberry, etc.) app, SMS to any mobile phone, as well as email, Skype, IM, and YubiKey.

Flexible Solution with Dynamic Authentication

An authentication device, such as a cell phone, can store unique profiles for multiple service providers. So users only need a single authentication device instead of multiple tokens for different cloud applications.

Security policy is dynamically enforced, based on attributes such as geo-location, IP address, LDAP group, etc. For example,

require an OTP when a user logs on from a hotel room via a VPN. The OTP software supports multiple authentication methods, including an additional PIN.

The solution is easy to implement and manage: most customers are up and running in a day or less. Fully automated key enrollment keeps management overhead low, which is perfect for organizations with high employee turnover or many external users.

OTP Capabilities

- Strong authentication for enterprise resources: OTP ensures only authenticated users have access
- Dynamic authentication: selects authentication methods based on user attributes
- Flexible software token: choice of authentication media replaces complex, expensive, single-purpose hardware tokens; one token can be used for multiple enterprise and cloud apps
- Low management overhead: easy to implement and manage, runs on existing IT infrastructure
- Standards-based: supports LDAP, SQL, RADIUS, Java, OATH, and most popular operating systems

McAfee Cloud Identity Manager Use Cases

Enterprise to SaaS Provisioning

This is the most typical use case that is aimed at automating the creation, updating, and deletion of user accounts on cloud hosted SaaS applications. Without a cloud provisioning solution, this is typically a point to point solution achieved via data feeds to services providers, or by administrators manually managing accounts within the application. This causes reduced visibility and security, increased user administration costs, and lost user productivity due to lack of timely access to applications. McAfee Cloud Identity Manager solves this problem by automatically provisioning and de-provisioning accounts based on security policies. As soon as a user is created, updated, or terminated in the trusted data source (like the HR system or Active Directory), it automatically picks up the change and applies the security policies to automatically create, update, or disable user accounts in the cloud applications.

Enterprise to SaaS SSO with Active Directory Authentication

This is the standard use case for Federation. Enterprise users can access the cloud hosted applications without having to know the passwords in the individual applications. Users can be authenticated using their Active Directory (AD) credentials, and authorized within the enterprise network and then federated into the SaaS application. Without a Federated SSO solution, users have to be provisioned into each application with native credentials, resulting in the user having to remember each of the user id/password combination. This increases the risk of password compromise, and increased help desk costs due to frequent forgotten passwords. This also increases the potential of unauthorized access by terminated users as they would still have access to the application from the internet even after their active directory account is disabled. Federated SSO requires the user to authenticate using their AD credentials for accessing the cloud applications, and this makes it really easy to turn off their access by disabling their AD account. The end result is that increased security, increased user productivity and reduced helpdesk costs.

Enterprise to SaaS Federation with Two-Factor Authentication using OTP

Moving applications and data into the cloud comes with additional security considerations, and for certain critical applications based on the user context it becomes necessary to implement strong authentication to ensure that the user is really who they say they are. This means in addition to a user id and password (something you know), and additional factor of authentication (something you have) is required. OTP delivered through an SMS or email or a Soft Token provides that second factor of authentication. In the event that the user's password was compromised, this ensures that that user is actually the intended user and not some fraudster who is trying to impersonate the user.

Typical use cases for using OTP with SaaS Federation include:

- Requiring OTP authentication for specific applications that contain critical/sensitive data
- Requiring OTP authentication for specific applications only when the user is coming from an external IP
- Requiring OTP authentication for specific applications only when the user is coming from a specific device type (e.g. mobile or an unknown device)

Enterprise to SaaS Federation for Authorized Users

Most applications are not available to every enterprise user. This decision should be made within the enterprise perimeter, rather than depending on the service provider to make this decision. This can only be achieved through Federated SSO, as it retains the authentication control within the enterprise (or by the Identity Provider). It allows for flexible authorization policies to be set so that when a user tries to federate to a SaaS application, the authorization policy specified for the application can be enforced prior to the user being federated to the end application. The authorization policies can be based on any of the following: user attributes and group memberships in AD, IP Address, device or browser type, time of day,

day of week, any item in the user agent string etc. Enforcing such authorization within the enterprise perimeter allows for centralized policy definition, administration and enforcement, allowing for consistent enforcement of policies across all applications.

Test Bed Blueprint

Solution Stack for Cloud Identity Management Reference Implementation

Here is a summary of the key solution stack components for the test bed as illustrated in Figure 3.

- Citrix XenServer*: Hypervisor containing the virtualized compute infrastructure in the enterprise data center
- Citrix XenCenter*: Virtualization management tool for the enterprise data center
- Microsoft Windows Server* 2008 R2: Operating system for enterprise infrastructure and Cloud Access 360 virtual machines (VMs)
- Microsoft Windows 7: Operating system for the virtual clients in the enterprise data center
- McAfee Cloud Identity Manager (SSO): Provides seamless single-sign-on for enterprise users to cloud applications
- Nordic Edge One Time Password Server (OTP): Provides two-factor strong authentication for enterprise users to cloud applications
- Salesforce.com SaaS application in the public cloud

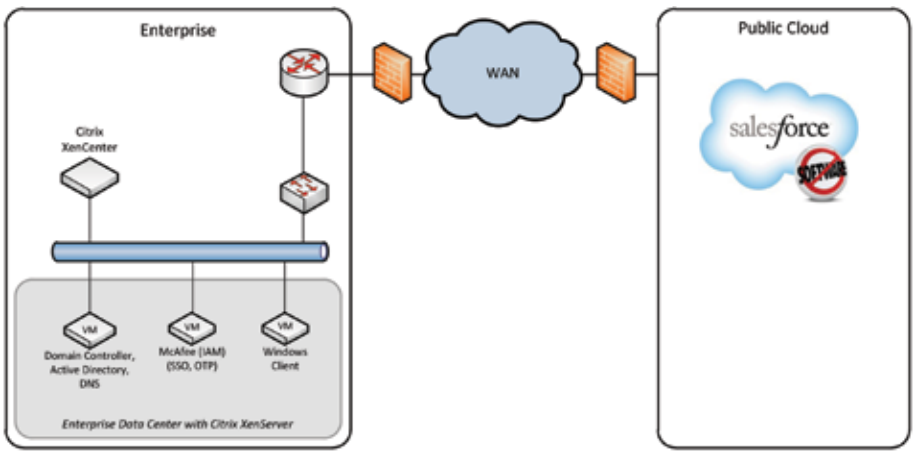


Figure 3: Cloud Identity Management Reference Architecture

Software Description

The data center was configured using a Citrix XenServer 5.6[2] Hypervisor and the Microsoft Windows Server 2008 R2 operating system.[1]

In the data center, a typical Intel® Cloud Access 360 installation was created utilizing 3 VMs:

- Microsoft Windows 7 Virtual Client (simulate user access to the Intel Cloud Access 360 Web portal)
- Domain controller (Active Directory, DNS)
- McAfee Cloud Identity Manager SSO and OTP (Microsoft Server 2008 R2)

In addition, a second physical server setup configured with Microsoft Windows 2008 R2 and Citrix XenCenter for VM management.

Table 1 shows all of the VMs used as the starting point for the use case.

Virtual Machine	Purpose
FMSCD01	Domain Controller (Active Directory, DNS)
FMSECA360	McAfee Cloud Identity Manager (SSO, OTP, Web Portal)
Win7-PC	Simulate client user

Table 1: Virtual Machine Configuration for Data Center

System Design

We used the virtual network interface in XenCenter to assign a static IP address to each VM.

Figure 4 shows the network IP configuration for the McAfee Cloud Identity Manager test bed that includes both physical and virtual servers.

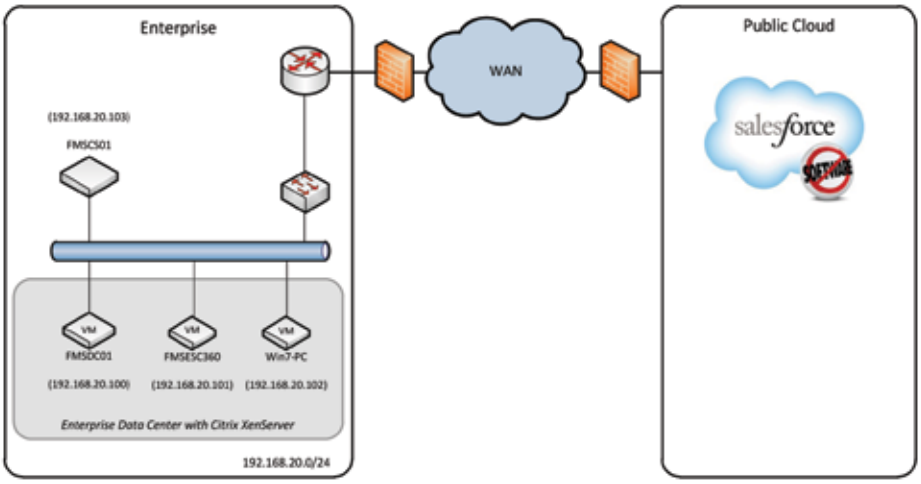


Figure 4: Network IP Configuration

Table 2 shows the network IP configuration for the cloud Identity and Access Management exercise.

Physical Hostname	Virtual Machine	Network
Xen-ECA360	FMSDC01	192.168.20.100
Xen-ECA360	FMSECA360	192.168.20.101
Xen-ECA360	Win7-PC	192.168.20.102
FMSCS01		193.168.20.103

Table 2: Network IP Configuration for Data Center

Hardware Description

We used the Intel® Xeon® processor 5600 series which automatically regulates power consumption and intelligently adjusts server performance according to application demand, maximizing both energy cost savings and performance

The Intel Xeon processor 5600 series offers several features that help it make the best performing server in the industry.

Some of these features include:

- **Intelligent Performance** boosts performance by up to 15 times over single-core servers with processors that intelligently adapt to your workload
- **Intel® Turbo Boost Technology** dynamically and automatically maximizes server application performance by increasing core frequencies, enabling faster speeds for specific threads, and mega tasking workloads.
- **Intel® Quickpath Technology** brings scalable shared memory architecture with high-speed, point-to-point processor interconnects, plus larger caches and larger memory for two-processor servers
- **Large memory capacity** of up to 18 DIMM slots with up to 288 GB of main memory for higher performance for your data-intensive applications

The hardware configuration consisted of two servers in the private cloud environment.

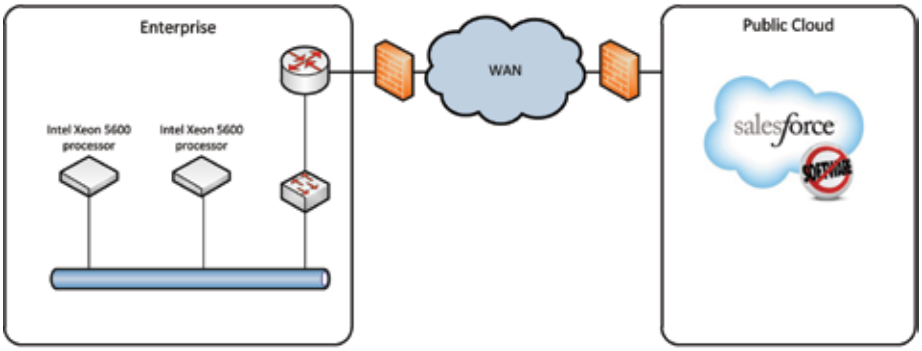


Figure 5

Table 3 contains the hardware configuration and details for the test bed.

System	Location	Other Info
FMSCS01	Data center	Processor: Two Intel Xeon processors X5670, 2.93 GHz Memory: 48 GB RAM Storage: Two 500 GB SATA HDD's, RAID 1 Network: Two GB Ethernet NICs, Two 10 GB Ethernet NICs
Xen-ECA360	FMSECA360	Processor: Two Intel Xeon processors X5680, 3.33 GHz Memory: 24 GB RAM Storage: Two 500 GB SATA HDD's, RAID 1 Network: Two GB Ethernet NICs, Two 10 GB Ethernet NICs
Network	LAN	100 MB

Table 3: Hardware Configuration

Network Requirements

The server running the McAfee Cloud Identity Manager requires two ports to be available – one for the Web server and the other is the JMX port. Both these ports are configurable, by default these ports are 8443 and 9999. The server and network firewall should allow port 8443 accept incoming connections. In addition, the server should have access to the Active Directory domain controller for user authentication.

For provisioning services, McAfee Cloud Identity Manager makes a direct API call to the Web services hosted by the cloud providers, and so the required proxies and firewalls should be configured to allow outbound traffic from the server to the internet.

For Federated SSO, the client machines (user's desktop, etc.) should have the ability to connect to port 8443 on the server via a Web browser, and also be able to connect to the cloud applications' Web servers. All communication in this scenario between server and the Cloud Application happens via HTTP redirects and posts via the user's browser.

Technical Review

This section provides a detailed overview of the actions performed to implement identity and access management solution for SaaS applications. Many of the steps and commands are unique to this particular design, but they should provide enough detail to understand how the test bed was setup.

For the details about application installation and setup, please see the respective product documentation. Be sure to check product release notes, service bulletins, and knowledge base articles.

Installation Overview

This section discusses the installation process for software prior to testing. The following setup steps assume you have an understanding of how to install and configure Microsoft Windows Server 2008 R2, Citrix XenServer, and Citrix XenCenter.

Private Cloud Installation

- Install Microsoft Windows Server 2008 R2 on host FMSCS01. (Physical host 1)
  - *Host name: FMSCS01
  - *Configure Static IP address
  - *Activate Windows
  - *Install Citrix XenCenter
- Install Citrix XenServer 5.6 hypervisor on host xen-eca360. (Physical host 2)
- Using Citrix XenCenter, create the following VMs:
  - *VM Name: W2K8 R2 (DC)

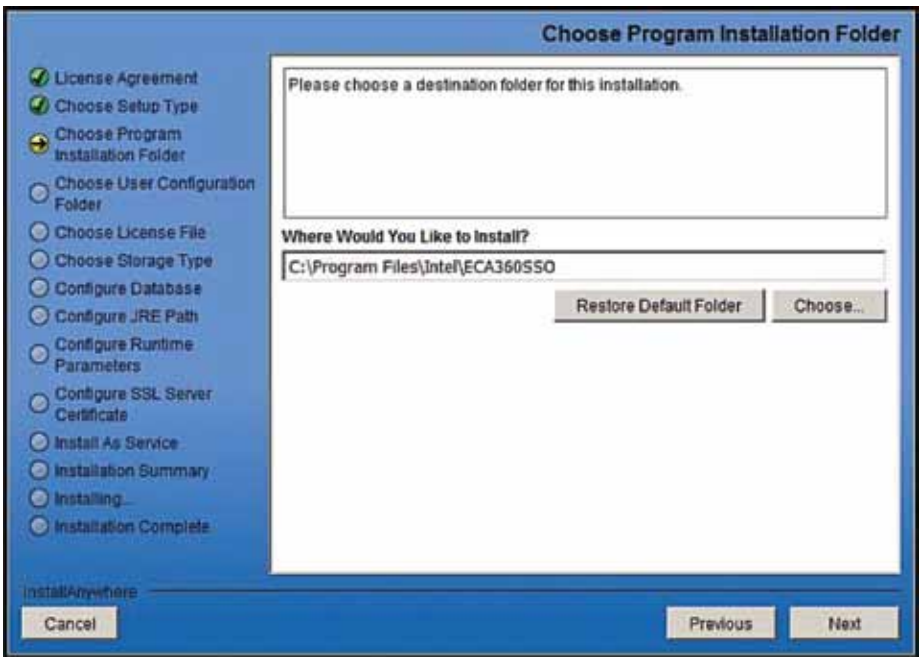
    OS: Windows Server 2008 R2 – 64 bit (for Domain Controller - Active Directory, DNS)
    - ° Host name: FMSDC01
    - ° Apply static IP address
    - ° Activate Windows
    - ° Install Active Directory Domain Services in accordance with your domain preferences
    - ° Enable and install DNS role:
      - Configure Forward Lookup zones
      - Configure Reverse Lookup zones
      - Ensure that nslookup resolves in both domains
  - *VM Name: W2K8 R2 (ECA360)

    OS: Windows Server 2008 R2 64 bit (for Intel Cloud Access 360 SSO and OTP components)
    - ° Hostname: FMSECA360
    - ° Apply static IP address
    - ° Install Intel Cloud Access 360 SSO application
    - ° Install Nordic Edge One Time Password application
  - *VM Name: Windows 7 -64 bit (Client)

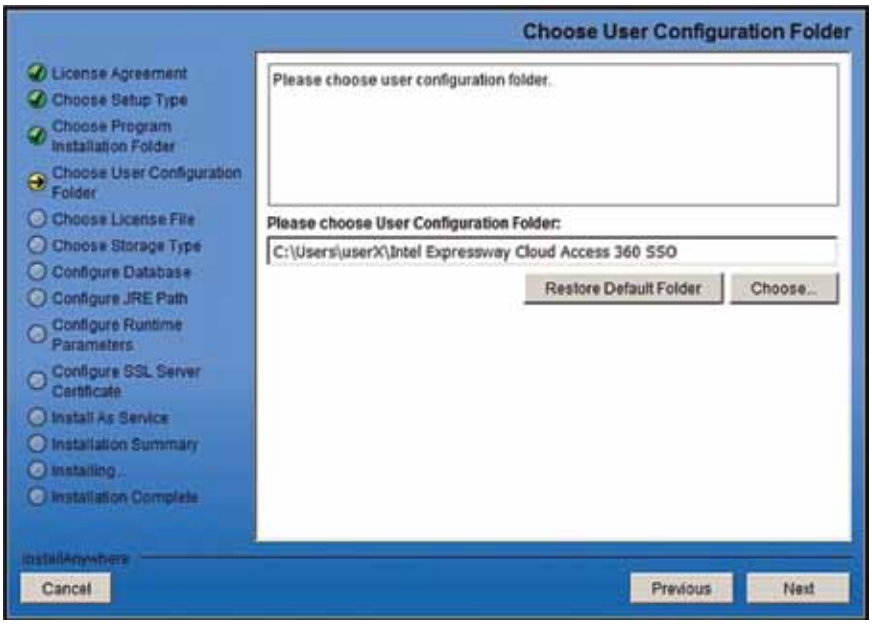
    OS: Windows 7 -64 bit (Virtual client to access web portal)
    - ° Hostname: Win7-PC
    - ° Apply static IP address
- In Active Directory, create a new user: a typical user with First name "Adam", last name "user" and login ID as "auser@eca360.com".
- Place all VMs and the physical host FMSCS01 into the eca360.com domain.

Installing McAfee Cloud Identity Manager on Windows – Custom Install Option

- Download one of the following installation packages to a download directory:
  - **Intel Package**
  - **64-bit Windows**: eca360_win64_2.0.0.zip
- Extract the zipped files from the installation package to the download directory.
- Start the installer. Run "eca360_sso_win64_2.0.0.exe".
- The installation wizard opens on the **License Agreement** step.



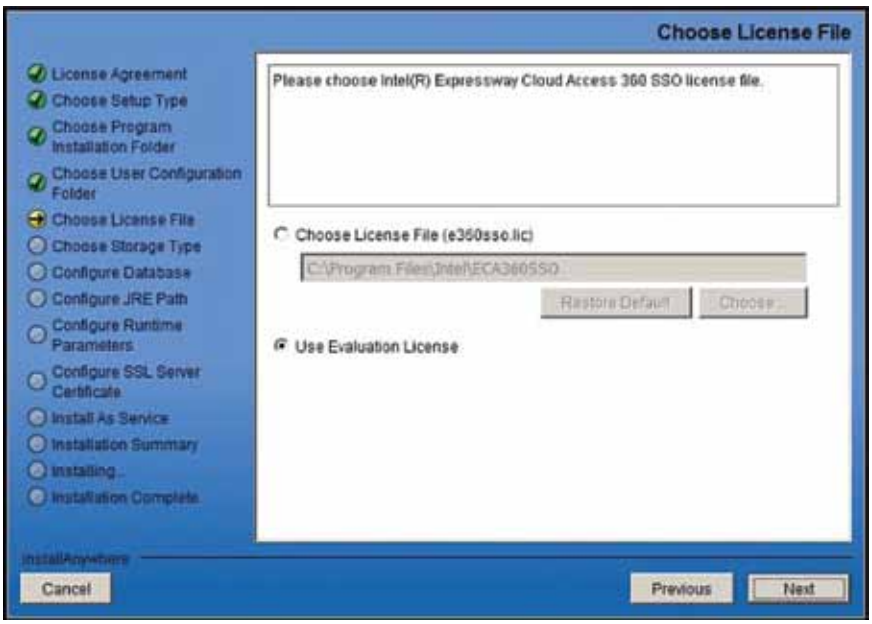
- Choose Program Installation Folder:
  - *Click **Choose**... to locate and select the installation directory on your computer.
  - *Select c:\Program files\intel\ECA360SSO.
  - *Click **Next**.



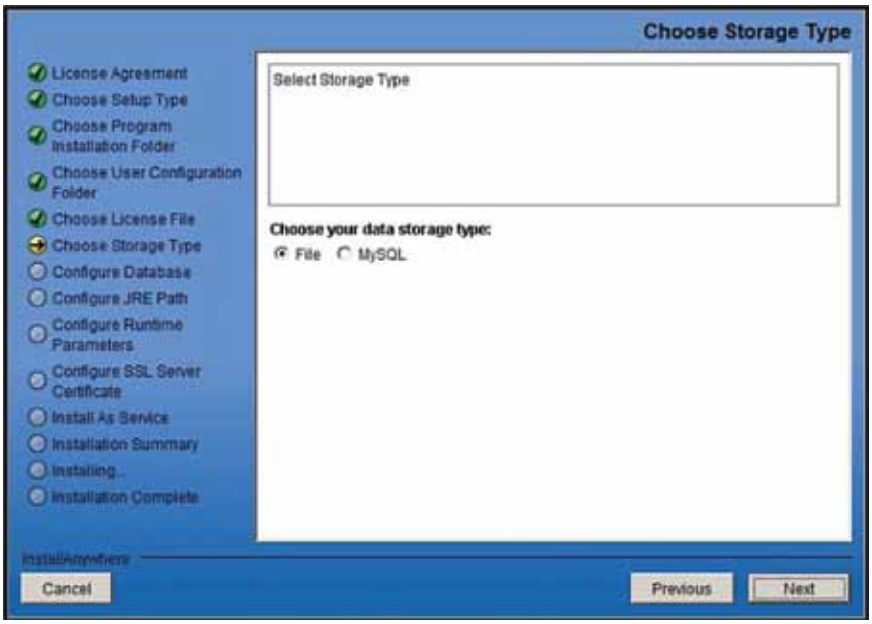
- Choose User Configuration Folder:
  - *Click **choose**... to locate and select the user configuration directory on your computer.
  - *Optionally, click **Restore Default** to restore the default user configuration location provided by the installer.

    Note: The user directory is where all user-specific configurations are installed.

    Default: %USERPROFILE%\Intel Expressway Cloud Access 360 SSO.
  - *Click Next.

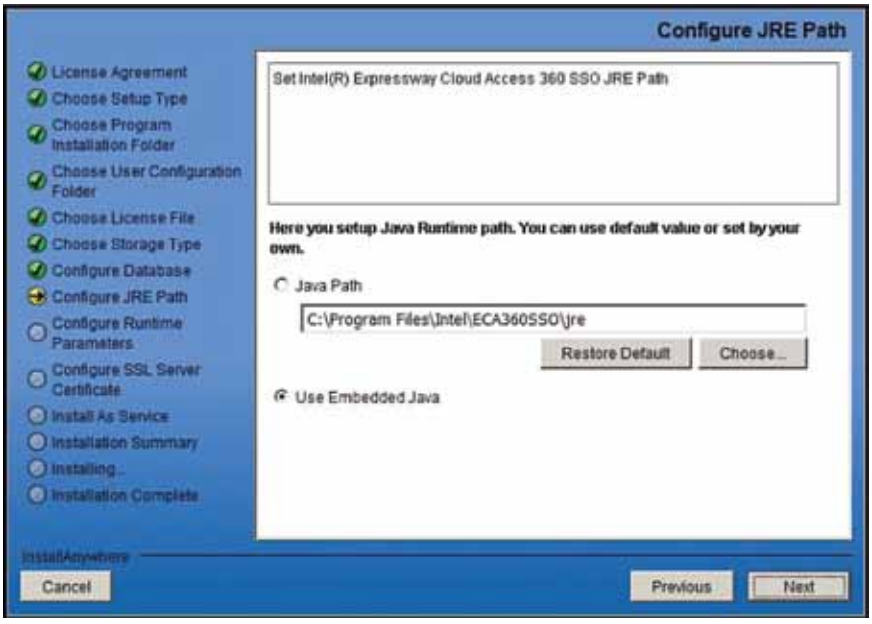


- Choose License File:
  - *Select "Use Evaluation License" to specify a 30-day evaluation license.



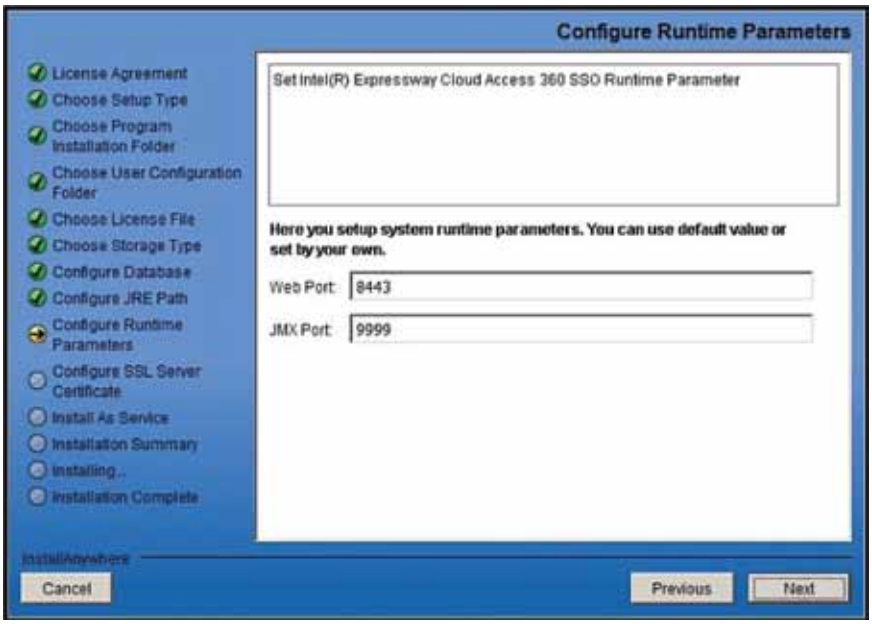
- Choose Storage Type:

  *Select the File option, and click **Next**.

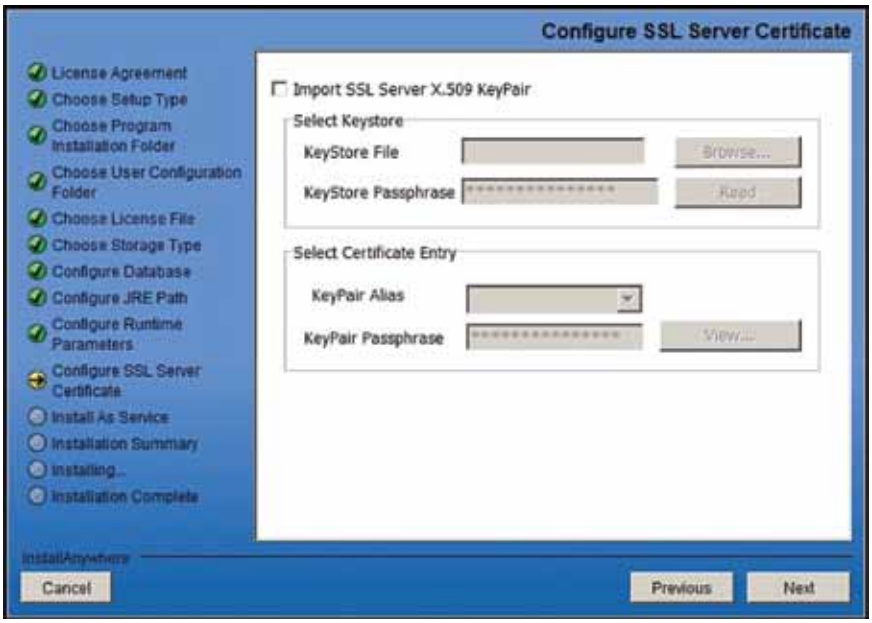


- Configure JRE Path:

  *Select Use **Embedded Jav**a option and click **Next**.

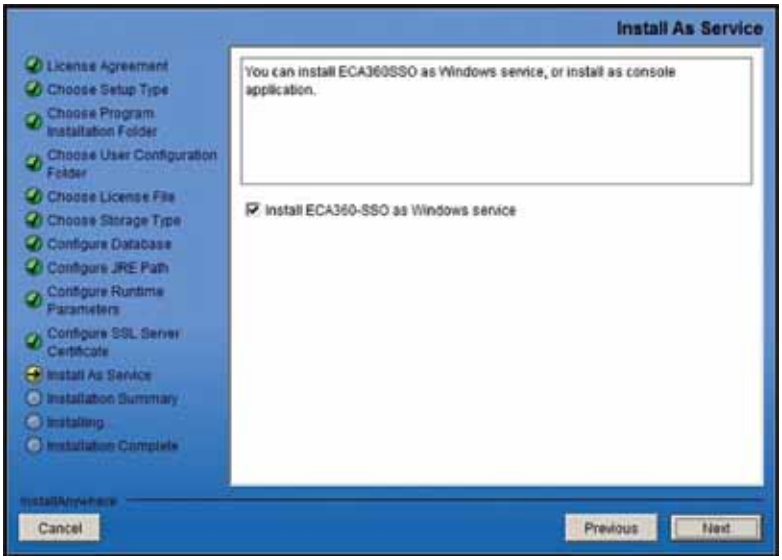


- Configure Runtime Parameters:
  - *Accept the default values and click **Next**.
  - ***Web Port**: Specifies the port number of the McAfee Cloud Identity Manager HTTP server
  - ***Default**: 8443
  - ***JMX Port**: Specifies the Java management port number
  - ***Default**: 9999



- To import an SSL server X.509 certificate key pair:
  - *Select the Import **SSL Server X.509 KeyPair** check box.
  - *Click **Browse**... to locate the **KeyStore File** on your computer.
  - *Type the password assigned to the keyStore in the **KeyStore Passphrase** field and click **Read**. The KeyStore file is read, and all key pair entries in the file are listed on the KeyPair Alias drop-down menu.
  - *Select the alias from the **KeyPair Alias** drop-down menu corresponding to the X.509 certificate that you want to import. The alias is the name assigned to the key pair when it was created. In the Management Console, the alias is used to reference the key pair.
  - *Type the password assigned to the selected key pair in the **KeyPair Passphrase** field and click **View**.

- Click OK.
- The SSL Certificate Information pane closes.
- Click Next.



- Select the **Install ECA360-SSO as Windows service** check box.

  ***Note**: We recommend that you install Intel® ECA360-SSO as a Windows service, because Windows restarts the service when it fails, minimizing down time.

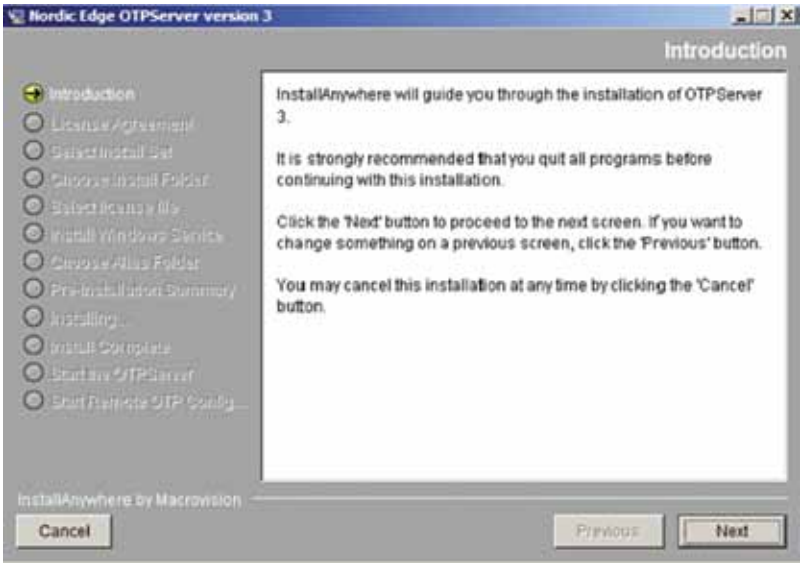
- Click **Next**. The Installation Summary step opens and displays the custom installation configuration.
- Review the installation summary, and click **Install**.
- Click **Done** when the installation is complete.

Installing One Time Password Server Version 3

We will use Windows as an operating system to show how the installation process is done on this platform.

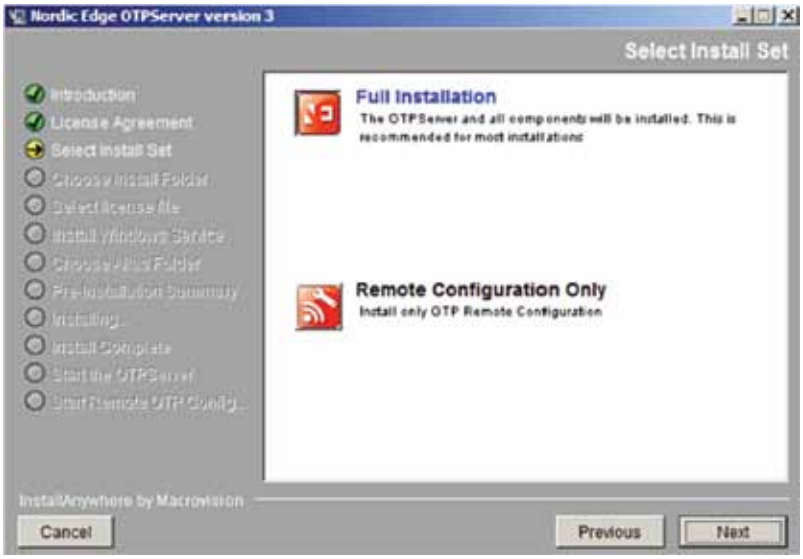
The install utility and process is pretty much the same on other operating system platforms. There are two version of the install program for each operating system platform, one with a bundle version of java and one without. In this example we will use the bundle version which is the recommended version.

Start the installation program, in this case the file otp3install.exe, and follow the instructions.

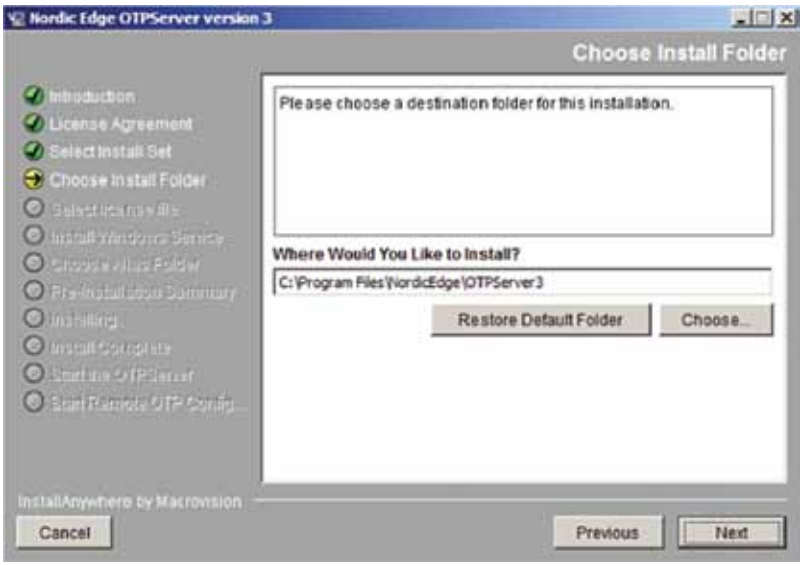


- Click on **Next** to continue.

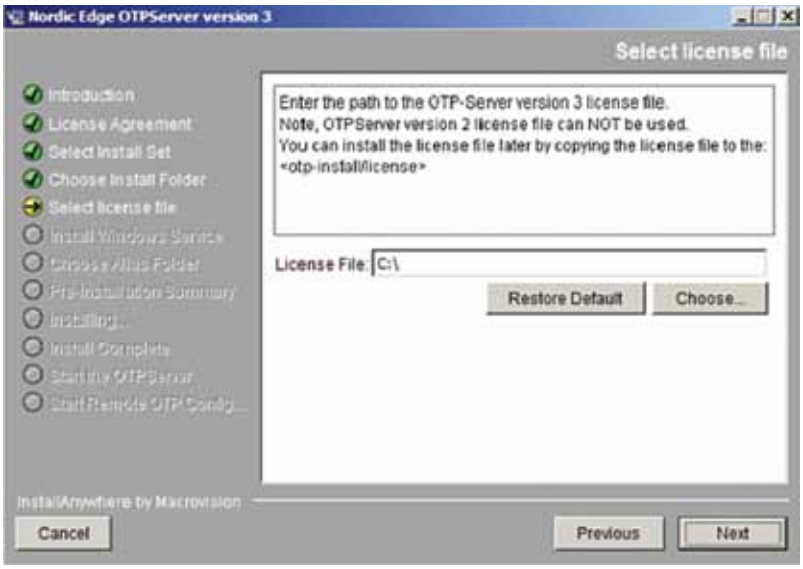
- Select "I accept the terms" and click on **Next**.



- Select the required Install Set. Choose **Full Installation**.



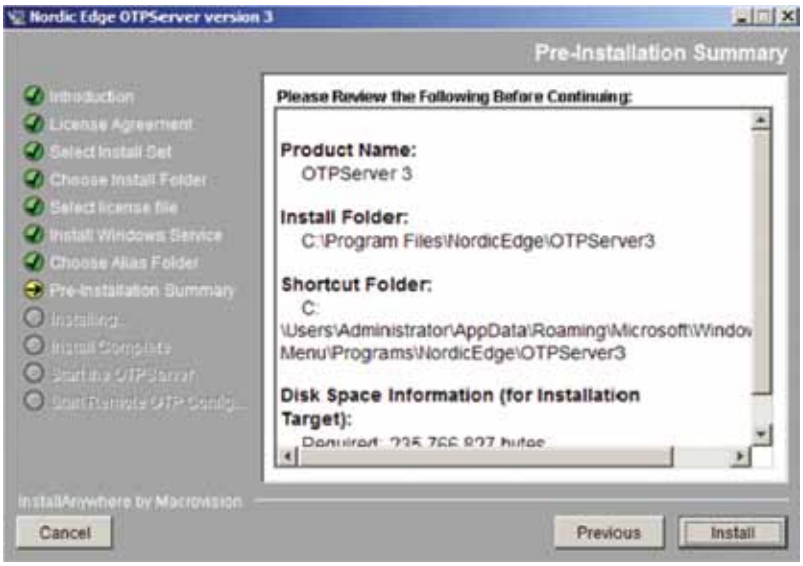
- Select where to install the OTP Server and click on **Next**.



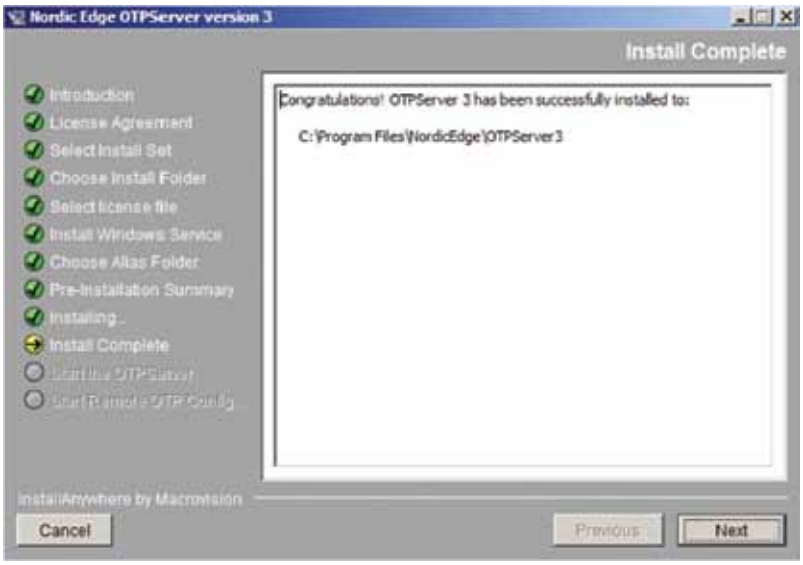
- Choose the license.dat that you have received via e-mail or other media from Nordic Edge and click on **Next**.

- Click the checkbox to install the OTP Server process a Windows Service. Click **Next**.

- Select where to place the product icons and shortcuts. Click **Next**.



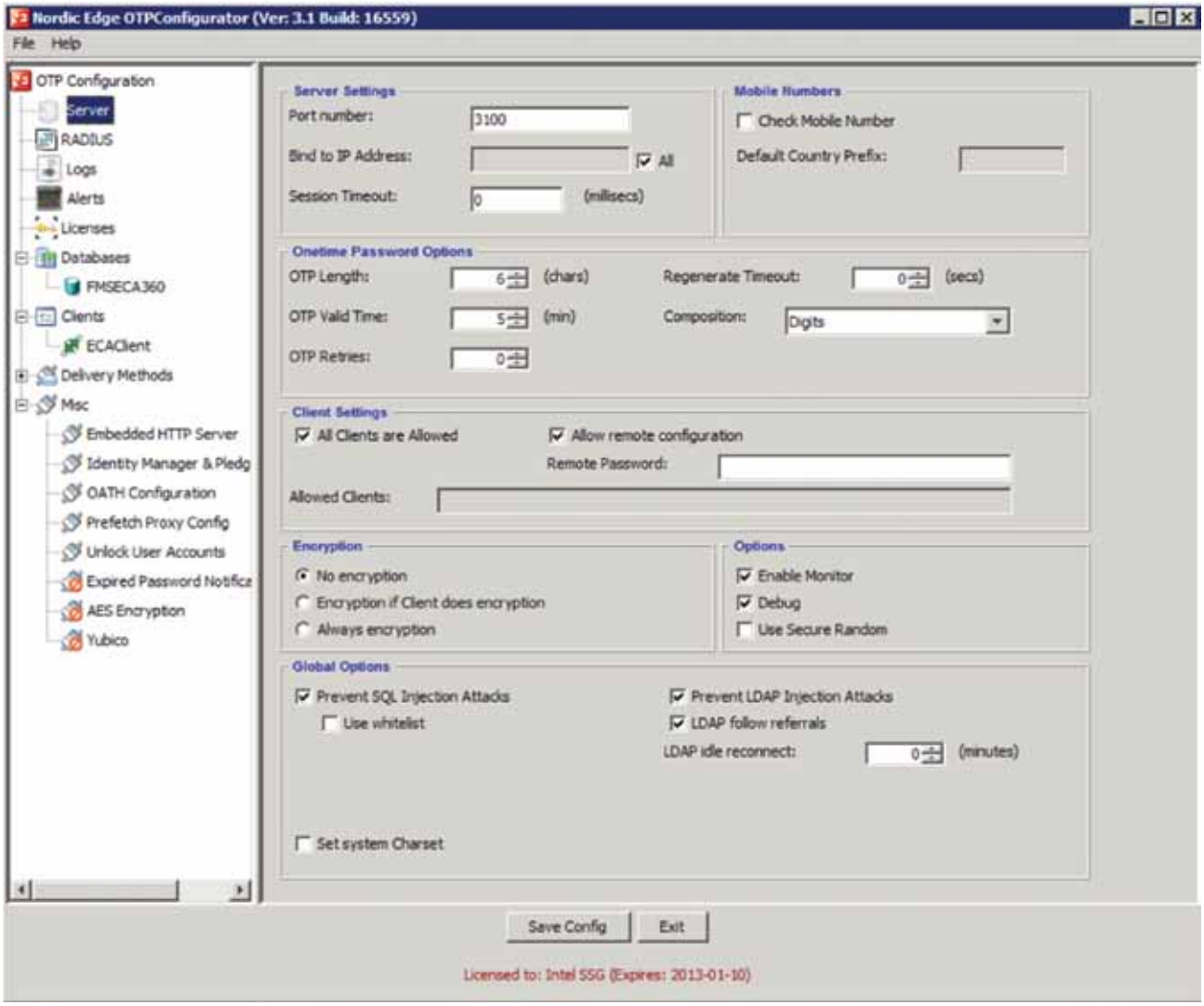
- Review the Pre-Installation Summary. Click on **Install** to continue the process.

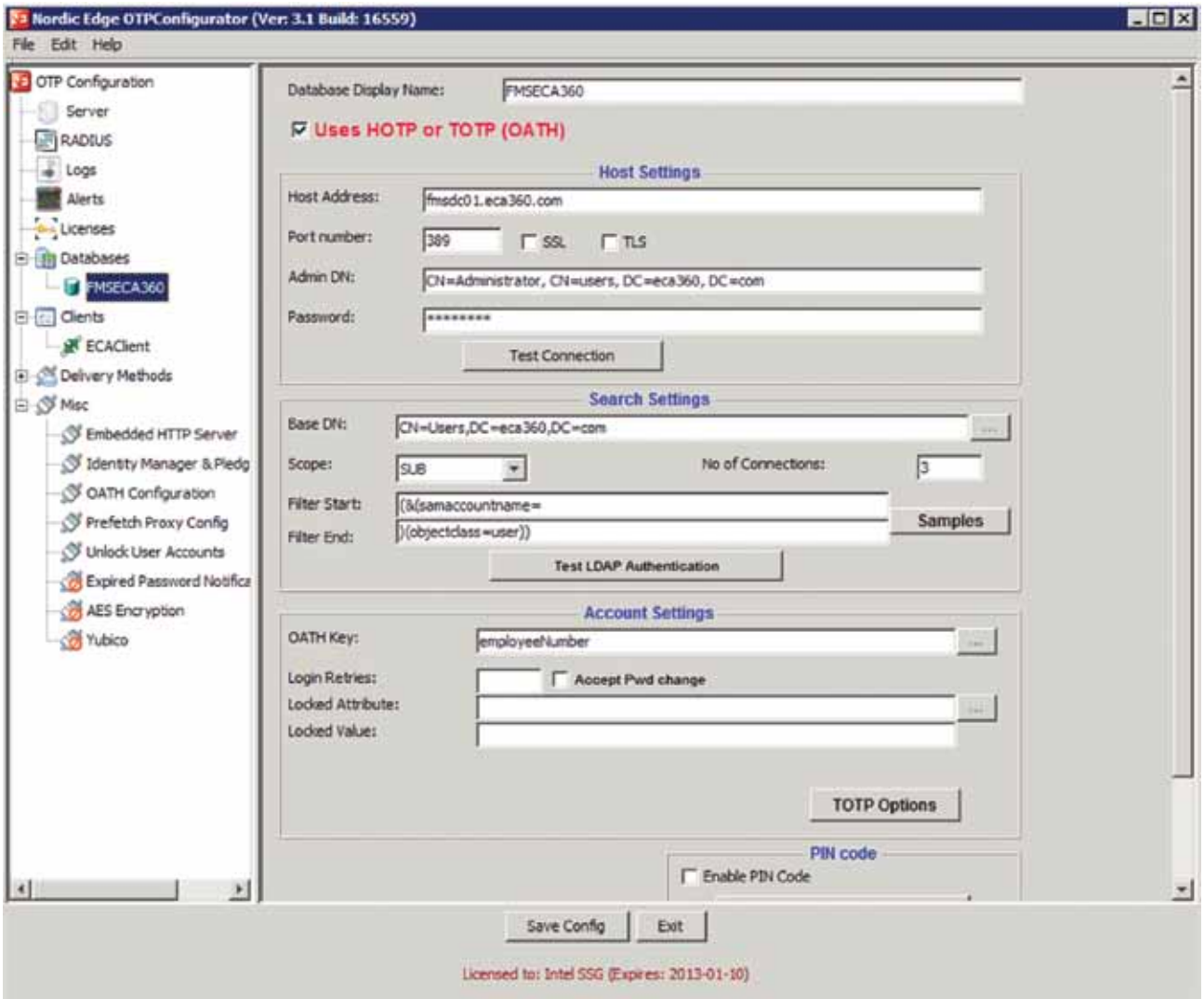


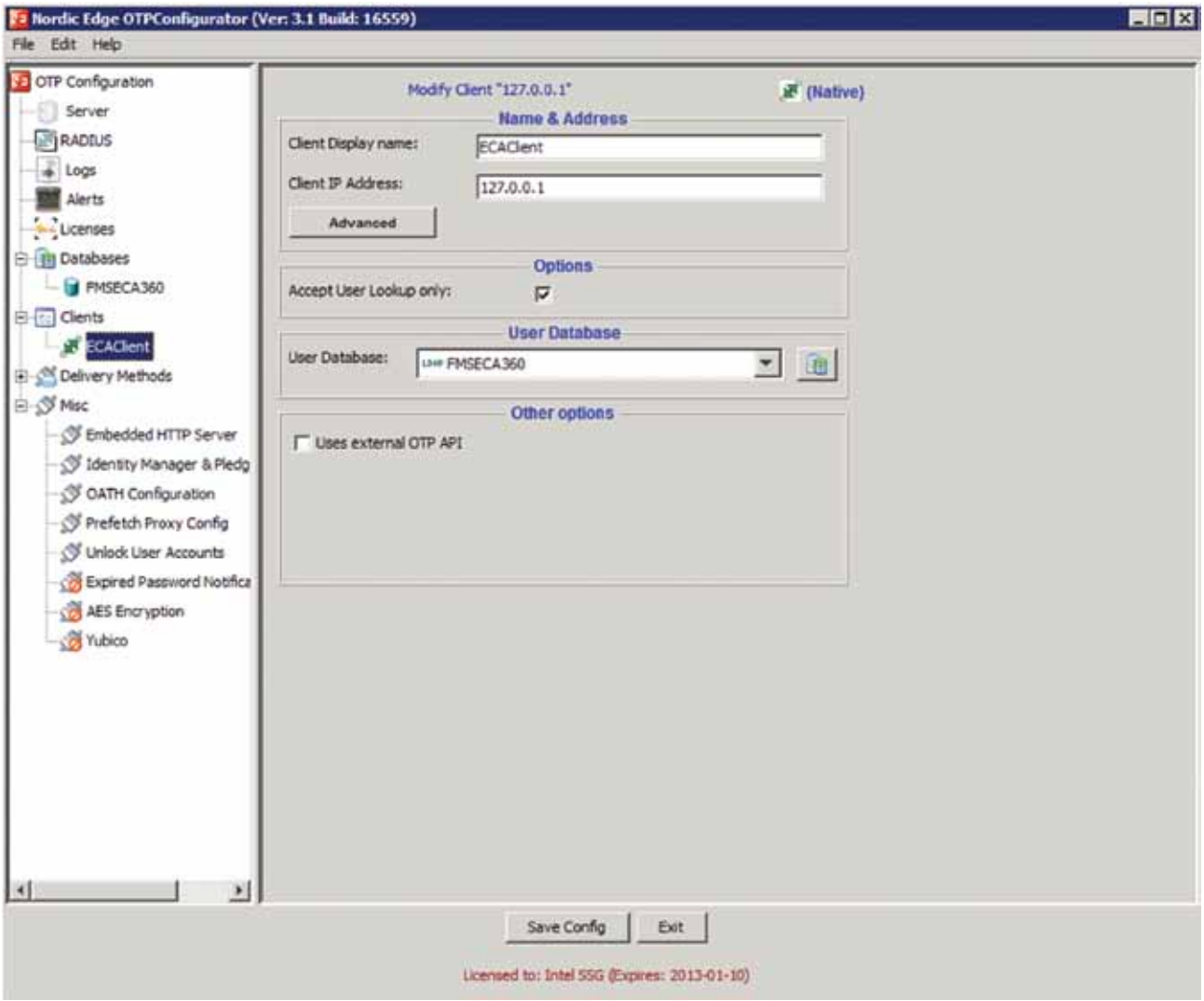
- The picture above shows that the installation is successful and that the installation process finished. Click **Next**.

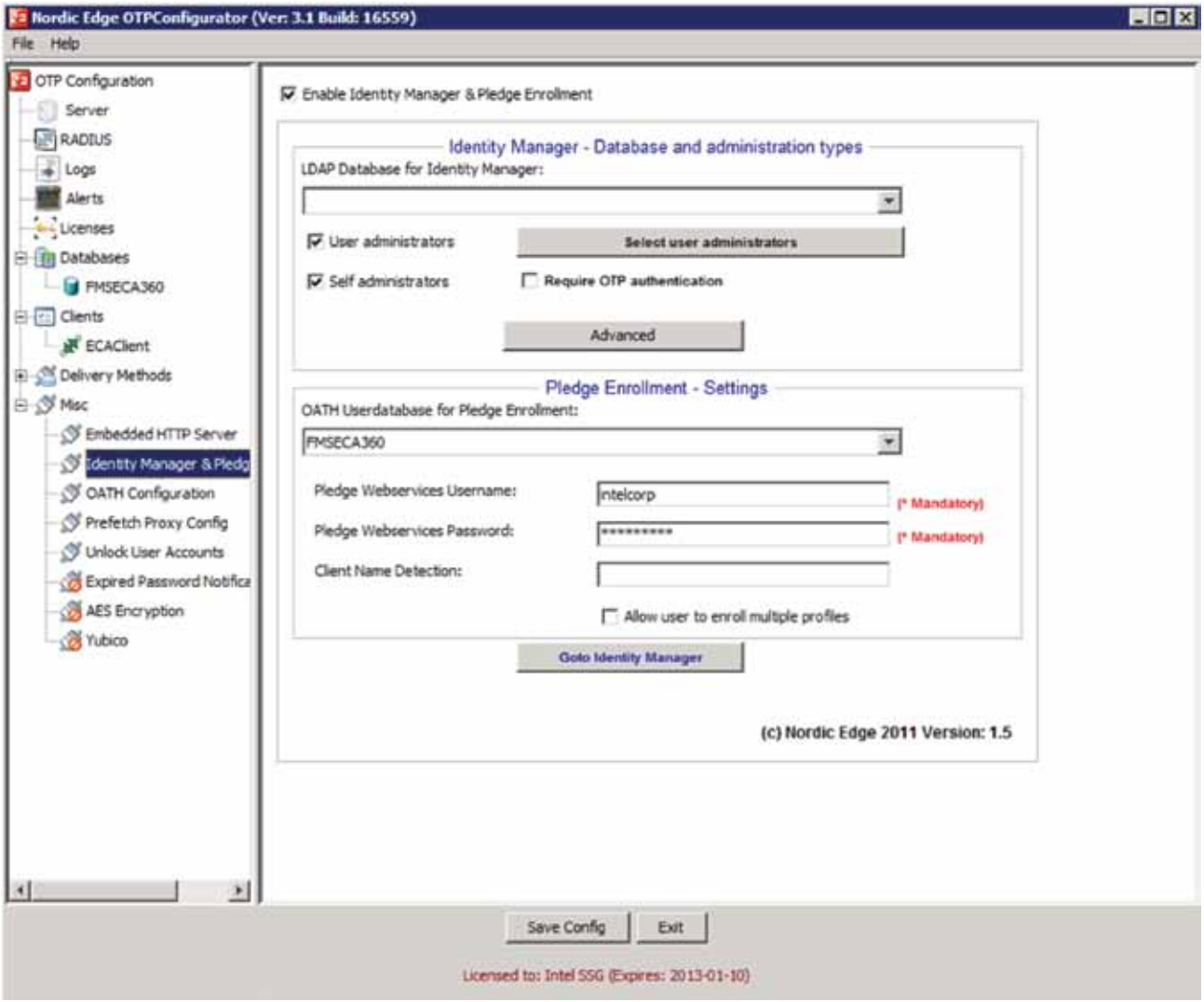
- Select **Yes** to start the OTP server process as the last action before starting to configure the OTP Sever.
- Click **Done** to end the installation process.

One Time Password Configuration Settings

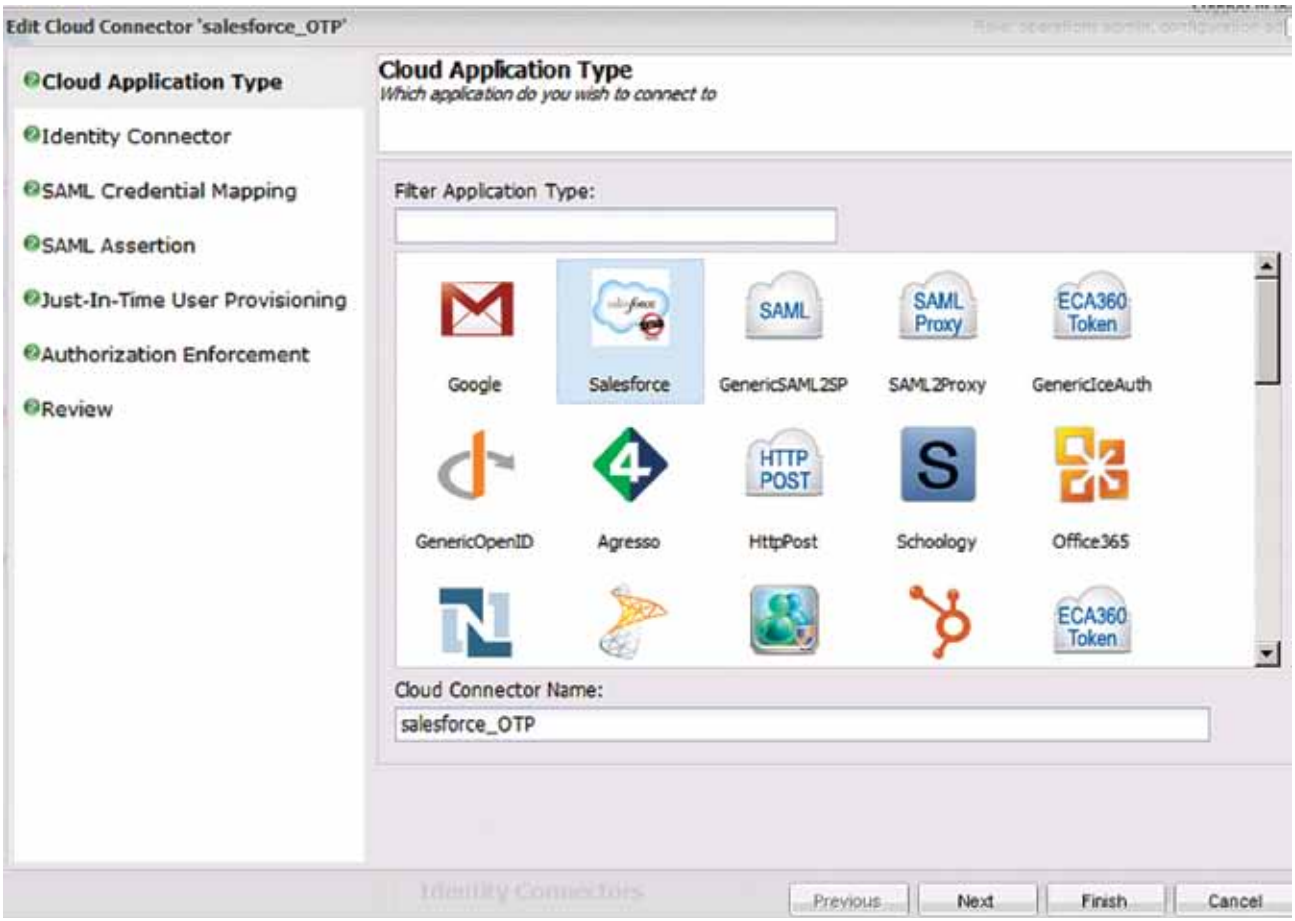



Nordic Edge OTPConfigurator (Ver: 3.1 Build: 16559)
File Edit Help
OTP Configuration
Server
RADIUS
Logs
Alerts
Licenses
Databases
FMSECA360
Clients
ECAClient
Delivery Methods
Misc
Embedded HTTP Server
Identity Manager & Pledg
OATH Configuration
Prefetch Proxy Config
Unlock User Accounts
Expired Password Notifica
AES Encryption
Yubico
Database Display Name:
FMSECA360
Uses HOTP or TOTP (OATH)
Host Settings
Host Address:
fmsdc01.eca360.com
Port number:
389
SSL
TLS
Admin DN:
CN=Administrator, CN=users, DC=eca360, DC=com
Password:
Test Connection
Search Settings
Base DN:
CN=Users,DC=eca360,DC=com
Scope:
SUB
No of Connections:
3
Filter Start:
(&(samaccountname=
Filter End:
)(objectclass=user))
Samples
Test LDAP Authentication
Account Settings
OATH Key:
employeeNumber
Login Retries:
Accept Pwd change
Locked Attribute:
Locked Value:
TOTP Options
PIN code
Enable PIN Code
Save Config
Exit
Licensed to: Intel SSG (Expires: 2013-01-10)

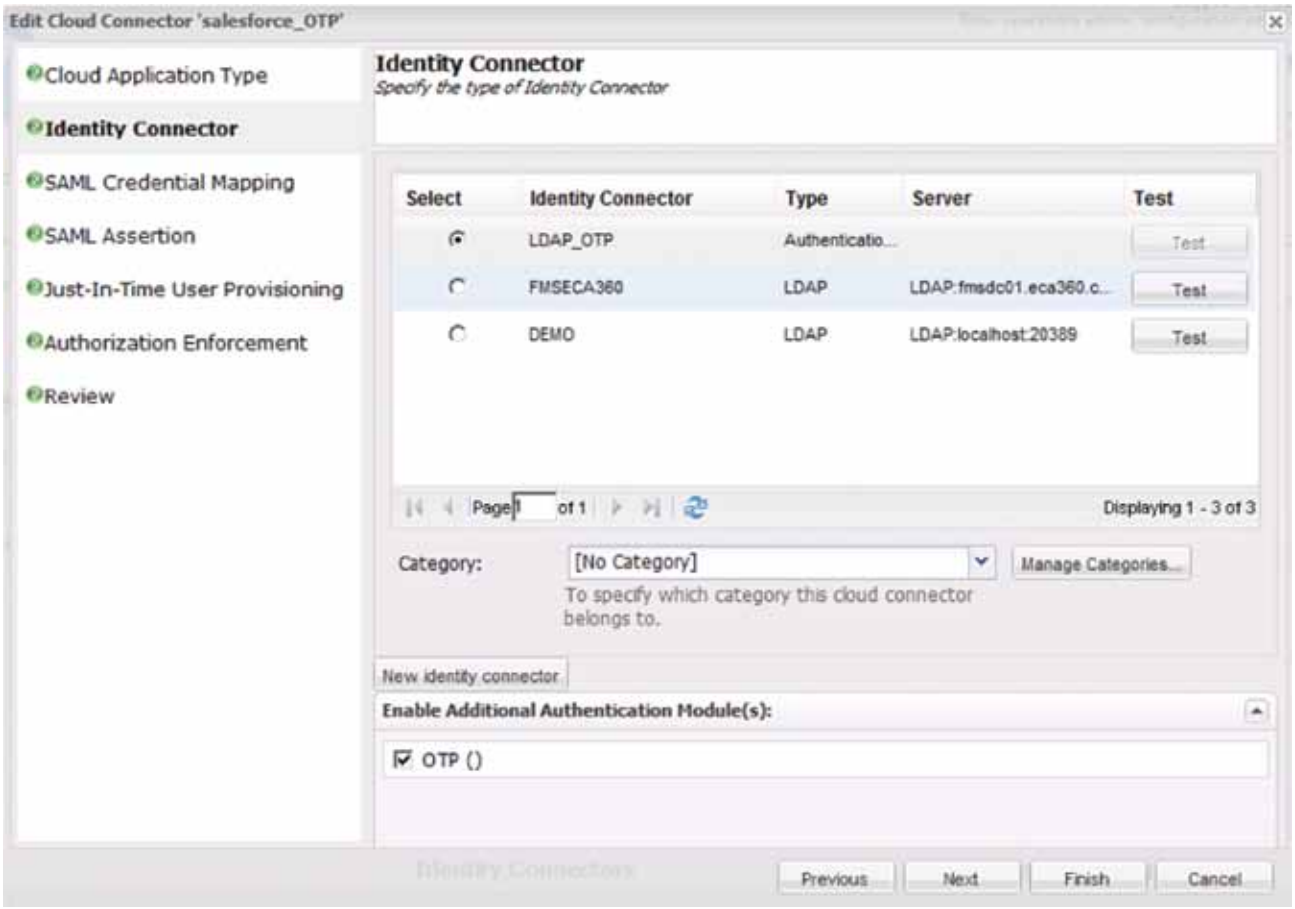

Nordic Edge OTPConfigurator (Ver: 3.1 Build: 16559)
File Edit Help
OTP Configuration
Server
RADIUS
Logs
Alerts
Licenses
Databases
FMSECA360
Clients
ECAClient
Delivery Methods
Misc
Embedded HTTP Server
Identity Manager & Pledg
OATH Configuration
Prefetch Proxy Config
Unlock User Accounts
Expired Password Notifica
AES Encryption
Yubico
Modify Client "127.0.0.1"
(Native)
Name & Address
Client Display name:
ECAClient
Client IP Address:
127.0.0.1
Advanced
Options
Accept User Lookup only:
User Database
User Database:
FMSECA360
Other options
Uses external OTP API
Save Config
Exit
Licensed to: Intel SSG (Expires: 2013-01-10)


Nordic Edge OTPConfigurator (Ver: 3.1 Build: 16559)
File
Help
OTP Configuration
Server
RADIUS
Logs
Alerts
Licenses
Databases
FMSECA360
Clients
ECAClient
Delivery Methods
Misc
Embedded HTTP Server
Identity Manager & Pledg
OATH Configuration
Prefetch Proxy Config
Unlock User Accounts
Expired Password Notifica
AES Encryption
Yubico
Enable Identity Manager & Pledge Enrollment
Identity Manager - Database and administration types
LDAP Database for Identity Manager:
User administrators
Select user administrators
Self administrators
Require OTP authentication
Advanced
Pledge Enrollment - Settings
OATH Userdatabase for Pledge Enrollment:
FMSECA360
Pledge Webservices Username:
intelcorp
(* Mandatory)
Pledge Webservices Password:
(* Mandatory)
Client Name Detection:
Allow user to enroll multiple profiles
Goto Identity Manager
(c) Nordic Edge 2011 Version: 1.5
Save Config
Exit
Licensed to: Intel SSG (Expires: 2013-01-10)

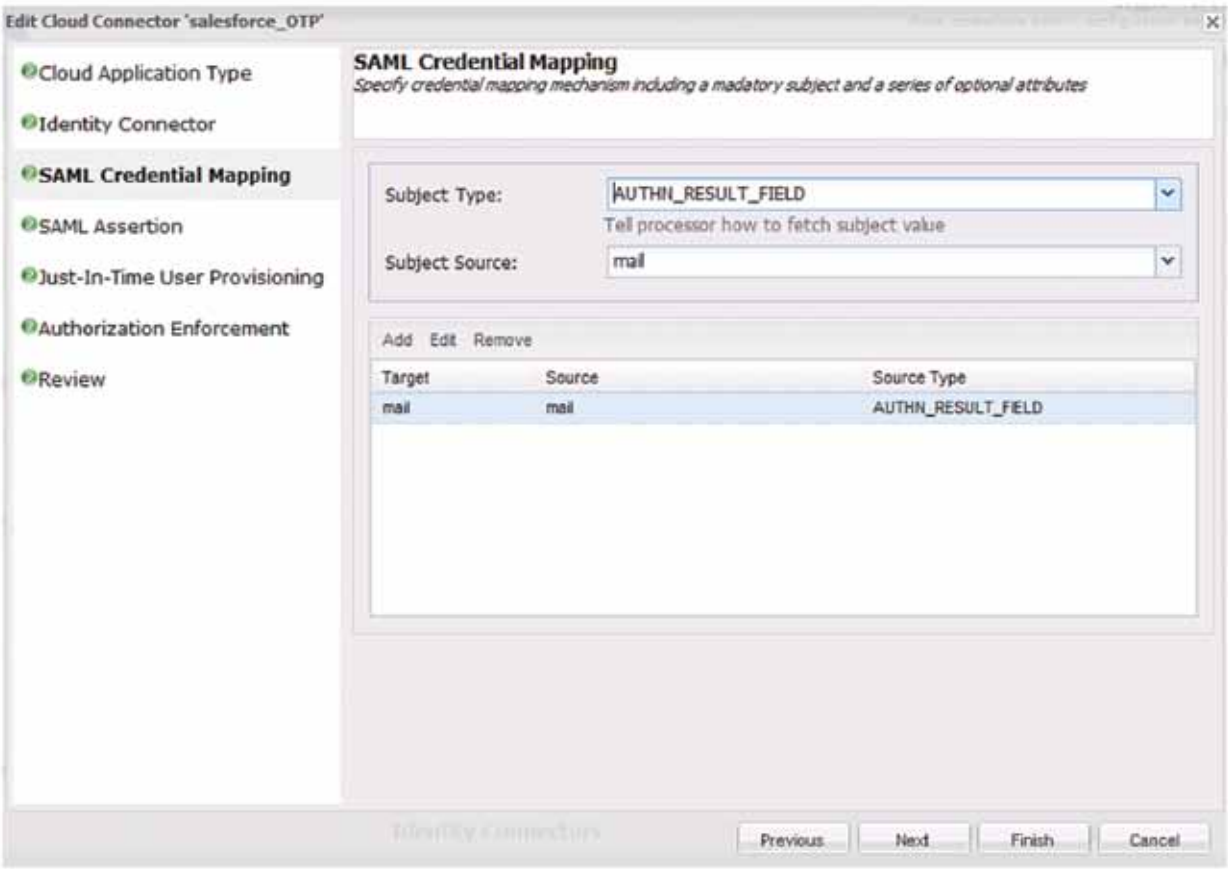
Salesforce.com Cloud Connector Configuration



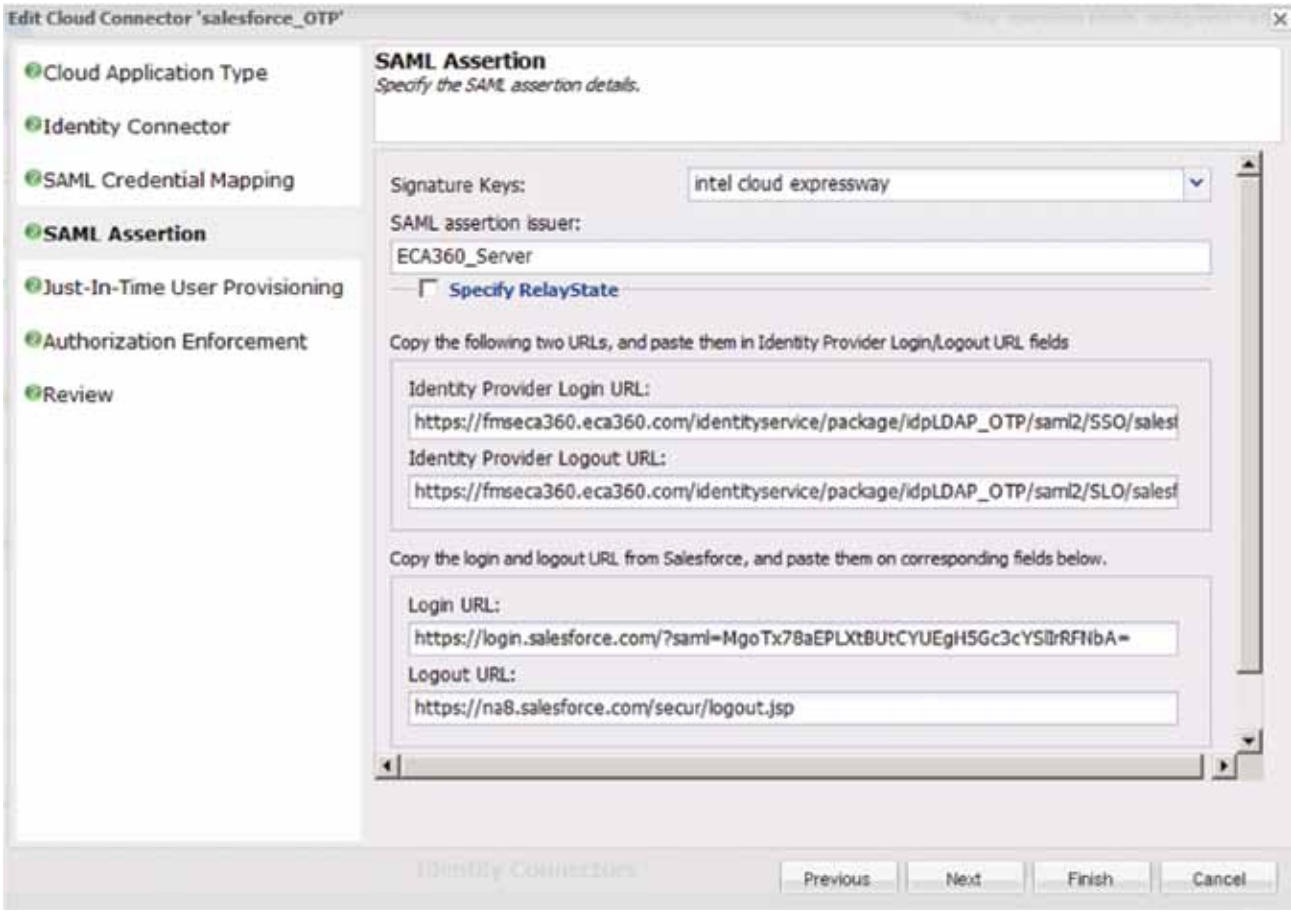
Configuration settings for Identity Connector:



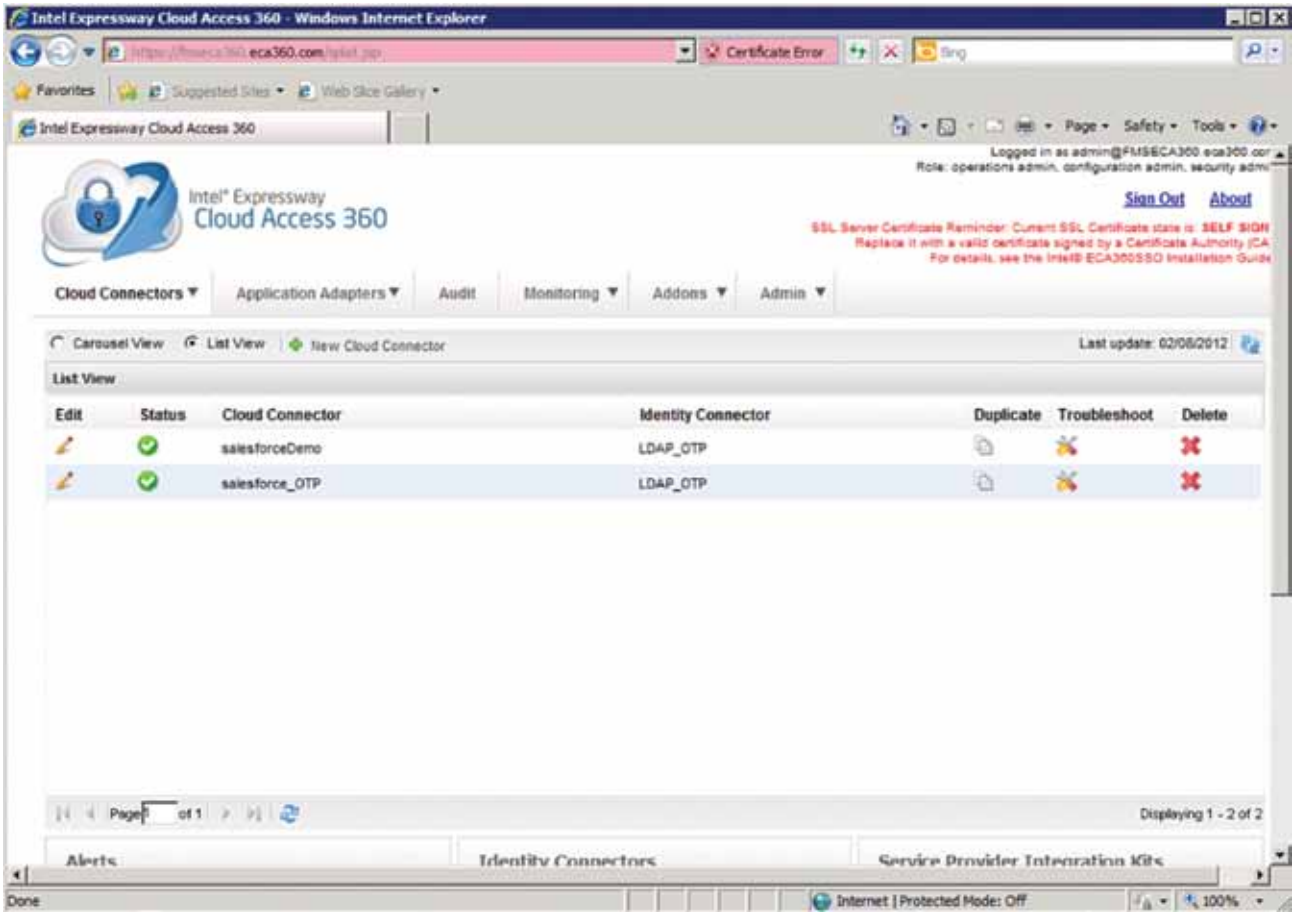
Configuration settings for SAML Credential Mapping:



Configuration settings for SAML Assertion:



Cloud Connectors Configuration Portal:



Things to Consider

The scalability of the cloud solution could be impacted by:

- Network technology (e.g. 10GigE) and architecture
- Selected storage architecture
- Choice of server hardware for the software version of Intel Cloud Access 360
- The ability to create templates of workflows and policies so that you can author an application once but use it for many services and operations
- Enabling and disabling access to services depending on the user scenario
- How many nodes you need in an Intel Cloud Access 360 cluster—you can have up to 24. A cluster is used for load balancing and failover. The more nodes you have, the greater the message throughput and system stability
- The level of security you need. You can explicitly guard against DoS, XML threats, and various content attacks. However, increasing security eventually decreases message throughput due to heavy security processing.

For More Information

- McAfee Cloud Security: http://www.mcafee.com/cloudsecurity
- Intel Application Security and Cloud Identity: http://www.intel.com/gp/identity
- Intel Cloud Builders: www.intel.com/cloudbuilders

Endnotes

1. Microsoft Technet "Windows Server 2008 and Windows Server 2008 R2," http://technet.microsoft.com/en-us/library/dd349801(WS.10).aspx
2. Citrix XenServer 5.6, http://support.citrix.com/product/xens/v5.6/

Disclaimers