NICE XBAP Update

Table of contents

[1 Introduction 1](#_Toc13228266)

[2 Target 1](#_Toc13228267)

[3 Software 1](#_Toc13228268)

[4 Impact 1](#_Toc13228269)

[5 Server Update 2](#_Toc13228270)

[5.1 Deployment (TeliaCompany) 2](#_Toc13228271)

[6 Client Update 2](#_Toc13228272)

[6.1 Scenario 1 - To install the NICE XBAP security certificate on systems using an Internet connection: 2](#_Toc13228273)

[6.2 Scenario 2 - Installing the NICE XBAP Security Certificate on Systems with a Blocked or No Internet Connection 3](#_Toc13228274)

[6.3 Scenario 3 – Adding certificate to Group Policy 8](#_Toc13228275)

[6.3.1 To deploy a certificate by using Group Policy 8](#_Toc13228276)

[6.4 Client – Troubleshooting 9](#_Toc13228277)

[7 Validate Certificate 9](#_Toc13228278)

[7.1 To validate that the certificate is updated: 9](#_Toc13228279)

# Introduction

On June 24, 2019, the XBAP certificate will expire. Therefore, you will need a new version of XBAP and new certificates to avoid a warning message when you connect to the NICE system for the first time. The XBAP is used on all clients who are connecting to Nice Engage system.

# Target

IT Administrators at the customer.

# Software

NICE Engage Platform Release 6.5 or higher.

# Impact

* Workstations that are already deployed and have an internet connection, will have no impact whatsoever as the XBAP was already deployed.
* New workstations, upon initial login, will get a security warning showing that the software is from an ‘unknown publisher’ until that latest XBAP software is updated. There is no impact on the user’s ability to continue working with the solution.

# Server Update

## **Deployment (TeliaCompany)**

After the XBAP software has been deployed on the Applications Server (performed by Telia), the new XBAP softwarewill automatically be deployed to the workstations at login.

The certificates are automatically transferred to the Certificates - Current User directory’s Personal folder. This will cause a security warning to appear during the deployment process.

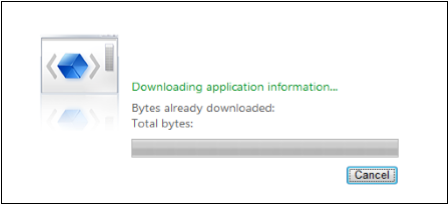
If you do not want a security warning to appear, you must manually move the NICE certificate to the Trusted publisher folder as described in Installing the NICE XBAP Security Certificate on Systems with a Blocked or No Internet Connection, steps 6.2

# Client Update

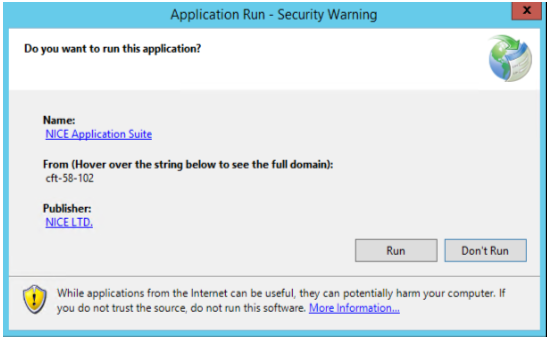
The certificates can be downloaded from <https://docs.ace.teliacompany.com/15.0/sv/Downloads.htm>

## Scenario 1 - To install the NICE XBAP security certificate on systems using an Internet connection:

1. Enter the URL <http://rec.callguide.telia.com/nice> or <http://rec.ace.teliacompany.com/nice> (depending on your location).



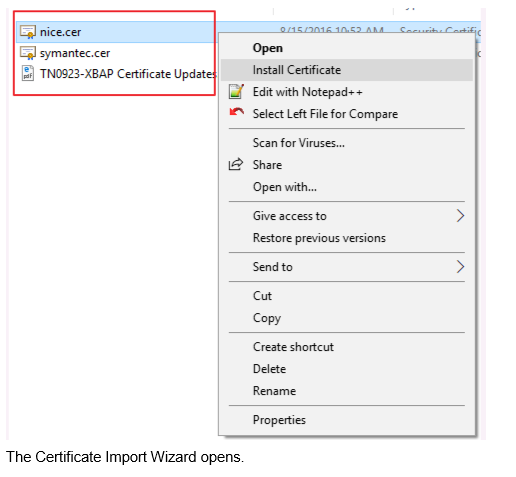




To avoid the Security warning install the certificates according to step 6.2

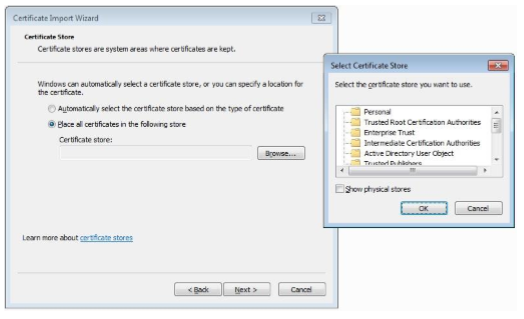
## Scenario 2 - Installing the NICE XBAP Security Certificate on Systems with a Blocked or No Internet Connection

1. Extract the contents of the NICE\_cert\_and\_documentation.zip to a local drive.
2. From this location, import the NICE certificate. Right-click nice.cer, and click Install Certificate.

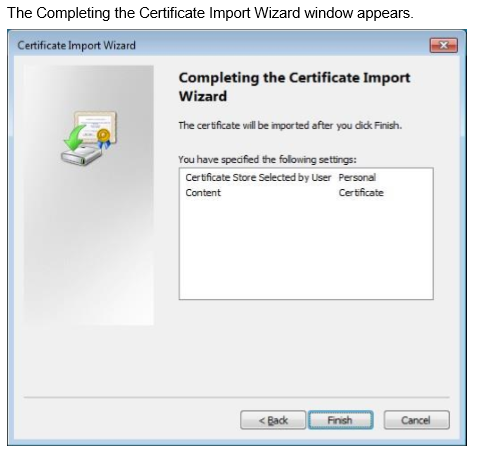




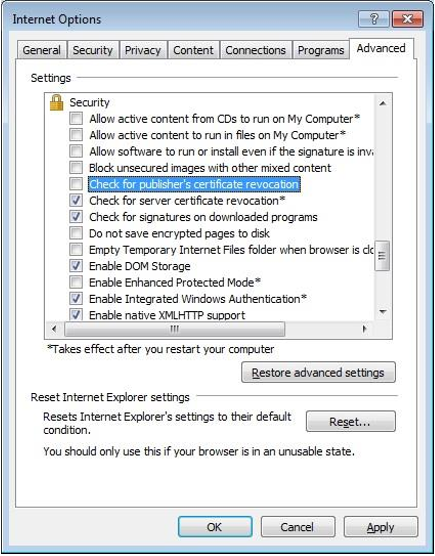
1. Select Local Machine, and click Next. The Certificate Store window opens.



* 1. Select Place all certificates in the following store, and click Browse.
  2. In the pop-up window, click Personal if you want a security warning to appear or Trusted Publishers if you want to prevent a security warning from appearing.
  3. Click OK.
  4. Click Next.

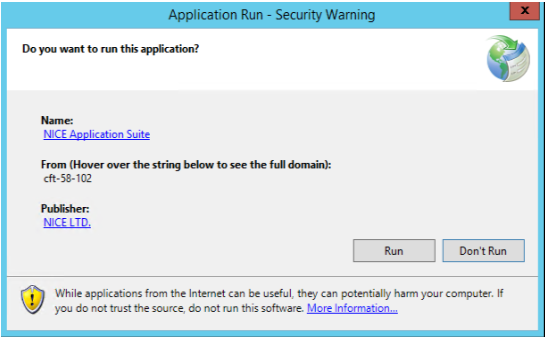


1. Click Finish.
2. To import the Symantec certificate, repeat steps 2 to 4 for the symantec.cer file. In step 3b, click Intermediate Certification Authorities to place the Symantec certificate in that folder.
3. In Internet Explorer, click Tools > Internet Options.

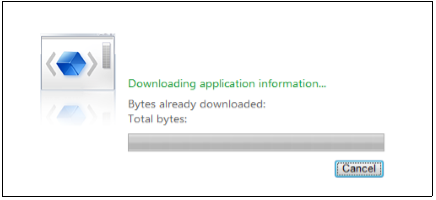


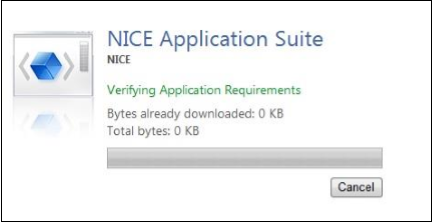
* 1. Clear Check for publisher's certificate revocation.
  2. Click Apply and then OK.

1. If the NICE certificate is placed in the Personal folder and not in the Trusted publishers folder, the following security warning appears on the workstation prior to logging into the system. Click Run.

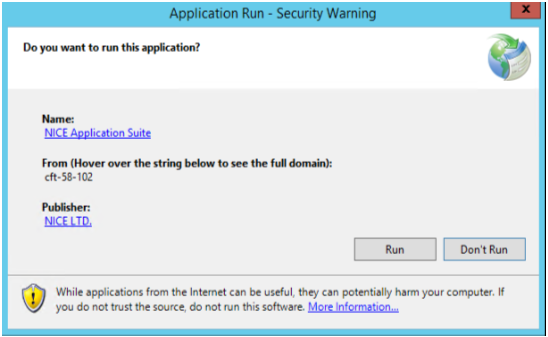


1. In the workstation, when logging in for the first time after installing the XBAP software, open a new Internet Explorer window, and enter the following URL <http://rec.callguide.telia.com/nice> or <http://rec.ace.teliacompany.com/nice> (depending on your location).





NOTE: If the NICE certificate was not placed in the Trusted Publishers folder (as mentioned in step 3), the following security warning appears. Click Run to complete the installation.



1. Once the installation is complete, log into NICE Engage Platform.

## Scenario 3 – Adding certificate to Group Policy

To deploy the certificates centrally on each workstation via group policy in Active Directory DC Server, refer to Microsoft’s Instructions in http://technet.microsoft.com/en-us/library/cc770315 (vws.10).aspx

You can use this procedure to deploy a certificate to multiple computers by using Active Directory Domain Services and a Group Policy object (GPO). A GPO can contain multiple configuration options, and is applied to all computers that are within the scope of the GPO.

Membership in the local **Administrators** group, or equivalent, is the minimum required to complete this procedure.

The Symantec certificate should be in the **Intermediate Certification Authorities** branch, Nice.LTD should be in the **Personal** or **Trusted Publishers** branch. If the Nice.LTD certificate is placed in the personal branch a security warning message will occur.

### To deploy a certificate by using Group Policy

Open Group Policy Management Console.

1. Find an existing or create a new GPO to contain the certificate settings. Ensure that the GPO is associated with the domain, site, or organizational unit whose users you want affected by the policy.
2. Right-click the GPO, and then select **Edit**.
3. Group Policy Management Editor opens, and displays the current contents of the policy object.
4. In the navigation pane, open **Computer Configuration**\**Windows Settings**\**Security Settings**\**Public Key Policies**\**Trusted Publishers**.
5. Click the **Action** menu, and then click **Import**.
6. Follow the instructions in the **Certificate Import Wizard** to find and import the certificate.

## Client – Troubleshooting

If there are issues when deploying XBAP, clear the system’s cache memory in two stages:

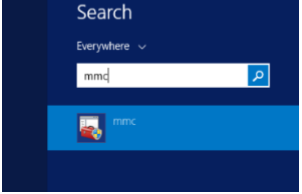
* Go to C:\Users\<username>\AppData>Local, and delete the Apps folder.
* Delete the browsing history in Internet Explorer.

# Validate Certificate

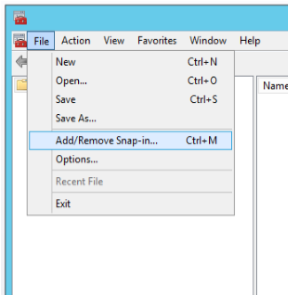
If a machine has internet access, you do not need to verify the certificates since the system compares the certificate with the internet certification authority and not the local one.

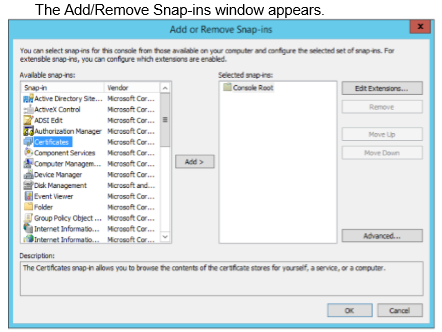
## To validate that the certificate is updated:

1. On the machine that needs to be verified, enter mmc in the search box and open the mmc console.

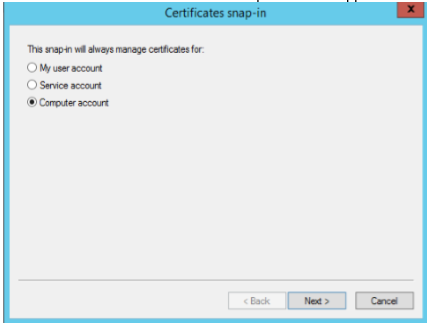


1. In the console, click File > Add/Remove Snap-in.

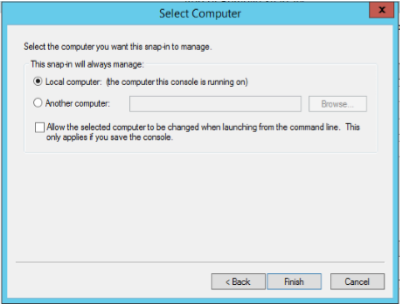




1. In the Add/Remove Snap-ins window:
   1. Click Certificates and Add to move the Certificates to the Selected snap-ins.
   2. Click OK. The Certificate Snap-in window appears.



1. In the Certificates snap-in window, select Computer account, and click Next. The Select Computer window appears.



1. In the Select Computer window, verify that Local computer is selected, and click Finish.
2. Go to the Console and verify that the Symantec certificate is in the Intermediate Certification Authorities branch, that Nice LTD. is in the Personal or Trusted Publishers branch.

